ZAP APPLICATION VULNERABILITY SCAN

ATTACKER'S NARRATIVE

An attacker targeting VulnBank could exploit multiple critical vulnerabilities to compromise the application and its users. The most severe issue is SQL injection, detected in both the login functionality and transaction API, allowing attackers to bypass authentication, extract sensitive data, and potentially gain administrative access. This vulnerability is compounded by cross-domain misconfiguration (CORS) that permits cross-origin requests from any domain, enabling attackers to access sensitive data from malicious websites when users are authenticated. Additionally, the outdated DOMPurify library (version 2.3.3) contains multiple CVEs that could allow attackers to bypass sanitization controls and execute cross-site scripting attacks.

The application also suffers from missing security headers, including Content Security Policy, X-Frame-Options, and Strict-Transport-Security, making it vulnerable to clickjacking, XSS, and man-in-the-middle attacks. Suspicious comments in the code and information disclosure in URLs further expose implementation details that attackers could leverage. The presence of user-controllable HTML attributes creates additional XSS opportunities, while improper cache control settings could lead to sensitive information being stored in browsers.

To remediate these issues, VulnBank should immediately implement parameterized queries for all database operations to prevent SQL injection. The CORS configuration should be restricted to only allow necessary domains. Security headers should be properly implemented, including CSP with appropriate directives, X-Frame-Options, and HSTS. The DOMPurify library should be updated to the latest version, and all user input should be properly validated and sanitized before being included in responses. Additionally, sensitive information should be removed from URLs and code comments, and proper cache control directives should be set to prevent caching of sensitive data.

ZAP Scanning Report

Sites: https://static.cloudflareinsights.com https://vulnbank.org

Generated on Sat, 27 Dec 2025 03:40:41

ZAP Version: 2.15.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	3
Medium	4
Low	8
Informational	6
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
SQL Injection	High	1
SQL Injection - PostgreSQL	High	5
Vulnerable JS Library	High	1
Content Security Policy (CSP) Header Not Set	Medium	39
Cross-Domain Misconfiguration	Medium	86
Missing Anti-clickjacking Header	Medium	29
ZAP is Out of Date	Medium	2
Application Error Disclosure	Low	2
Big Redirect Detected (Potential Sensitive Information Leak)	Low	1
Cookie Without Secure Flag	Low	1
Cookie without SameSite Attribute	Low	1
Cross Site Scripting Weakness (Persistent in JSON Response)	Low	2
Strict-Transport-Security Header Not Set	Low	90
Timestamp Disclosure - Unix	Low	69
X-Content-Type-Options Header Missing	Low	65
Information Disclosure - Sensitive Information in URL	Informational	5
Information Disclosure - Suspicious Comments	Informational	32
Modern Web Application	Informational	28
Re-examine Cache-control Directives	Informational	40
User Agent Fuzzer	Informational	420
User Controllable HTML Element Attribute (Potential XSS)	Informational	18

Alert Detail

High	SQL Injection
Description	SQL injection may be possible.
URL	https://vulnbank.org/api/transactions?account_number=account_number%27+AND+%271%27%3D%271%27+--+
Method	GET
Parameter	account_number
Attack	account_number' OR '1'='1' --

Evidence	
Other Info	The page results were successfully manipulated using the boolean conditions [account_number' AND '1'='1' --] and [account_number' OR '1'='1' --] The parameter value being modified was stripped from the HTML output for the purposes of the comparison. Data was NOT returned for the original parameter. The vulnerability was detected by successfully retrieving more data than originally returned, by manipulating the parameter.
Instances	1
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
CWE Id	89
WASC Id	19
Plugin Id	40018

High	**SQL Injection - PostgreSQL**
Description	SQL injection may be possible.
URL	https://vulnbank.org/api/virtual-cards/create
Method	POST
Parameter	card_type
Attack	standard') UNION ALL select NULL --
Evidence	each UNION query must have the same number of columns
Other Info	RDBMS [PostgreSQL] likely, given UNION-specific error message regular expression [\Qeach UNION query must have the same number of columns\E] matched by the HTML results The vulnerability was detected by manipulating the parameter with an SQL UNION clause to cause a database error message to be returned and recognised.
URL	https://vulnbank.org/login
Method	POST
Parameter	password
Attack	justatest' UNION ALL select NULL --
Evidence	each UNION query must have the same number of columns
Other Info	RDBMS [PostgreSQL] likely, given UNION-specific error message regular expression [\Qeach UNION query must have the same number of columns\E] matched by the HTML results The vulnerability was detected by manipulating the parameter with an SQL UNION clause to cause a database error message to be returned and recognised.
URL	https://vulnbank.org/login
Method	POST
Parameter	password
Attack	password123' UNION ALL select NULL --
Evidence	each UNION query must have the same number of columns
Other Info	RDBMS [PostgreSQL] likely, given UNION-specific error message regular expression [\Qeach UNION query must have the same number of columns\E] matched by the HTML results The vulnerability was detected by manipulating the parameter with an SQL UNION clause to cause a database error message to be returned and recognised.
URL	https://vulnbank.org/login
Method	POST
Parameter	username

Attack	justatest' UNION ALL select NULL --
Evidence	each UNION query must have the same number of columns
Other Info	RDBMS [PostgreSQL] likely, given UNION-specific error message regular expression [\Qeach UNION query must have the same number of columns\E] matched by the HTML results The vulnerability was detected by manipulating the parameter with an SQL UNION clause to cause a database error message to be returned and recognised.
URL	https://vulnbank.org/login
Method	POST
Parameter	username
Attack	testuser' UNION ALL select NULL --
Evidence	each UNION query must have the same number of columns
Other Info	RDBMS [PostgreSQL] likely, given UNION-specific error message regular expression [\Qeach UNION query must have the same number of columns\E] matched by the HTML results The vulnerability was detected by manipulating the parameter with an SQL UNION clause to cause a database error message to be returned and recognised.
Instances	5
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
CWE Id	89
WASC Id	19
Plugin Id	40018

High	**Vulnerable JS Library**
Description	The identified library DOMPurify, version 2.3.3 is vulnerable.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	var o="dompurify"+(n?"#"+n:"");try{return e.createPolicy(o,{createHTML:function(e){return e}})}catch(e){return console.warn("TrustedTypes policy "+o+" could not be created."),null}};function G(){var e=arguments.length>0&&void 0!==arguments[0]?arguments[0]:J(),t=function(e){return G(e)};if(t.version="2.3.3"
Other Info	CVE-2024-47875 CVE-2024-48910 CVE-2024-45801
Instances	1
Solution	Please upgrade to the latest version of DOMPurify.
Reference	https://github.com/advisories/GHSA-gx9m-whjm-85jf https://github.com/cure53/DOMPurify/commit/6ea80cd8b47640c20f2f230c7920b1f4ce4fdf7a https://github.com/advisories/GHSA-p3vf-v8qc-cwcr https://github.com/cure53/DOMPurify/commit/0ef5e537a514f904b6aa1d7ad9e749e365d7185f https://github.com/cure53/DOMPurify/security/advisories/GHSA-p3vf-v8qc-cwcr https://nvd.nist.gov/vuln/detail/CVE-2024-45801 https://github.com/cure53/DOMPurify/security/advisories/GHSA-mmhx-hmjr-r674 https://github.com/cure53/DOMPurify/commit/d1dd0374caef2b4c56c3bd09fe1988c3479166dc https://github.com/cure53/DOMPurify https://github.com/advisories/GHSA-mmhx-hmjr-r674 https://github.com/cure53/DOMPurify/commit/26e1d69ca7f769f5c558619d644d90dd8bf26ebc

	https://nvd.nist.gov/vuln/detail/CVE-2024-47875 https://github.com/cure53/DOMPurify/security/advisories/GHSA-gx9m-whjm-85jf https://github.com/cure53/DOMPurify/blob/0ef5e537a514f904b6aa1d7ad9e749e365d7185f/test/test-suite.js#L2098 https://github.com/cure53/DOMPurify/commit/1e520262bf4c66b5efda49e2316d6d1246ca7b21 https://nvd.nist.gov/vuln/detail/CVE-2024-48910
CWE Id	1395
WASC Id	
Plugin Id	10003

Medium	**Content Security Policy (CSP) Header Not Set**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://vulnbank.org
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/docs/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/cdn-cgi/rum
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&profile_picture=test_file.txt

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/forgot-password
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/forgot-password?username=ZAP
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/latest/meta-data/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/latest/meta-data/iam/security-credentials/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/login
Method	GET
Parameter	
Attack	

Evidence	
Other Info	
URL	https://vulnbank.org/login?password=ZAP&username=ZAP
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/register
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/register?password=ZAP&username=ZAP
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/static
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/static/uploads
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/sup3r_s3cr3t_admin
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/transactions
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	39

Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	**Cross-Domain Misconfiguration**
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
URL	https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api/ai/system-info
Method	GET
Parameter	
Attack	

Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api/bill-categories
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api/bill-payments
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api/bill-payments/history
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api/billers/by-category/10
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api/docs
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api/docs/
Method	GET
Parameter	

Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api/docs/favicon-16x16.png
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api/docs/favicon-32x32.png
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api/docs/index.css
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api/docs/swagger-ui.css
Method	GET
Parameter	

Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api/transactions?account_number=account_number
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api/virtual-cards
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api/virtual-cards/10/transactions
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/check_balance/account_number
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/dashboard
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/dashboard?amount=1
Method	GET
Parameter	

Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *

Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&to_account=ZAP
Method	GET
Parameter	

Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/dashboard?amount=1&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/dashboard?amount=1&description&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/dashboard?amount=1&profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	

Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/dashboard?profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/forgot-password
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/forgot-password?username=ZAP
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/internal/config.json
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/internal/secret
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/latest/meta-data/
Method	GET

Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/latest/meta-data/iam/security-credentials/
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/latest/meta-data/iam/security-credentials/vulnbank-role
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/login
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/login?password=ZAP&username=ZAP
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/register
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/register?password=ZAP&username=ZAP
Method	GET

Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/static
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/static/auth.css
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/static/dashboard.css
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/static/dashboard.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/static/favicon-16.svg

Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/static/favicon.svg
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/static/openapi.json
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/static/style.css
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/static/uploads
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/static/uploads/199396_SampleZAPFile
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

URL	https://vulnbank.org/static/uploads/banking-app.png
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/static/uploads/user.png
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/sup3r_s3cr3t_admin
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/transactions
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/transactions/0080071723
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/transactions/account_number
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

URL	https://vulnbank.org/admin/approve_loan/10
Method	POST
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/admin/create_admin
Method	POST
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/admin/delete_account/10
Method	POST
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api/ai/chat
Method	POST
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api/ai/chat/anonymous
Method	POST
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api/bill-payments/create
Method	POST
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

URL	https://vulnbank.org/api/v3/forgot-password
Method	POST
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api/v3/reset-password
Method	POST
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api/virtual-cards/10/toggle-freeze
Method	POST
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api/virtual-cards/10/update-limit
Method	POST
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/api/virtual-cards/create
Method	POST
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/login
Method	POST
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP

	address white-listing.
URL	https://vulnbank.org/register
Method	POST
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/request_loan
Method	POST
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/transfer
Method	POST
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/upload_profile_picture
Method	POST
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://vulnbank.org/upload_profile_picture_url
Method	POST
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Instances	86
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
CWE Id	264
WASC Id	14

Plugin Id	10098

Medium	Missing Anti-clickjacking Header
Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	https://vulnbank.org
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/docs/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card
Method	GET

Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	x-frame-options
Attack	
Evidence	

Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&to_account=ZAP
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&to_account=ZAP
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&profile_picture=test_file.txt
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?profile_picture=test_file.txt
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/forgot-password

Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/forgot-password?username=ZAP
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/login
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/login?password=ZAP&username=ZAP
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/register
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/register?password=ZAP&username=ZAP
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
Instances	29
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Medium	**ZAP is Out of Date**
Description	The version of ZAP you are using to test your app is out of date and is no longer being updated. The risk level is set based on how out of date your ZAP version is.
URL	https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015
Method	GET
Parameter	

Attack	
Evidence	
Other Info	The latest version of ZAP is 2.17.0
URL	https://vulnbank.org/static/style.css
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The latest version of ZAP is 2.17.0
Instances	2
Solution	Download the latest version of ZAP from https://www.zaproxy.org/download/ and install it.
Reference	https://www.zaproxy.org/download/
CWE Id	1104
WASC Id	45
Plugin Id	10116

Low	**Application Error Disclosure**
Description	This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.
URL	https://vulnbank.org/api/virtual-cards/10/update-limit
Method	POST
Parameter	
Attack	
Evidence	HTTP/1.1 500 Internal Server Error
Other Info	
URL	https://vulnbank.org/upload_profile_picture_url
Method	POST
Parameter	
Attack	
Evidence	HTTP/1.1 500 Internal Server Error
Other Info	
Instances	2
Solution	Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	90022

Low	**Big Redirect Detected (Potential Sensitive Information Leak)**
Description	The server has responded with a redirect that seems to provide a large response. This may indicate that although the server sent a redirect it also responded with body content (which may include sensitive details, PII, etc.).
URL	https://vulnbank.org/api/docs
Method	GET
Parameter	
Attack	
Evidence	
Other Info	Location header URI length: 29 [http://vulnbank.org/api/docs/]. Predicted response size: 329. Response Body Length: 769.
Instances	1
Solution	Ensure that no sensitive information is leaked via redirect responses. Redirect responses should have almost no content.
Reference	
CWE Id	201

WASC Id	13
Plugin Id	10044

Low	**Cookie Without Secure Flag**
Description	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
URL	https://vulnbank.org/login
Method	POST
Parameter	token
Attack	
Evidence	Set-Cookie: token
Other Info	
Instances	1
Solution	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Reference	https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html
CWE Id	614
WASC Id	13
Plugin Id	10011

Low	**Cookie without SameSite Attribute**
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	https://vulnbank.org/login
Method	POST
Parameter	token
Attack	
Evidence	Set-Cookie: token
Other Info	
Instances	1
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Low	**Cross Site Scripting Weakness (Persistent in JSON Response)**
Description	A XSS attack was found in a JSON response, this might leave content consumers vulnerable to attack if they don't appropriately handle the data (response).
URL	https://vulnbank.org/api/bill-payments/history
Method	GET
Parameter	payment_method
Attack	<script>alert(1);</script>
Evidence	
Other Info	Raised with LOW confidence as the Content-Type is not HTML.
URL	https://vulnbank.org/api/virtual-cards
Method	GET
Parameter	card_type
Attack	<script>alert(1);</script>
Evidence	
Other Info	Raised with LOW confidence as the Content-Type is not HTML.
Instances	2
	Phase: Architecture and Design

Solution	Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket. Phases: Implementation; Architecture and Design Understand the context in which your data will be used and the encoding that will be expected. This is especially important when transmitting data between different components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to determine the required encoding strategies. For any data that will be output to another web page, especially any data that was received from external inputs, use the appropriate encoding on all non-alphanumeric characters. Consult the XSS Prevention Cheat Sheet for more details on the types of encoding and escaping that are needed. Phase: Architecture and Design For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server. If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated. Phase: Implementation For every web page that is generated, use and specify a character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actually being used by the web page. This can cause the web browser to treat certain sequences as special, opening up the client to subtle XSS attacks. See CWE-116 for more mitigations related to encoding/escaping. To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHTTPRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set. Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." Ensure that you perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved elsewhere.
Reference	https://owasp.org/www-community/attacks/xss/ https://cwe.mitre.org/data/definitions/79.html
CWE Id	79
WASC Id	8
Plugin Id	40014

Low	**Strict-Transport-Security Header Not Set**
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
URL	https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://vulnbank.org
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/system-info
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-categories
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/history
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/billers/by-category/10
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/docs
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/docs/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/docs/favicon-16x16.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/docs/favicon-32x32.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/docs/index.css
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/docs/swagger-ui.css
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/transactions?account_number=account_number
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://vulnbank.org/api/virtual-cards
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards/10/transactions
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/cdn-cgi
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/cdn-cgi/rum
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/check_balance/account_number
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	
Attack	

Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/forgot-password
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/forgot-password?username=ZAP
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/internal/config.json
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/internal/secret
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/latest/meta-data/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/latest/meta-data/iam/security-credentials/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/latest/meta-data/iam/security-credentials/vulnbank-role
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/login

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/login?password=ZAP&username=ZAP
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/register
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/register?password=ZAP&username=ZAP
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/static
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/static/auth.css
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/static/dashboard.css
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/static/dashboard.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/static/favicon-16.svg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/static/favicon.svg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/static/openapi.json
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/static/style.css
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/static/uploads
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/static/uploads/199396_SampleZAPFile
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/static/uploads/banking-app.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	https://vulnbank.org/static/uploads/user.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/sup3r_s3cr3t_admin
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/transactions
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/0080071723
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/account_number
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/admin/approve_loan/10
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/admin/create_admin
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/admin/delete_account/10
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat
Method	POST

Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat/anonymous
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/create
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/v3/forgot-password
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/v3/reset-password
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards/10/toggle-freeze
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards/10/update-limit
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards/create
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/cdn-cgi/rum
Method	POST
Parameter	
Attack	
Evidence	

Other Info	
URL	https://vulnbank.org/login
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/register
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/request_loan
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/transfer
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture_url
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
Instances	90
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET

Parameter	
Attack	
Evidence	1467031594
Other Info	1467031594, which evaluates to: 2016-06-27 12:46:34.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1495990901
Other Info	1495990901, which evaluates to: 2017-05-28 17:01:41.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1501505948
Other Info	1501505948, which evaluates to: 2017-07-31 12:59:08.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1508970993
Other Info	1508970993, which evaluates to: 2017-10-25 22:36:33.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1518500249
Other Info	1518500249, which evaluates to: 2018-02-13 05:37:29.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1522805485
Other Info	1522805485, which evaluates to: 2018-04-04 01:31:25.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1537002063
Other Info	1537002063, which evaluates to: 2018-09-15 09:01:03.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1541459225
Other Info	1541459225, which evaluates to: 2018-11-05 23:07:05.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1546045734

Other Info	1546045734, which evaluates to: 2018-12-29 01:08:54.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1555081692
Other Info	1555081692, which evaluates to: 2019-04-12 15:08:12.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1575990012
Other Info	1575990012, which evaluates to: 2019-12-10 15:00:12.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1595750129
Other Info	1595750129, which evaluates to: 2020-07-26 07:55:29.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1607167915
Other Info	1607167915, which evaluates to: 2020-12-05 11:31:55.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1654270250
Other Info	1654270250, which evaluates to: 2022-06-03 15:30:50.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1694076839
Other Info	1694076839, which evaluates to: 2023-09-07 08:53:59.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1695183700
Other Info	1695183700, which evaluates to: 2023-09-20 04:21:40.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1731405415
Other Info	1731405415, which evaluates to: 2024-11-12 09:56:55.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js

Method	GET
Parameter	
Attack	
Evidence	1732584193
Other Info	1732584193, which evaluates to: 2024-11-26 01:23:13.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1747873779
Other Info	1747873779, which evaluates to: 2025-05-22 00:29:39.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1750603025
Other Info	1750603025, which evaluates to: 2025-06-22 14:37:05.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1779033703
Other Info	1779033703, which evaluates to: 2026-05-17 16:01:43.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1816402316
Other Info	1816402316, which evaluates to: 2027-07-24 04:11:56.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1856431235
Other Info	1856431235, which evaluates to: 2028-10-29 11:20:35.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1859775393
Other Info	1859775393, which evaluates to: 2028-12-07 04:16:33.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1894007588
Other Info	1894007588, which evaluates to: 2030-01-07 09:13:08.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	

Attack	
Evidence	1899447441
Other Info	1899447441, which evaluates to: 2030-03-11 08:17:21.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1914138554
Other Info	1914138554, which evaluates to: 2030-08-28 09:09:14.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1925078388
Other Info	1925078388, which evaluates to: 2031-01-01 23:59:48.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1955562222
Other Info	1955562222, which evaluates to: 2031-12-20 19:43:42.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1986661051
Other Info	1986661051, which evaluates to: 2032-12-14 18:17:31.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	1996064986
Other Info	1996064986, which evaluates to: 2033-04-02 14:29:46.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	2003034995
Other Info	2003034995, which evaluates to: 2033-06-22 06:36:35.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	2007800933
Other Info	2007800933, which evaluates to: 2033-08-16 10:28:53.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	2024104815

Other Info	2024104815, which evaluates to: 2034-02-21 03:20:15.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1467031594
Other Info	1467031594, which evaluates to: 2016-06-27 12:46:34.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1495990901
Other Info	1495990901, which evaluates to: 2017-05-28 17:01:41.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1501505948
Other Info	1501505948, which evaluates to: 2017-07-31 12:59:08.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1508970993
Other Info	1508970993, which evaluates to: 2017-10-25 22:36:33.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1518500249
Other Info	1518500249, which evaluates to: 2018-02-13 05:37:29.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1522805485
Other Info	1522805485, which evaluates to: 2018-04-04 01:31:25.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1537002063
Other Info	1537002063, which evaluates to: 2018-09-15 09:01:03.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1541459225
Other Info	1541459225, which evaluates to: 2018-11-05 23:07:05.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET

Parameter	
Attack	
Evidence	1546045734
Other Info	1546045734, which evaluates to: 2018-12-29 01:08:54.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1555081692
Other Info	1555081692, which evaluates to: 2019-04-12 15:08:12.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1575990012
Other Info	1575990012, which evaluates to: 2019-12-10 15:00:12.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1595750129
Other Info	1595750129, which evaluates to: 2020-07-26 07:55:29.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1607167915
Other Info	1607167915, which evaluates to: 2020-12-05 11:31:55.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1654270250
Other Info	1654270250, which evaluates to: 2022-06-03 15:30:50.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1694076839
Other Info	1694076839, which evaluates to: 2023-09-07 08:53:59.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1695183700
Other Info	1695183700, which evaluates to: 2023-09-20 04:21:40.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	

Evidence	1731405415
Other Info	1731405415, which evaluates to: 2024-11-12 09:56:55.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1732584193
Other Info	1732584193, which evaluates to: 2024-11-26 01:23:13.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1747873779
Other Info	1747873779, which evaluates to: 2025-05-22 00:29:39.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1750603025
Other Info	1750603025, which evaluates to: 2025-06-22 14:37:05.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1779033703
Other Info	1779033703, which evaluates to: 2026-05-17 16:01:43.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1816402316
Other Info	1816402316, which evaluates to: 2027-07-24 04:11:56.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1856431235
Other Info	1856431235, which evaluates to: 2028-10-29 11:20:35.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1859775393
Other Info	1859775393, which evaluates to: 2028-12-07 04:16:33.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1894007588
Other Info	1894007588, which evaluates to: 2030-01-07 09:13:08.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js

Method	GET
Parameter	
Attack	
Evidence	1899447441
Other Info	1899447441, which evaluates to: 2030-03-11 08:17:21.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1914138554
Other Info	1914138554, which evaluates to: 2030-08-28 09:09:14.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1925078388
Other Info	1925078388, which evaluates to: 2031-01-01 23:59:48.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1955562222
Other Info	1955562222, which evaluates to: 2031-12-20 19:43:42.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1986661051
Other Info	1986661051, which evaluates to: 2032-12-14 18:17:31.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	1996064986
Other Info	1996064986, which evaluates to: 2033-04-02 14:29:46.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	2003034995
Other Info	2003034995, which evaluates to: 2033-06-22 06:36:35.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	2007800933
Other Info	2007800933, which evaluates to: 2033-08-16 10:28:53.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	

Evidence	2024104815
Other Info	2024104815, which evaluates to: 2034-02-21 03:20:15.
URL	https://vulnbank.org/login
Method	POST
Parameter	
Attack	
Evidence	2004262550
Other Info	2004262550, which evaluates to: 2033-07-06 11:35:50.
Instances	69
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	200
WASC Id	13
Plugin Id	10096

Low	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/api/ai/system-info
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/api/bill-categories
Method	GET
Parameter	x-content-type-options

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/api/bill-payments/history
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/api/billers/by-category/10
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/api/docs/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/api/docs/favicon-16x16.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/api/docs/favicon-32x32.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/api/docs/index.css
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	x-content-type-options

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/api/docs/swagger-ui.css
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/api/transactions?account_number=account_number
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/api/virtual-cards
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/api/virtual-cards/10/transactions
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/dashboard
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/dashboard?amount=1
Method	GET
Parameter	x-content-type-options

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	x-content-type-options
Attack	

Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&to_account=ZAP
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/dashboard?amount=1&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	x-content-type-options

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/dashboard?amount=1&description&to_account=ZAP
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/dashboard?amount=1&profile_picture=test_file.txt
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/dashboard?profile_picture=test_file.txt
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/forgot-password
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/forgot-password?username=ZAP
Method	GET
Parameter	x-content-type-options

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/login
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/login?password=ZAP&username=ZAP
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/register
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/register?password=ZAP&username=ZAP
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/robots.txt
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/static/auth.css
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/static/dashboard.css
Method	GET
Parameter	x-content-type-options

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/static/dashboard.js
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/static/favicon-16.svg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/static/favicon.svg
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/static/openapi.json
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/static/style.css
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/static/uploads/199396_SampleZAPFile
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/static/uploads/banking-app.png
Method	GET
Parameter	x-content-type-options

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/static/uploads/user.png
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/transactions/0080071723
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/transactions/account_number
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/api/ai/chat
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/api/ai/chat/anonymous
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/api/bill-payments/create
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/api/v3/forgot-password
Method	POST
Parameter	x-content-type-options

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/api/virtual-cards/create
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/login
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/request_loan
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/transfer
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://vulnbank.org/upload_profile_picture
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	65
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	**Information Disclosure - Sensitive Information in URL**

Description	The request appeared to contain sensitive information leaked in the URL. This can violate PCI and most organizational compliance policies. You can configure the list of strings for this check to add or remove values specific to your environment.
URL	https://vulnbank.org/forgot-password?username=ZAP
Method	GET
Parameter	username
Attack	
Evidence	username
Other Info	The URL contains potentially sensitive information. The following string was found via the pattern: user username
URL	https://vulnbank.org/login?password=ZAP&username=ZAP
Method	GET
Parameter	password
Attack	
Evidence	password
Other Info	The URL contains potentially sensitive information. The following string was found via the pattern: pass password
URL	https://vulnbank.org/login?password=ZAP&username=ZAP
Method	GET
Parameter	username
Attack	
Evidence	username
Other Info	The URL contains potentially sensitive information. The following string was found via the pattern: user username
URL	https://vulnbank.org/register?password=ZAP&username=ZAP
Method	GET
Parameter	password
Attack	
Evidence	password
Other Info	The URL contains potentially sensitive information. The following string was found via the pattern: pass password
URL	https://vulnbank.org/register?password=ZAP&username=ZAP
Method	GET
Parameter	username
Attack	
Evidence	username
Other Info	The URL contains potentially sensitive information. The following string was found via the pattern: user username
Instances	5
Solution	Do not pass sensitive information in URIs.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	10024

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	https://vulnbank.org
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script> // Landing Page Chat Widget JavaScript let landingChatOpen = false; // Initialize chat widget ", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/
Method	GET

Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script> // Landing Page Chat Widget JavaScript let landingChatOpen = false; // Initialize chat widget ", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/api/docs/
Method	GET
Parameter	
Attack	
Evidence	User
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script> var config = { presets: [SwaggerUIBundle.presets.apis, SwaggerUIStandalonePreset], ", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/api/docs/swagger-ui-bundle.js
Method	GET
Parameter	
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected in the element starting with: "!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?define", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/api/docs/swagger-ui-standalone-preset.js
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "!function(t,e){"object"==typeof exports&&"object"==typeof module?module.exports=e():"function"==typeof define&&define.amd?define", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/static/dashboard.js
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 7 times, the first in the element starting with: " // Remove active class from all links", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/static/dashboard.js
Method	GET
Parameter	
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected 4 times, the first in the element starting with: " rateLimitMessage += `${data.message || 'Too many requests. Please try again later.'}\n\n`;", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/static/dashboard.js
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 18 times, the first in the element starting with: " const select = document.getElementById('billCategory');", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/static/dashboard.js
Method	GET
Parameter	
Attack	

Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 8 times, the first in the element starting with: " // Add user message to chat", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/static/dashboard.js
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: " statusMessage += `**Authenticated Mode (${data.authenticated_user.username}):**\n`;", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/dashboard
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<!-- Vulnerability: XSS possible in username -->", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/dashboard?amount=1
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<!-- Vulnerability: XSS possible in username -->", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<!-- Vulnerability: XSS possible in username -->", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<!-- Vulnerability: XSS possible in username -->", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<!-- Vulnerability: XSS possible in username -->", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	
Attack	

Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<!-- Vulnerability: XSS possible in username -->", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<!-- Vulnerability: XSS possible in username -->", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<!-- Vulnerability: XSS possible in username -->", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<!-- Vulnerability: XSS possible in username -->", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<!-- Vulnerability: XSS possible in username -->", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<!-- Vulnerability: XSS possible in username -->", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<!-- Vulnerability: XSS possible in username -->", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	username

Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<!-- Vulnerability: XSS possible in username -->", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<!-- Vulnerability: XSS possible in username -->", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/dashboard?amount=1&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<!-- Vulnerability: XSS possible in username -->", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/dashboard?amount=1&description&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<!-- Vulnerability: XSS possible in username -->", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/dashboard?amount=1&profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<!-- Vulnerability: XSS possible in username -->", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<!-- Vulnerability: XSS possible in username -->", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<!-- Vulnerability: XSS possible in username -->", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/dashboard?profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<!-- Vulnerability: XSS possible in username -->", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/forgot-password
Method	GET
Parameter	

Attack	
Evidence	Username
Other Info	The following pattern was used: \bUSERNAME\b and was detected 2 times, the first in the element starting with: "<!-- Vulnerability: Username enumeration possible -->", see evidence field for the suspicious comment/snippet.
URL	https://vulnbank.org/forgot-password?username=ZAP
Method	GET
Parameter	
Attack	
Evidence	Username
Other Info	The following pattern was used: \bUSERNAME\b and was detected 2 times, the first in the element starting with: "<!-- Vulnerability: Username enumeration possible -->", see evidence field for the suspicious comment/snippet.
Instances	32
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	10027

Informational	**Modern Web Application**
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	https://vulnbank.org/api
Method	GET
Parameter	
Attack	
Evidence	<script defer src="https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015" integrity="sha512-ZpsOmlRQV6y907TI0dKBHq9Md29nnaEIPlkf84rnaERnq6zvWvPUqr2ft8M1aS28oN72PdrCzSjY4U6VaAw1EQ==" data-cf-beacon='{"version":"2024.11.0","token":"33081947b1cc42c6af62c2c84d28a474","r":1,"server_timing":{"name":{"cfCacheStatus":true,"cfEdge":true,"cfExtPri":true,"cfL4":true,"cfOrigin":true,"cfSpeedBrain":true},"location_startswith":null}}' crossorigin="anonymous"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://vulnbank.org/api/bill-payments
Method	GET
Parameter	
Attack	
Evidence	<script defer src="https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015" integrity="sha512-ZpsOmlRQV6y907TI0dKBHq9Md29nnaEIPlkf84rnaERnq6zvWvPUqr2ft8M1aS28oN72PdrCzSjY4U6VaAw1EQ==" data-cf-beacon='{"version":"2024.11.0","token":"33081947b1cc42c6af62c2c84d28a474","r":1,"server_timing":{"name":{"cfCacheStatus":true,"cfEdge":true,"cfExtPri":true,"cfL4":true,"cfOrigin":true,"cfSpeedBrain":true},"location_startswith":null}}' crossorigin="anonymous"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://vulnbank.org/api/docs/
Method	GET
Parameter	
Attack	
Evidence	<script src="/api/docs/swagger-ui-bundle.js"> </script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://vulnbank.org/cdn-cgi/rum
Method	GET
Parameter	
Attack	
Evidence	<script defer src="https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015" integrity="sha512-ZpsOmlRQV6y907TI0dKBHq9Md29nnaEIPlkf84rnaERnq6zvWvPUqr2ft8M1aS28oN72PdrCzSjY4U6VaAw1EQ==" data-cf-beacon='{"version":"2024.11.0","token":"33081947b1cc42c6af62c2c84d28a474","r":1,"server_timing":{"name":{"cfCacheStatus":true,"cfEdge":true,"cfExtPri":true,"cfL4":true,"cfOrigin":true,"cfSpeedBrain":true},"location_startswith":null}}'

	crossorigin="anonymous"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://vulnbank.org/dashboard
Method	GET
Parameter	
Attack	
Evidence	 Logout
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://vulnbank.org/dashboard?amount=1
Method	GET
Parameter	
Attack	
Evidence	 Logout
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	 Logout
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	 Logout
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	
Attack	
Evidence	 Logout
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	 Logout
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	 Logout
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&to_account=ZAP

Method	GET
Parameter	
Attack	
Evidence	 Logout
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	
Attack	
Evidence	 Logout
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	 Logout
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium
Method	GET
Parameter	
Attack	
Evidence	 Logout
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	 Logout
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	 Logout
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	 Logout
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://vulnbank.org/dashboard?amount=1&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	
Attack	
Evidence	 Logout
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://vulnbank.org/dashboard?amount=1&description&to_account=ZAP
Method	GET

Parameter	
Attack	
Evidence	 Logout
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://vulnbank.org/dashboard?amount=1&profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	 Logout
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium
Method	GET
Parameter	
Attack	
Evidence	 Logout
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	 Logout
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://vulnbank.org/dashboard?profile_picture=test_file.txt
Method	GET
Parameter	
Attack	
Evidence	 Logout
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://vulnbank.org/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	<script defer src="https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015" integrity="sha512-ZpsOmlRQV6y907TI0dKBHq9Md29nnaEIPlkf84rnaERnq6zvWvPUqr2ft8M1aS28oN72PdrCzSjY4U6VaAw1EQ==" data-cf-beacon='{"version":"2024.11.0","token":"33081947b1cc42c6af62c2c84d28a474","r":1,"server_timing":{"name":{"cfCacheStatus":true,"cfEdge":true,"cfExtPri":true,"cfL4":true,"cfOrigin":true,"cfSpeedBrain":true},"location_startswith":null}}' crossorigin="anonymous"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://vulnbank.org/static
Method	GET
Parameter	
Attack	
Evidence	<script defer src="https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015" integrity="sha512-ZpsOmlRQV6y907TI0dKBHq9Md29nnaEIPlkf84rnaERnq6zvWvPUqr2ft8M1aS28oN72PdrCzSjY4U6VaAw1EQ==" data-cf-beacon='{"version":"2024.11.0","token":"33081947b1cc42c6af62c2c84d28a474","r":1,"server_timing":{"name":{"cfCacheStatus":true,"cfEdge":true,"cfExtPri":true,"cfL4":true,"cfOrigin":true,"cfSpeedBrain":true},"location_startswith":null}}' crossorigin="anonymous"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://vulnbank.org/static/uploads
Method	GET
Parameter	
Attack	
	<script defer src="https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015"

Evidence	integrity="sha512-ZpsOmlRQV6y907TI0dKBHq9Md29nnaEIPlkf84rnaERnq6zvWvPUqr2ft8M1aS28oN72PdrCzSjY4U6VaAw1EQ==" data-cf-beacon='{"version":"2024.11.0","token":"33081947b1cc42c6af62c2c84d28a474","r":1,"server_timing":{"name":{"cfCacheStatus":true,"cfEdge":true,"cfExtPri":true,"cfL4":true,"cfOrigin":true,"cfSpeedBrain":true},"location_startswith":null}}' crossorigin="anonymous"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://vulnbank.org/transactions
Method	GET
Parameter	
Attack	
Evidence	<script defer src="https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015" integrity="sha512-ZpsOmlRQV6y907TI0dKBHq9Md29nnaEIPlkf84rnaERnq6zvWvPUqr2ft8M1aS28oN72PdrCzSjY4U6VaAw1EQ==" data-cf-beacon='{"version":"2024.11.0","token":"33081947b1cc42c6af62c2c84d28a474","r":1,"server_timing":{"name":{"cfCacheStatus":true,"cfEdge":true,"cfExtPri":true,"cfL4":true,"cfOrigin":true,"cfSpeedBrain":true},"location_startswith":null}}' crossorigin="anonymous"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
Instances	28
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	**Re-examine Cache-control Directives**
Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://vulnbank.org
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/system-info
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-categories
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/history
Method	GET
Parameter	cache-control
Attack	

Evidence	
Other Info	
URL	https://vulnbank.org/api/billers/by-category/10
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/docs/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/transactions?account_number=account_number
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards/10/transactions
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	cache-control
Attack	
Evidence	

Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium
Method	GET

Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&to_account=ZAP
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&to_account=ZAP
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&profile_picture=test_file.txt
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	cache-control
Attack	

Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?profile_picture=test_file.txt
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/forgot-password
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/forgot-password?username=ZAP
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/login
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/login?password=ZAP&username=ZAP
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/register
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/register?password=ZAP&username=ZAP
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/robots.txt
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/static/openapi.json

Method	GET
Parameter	cache-control
Attack	
Evidence	no-cache
Other Info	
URL	https://vulnbank.org/transactions/0080071723
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/account_number
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
Instances	40
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015

Informational	**User Agent Fuzzer**
Description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	https://vulnbank.org/api/ai/system-info
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/system-info
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/system-info
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/system-info
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	

Other Info	
URL	https://vulnbank.org/api/ai/system-info
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/system-info
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/system-info
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/system-info
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/system-info
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/system-info
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/system-info
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/system-info
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	

URL	https://vulnbank.org/api/bill-payments/history
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/history
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/history
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/history
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/history
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/history
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/history
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/history
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/history
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/history
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/history
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/history
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards
Method	GET
Parameter	Header User-Agent
	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36

Attack	Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

Evidence	
Other Info	
URL	https://vulnbank.org/dashboard
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	

URL	https://vulnbank.org/dashboard
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1

Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_car

	d&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
	https://vulnbank.org/dashboard?

URL	amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	

URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	

Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card

Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36

	Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	

URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?

	amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent

Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	

Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko

Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?

	amount=1&card_limit=1&card_type=premium&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&to_account=ZAP
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko

Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	

Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&profile_picture=test_file.txt&to_account=ZAP

Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&to_account=ZAP
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&description&to_account=ZAP
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	

Other Info	
URL	https://vulnbank.org/dashboard?amount=1&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?amount=1&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	

URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium&profile_picture=test_file.txt

Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36

Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/dashboard?profile_picture=test_file.txt
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/0080071723
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/0080071723
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	

Other Info	
URL	https://vulnbank.org/transactions/0080071723
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/0080071723
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/0080071723
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/0080071723
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/0080071723
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/0080071723
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/0080071723
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/0080071723
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	

URL	https://vulnbank.org/transactions/0080071723
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/0080071723
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/account_number
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/account_number
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/account_number
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/account_number
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/account_number
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/account_number
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/account_number

Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/account_number
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/account_number
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/account_number
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/account_number
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/transactions/account_number
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat
Method	POST
Parameter	Header User-Agent

Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0

	Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat/anonymous
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat/anonymous
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat/anonymous
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat/anonymous
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat/anonymous
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat/anonymous
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat/anonymous
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	

Other Info	
URL	https://vulnbank.org/api/ai/chat/anonymous
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat/anonymous
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat/anonymous
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat/anonymous
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/api/ai/chat/anonymous
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/create
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/create
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/create
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/create

Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/create
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/create
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/create
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/create
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/create
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/create
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/create
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/api/bill-payments/create
Method	POST

Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/api/v3/forgot-password
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/api/v3/forgot-password
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/api/v3/forgot-password
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/api/v3/forgot-password
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/api/v3/forgot-password
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/api/v3/forgot-password
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/api/v3/forgot-password
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/api/v3/forgot-password
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

Evidence	
Other Info	
URL	https://vulnbank.org/api/v3/forgot-password
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/api/v3/forgot-password
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/api/v3/forgot-password
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/api/v3/forgot-password
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards/create
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards/create
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards/create
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards/create
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	

URL	https://vulnbank.org/api/virtual-cards/create
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards/create
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards/create
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards/create
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards/create
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards/create
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards/create
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/api/virtual-cards/create
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/login

Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/login
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/login
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/login
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/login
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/login
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/login
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/login
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/login
Method	POST
Parameter	Header User-Agent

Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/login
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/login
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/login
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/register
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/register
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/register
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/register
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/register
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0

Evidence	
Other Info	
URL	https://vulnbank.org/register
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/register
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/register
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/register
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/register
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/register
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/register
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/transfer
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	

Other Info	
URL	https://vulnbank.org/transfer
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/transfer
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/transfer
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/transfer
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/transfer
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/transfer
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/transfer
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/transfer
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/transfer

Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/transfer
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/transfer
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture
Method	POST

Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture_url
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture_url
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)

Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture_url
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture_url
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture_url
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture_url
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture_url
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture_url
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture_url
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture_url
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	

Other Info	
URL	https://vulnbank.org/upload_profile_picture_url
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://vulnbank.org/upload_profile_picture_url
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	420
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104

Informational	**User Controllable HTML Element Attribute (Potential XSS)**
Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	card_type
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP appears to include user input in: a(n) [option] tag [value] attribute The user input found was: card_type=premium The user-controlled value was: premium
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	payment_method
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP appears to include user input in: a(n) [option] tag [value] attribute The user input found was: payment_method=virtual_card The user-controlled value was: virtual_card
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	card_type
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://vulnbank.org/dashboard?

Other Info	amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP appears to include user input in: a(n) [option] tag [value] attribute The user input found was: card_type=premium The user-controlled value was: premium
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	payment_method
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description&description=ZAP&payment_method=virtual_card&to_account=ZAP appears to include user input in: a(n) [option] tag [value] attribute The user input found was: payment_method=virtual_card The user-controlled value was: virtual_card
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	card_type
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card appears to include user input in: a(n) [option] tag [value] attribute The user input found was: card_type=premium The user-controlled value was: premium
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	payment_method
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card appears to include user input in: a(n) [option] tag [value] attribute The user input found was: payment_method=virtual_card The user-controlled value was: virtual_card
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	card_type
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt appears to include user input in: a(n) [option] tag [value] attribute The user input found was: card_type=premium The user-controlled value was: premium
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	payment_method
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://vulnbank.org/dashboard?amount=1&biller_id&card_id&card_limit=1&card_type=premium&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt appears to include user input in: a(n) [option] tag [value] attribute The user input found was: payment_method=virtual_card The user-controlled value was: virtual_card
	https://vulnbank.org/dashboard?

URL	amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	payment_method
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt&to_account=ZAP appears to include user input in: a(n) [option] tag [value] attribute The user input found was: payment_method=virtual_card The user-controlled value was: virtual_card
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&to_account=ZAP
Method	GET
Parameter	payment_method
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description&description=ZAP&payment_method=virtual_card&to_account=ZAP appears to include user input in: a(n) [option] tag [value] attribute The user input found was: payment_method=virtual_card The user-controlled value was: virtual_card
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card
Method	GET
Parameter	payment_method
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card appears to include user input in: a(n) [option] tag [value] attribute The user input found was: payment_method=virtual_card The user-controlled value was: virtual_card
URL	https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt
Method	GET
Parameter	payment_method
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://vulnbank.org/dashboard?amount=1&biller_id&card_id&description=ZAP&payment_method=virtual_card&profile_picture=test_file.txt appears to include user input in: a(n) [option] tag [value] attribute The user input found was: payment_method=virtual_card The user-controlled value was: virtual_card
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium
Method	GET
Parameter	card_type
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium appears to include user input in: a(n) [option] tag [value] attribute The user input found was: card_type=premium The user-controlled value was: premium
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&profile_picture=test_file.txt&to_account=ZAP
Method	GET
Parameter	card_type
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&profile_picture=test_file.txt&to_account=ZAP appears to include

	user input in: a(n) [option] tag [value] attribute The user input found was: card_type=premium The user-controlled value was: premium
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&to_account=ZAP
Method	GET
Parameter	card_type
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&description&to_account=ZAP appears to include user input in: a(n) [option] tag [value] attribute The user input found was: card_type=premium The user-controlled value was: premium
URL	https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	card_type
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://vulnbank.org/dashboard?amount=1&card_limit=1&card_type=premium&profile_picture=test_file.txt appears to include user input in: a(n) [option] tag [value] attribute The user input found was: card_type=premium The user-controlled value was: premium
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium
Method	GET
Parameter	card_type
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://vulnbank.org/dashboard?card_limit=1&card_type=premium appears to include user input in: a(n) [option] tag [value] attribute The user input found was: card_type=premium The user-controlled value was: premium
URL	https://vulnbank.org/dashboard?card_limit=1&card_type=premium&profile_picture=test_file.txt
Method	GET
Parameter	card_type
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://vulnbank.org/dashboard?card_limit=1&card_type=premium&profile_picture=test_file.txt appears to include user input in: a(n) [option] tag [value] attribute The user input found was: card_type=premium The user-controlled value was: premium
Instances	18
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html
CWE Id	20
WASC Id	20
Plugin Id	10031