Web Application Security Assessment Report

Sec1
Cybersecurity AI Fortified

Executive Summary

This report presents the findings of the Web Application Security Assessment conducted using an Sec1 online, automated scanning tool to identify vulnerabilities in real-time within the web application of **. The assessment leverages advanced scanning technology to dynamically evaluate the application against industry-standard security benchmarks and identify potential security risks.

The identified vulnerabilities and corresponding recommendations are structured to facilitate an efficient remediation process, enabling ** to enhance its security posture. The evaluation results offer a snapshot of the application's current security status, providing actionable insights to address any weaknesses and mitigate risks.

Assumptions & Constraints

As the environment changes and new vulnerabilities and risks are discovered and made public, an application's overall security posture will change. Such changes may affect the validity of this report. Therefore, the conclusion reached from our analysis only represents a “snapshot” in time.

Objectives & Scope

Audit type	Automated Web Application Security Testing
Asset URL	**
Scan Datetime	05:50 GMT 09-Dec-2024

The assessment leveraged an automated scanning process to efficiently gather information about the target application and identify potential vulnerabilities in real time. The automated tool performed comprehensive discovery to detect information disclosure risks, input validation flaws, authentication and authorization weaknesses and session state management issues. By simulating real-world attack scenarios, the automated approach illuminated security risks by identifying weaknesses that could lead to unauthorized access or the exposure of sensitive information. The findings from this assessment were analyzed to develop targeted recommendations and mitigation strategies aimed at strengthening the overall security posture of the application. This automated approach ensured a consistent, scalable, and time-efficient evaluation while maintaining alignment with industry security standards.

Automated Web Application Testing Methodology

Our automated web application testing methodology is grounded in the following recognized industry standards and guidelines:

- OWASP Top 10 Application Security Risks - 2021
- OWASP Testing Guide
- OWASP Application Security Verification Standard (ASVS)

The Open Web Application Security Project (OWASP) is a globally recognized initiative that provides standards and resources for web application security. The OWASP Top 10 identifies the most common and critical vulnerabilities that threaten web applications today.

In our automated testing approach, we assess all of the vulnerabilities listed in the OWASP Top 10 and additional security concerns. The automated tools used in the testing process simulate real-world attack vectors to identify and report vulnerabilities in the application. This includes detecting issues related to authentication, authorization, input validation, session management and more.

The findings from the automated assessment, including identified vulnerabilities and the application security status against the OWASP Top 10, are summarized in the table below. This ensures that the testing covers the most critical security risks, providing an efficient and thorough evaluation of the application security posture.

Discovered URLs

As part of the Web Application Security Crawling process, a total of 100 URLs have been discovered. These resources represent the application accessible endpoints and will serve as the foundation for further security testing and analysis.

- *********************/js/hs.validation.js
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchantid=Test&status=SUCCESS&transactionid=Test&type=payments
- *********************/images/flyers.jpg
- *********************/js/phone.js
- *********************/account/transactions/quick-search?lang=en
- *********************/account/transactions?lang=en&lang=fr
- *********************/account/ticketing/liste?lang=fr
- *********************/account/profile?lang=en
- *********************/account/recharges?lang=fr
- *********************/account/ticketing/liste
- *********************/plugins/font-awesome/css/all.css
- *********************/account/manage/user
- *********************/account
- *********************/account/profile
- *********************/js/hs.fancybox.js
- *********************/account/ticketing/store
- *********************/js/hs.select2.js
- *********************/account/ticketing/liste?lang=en
- *********************/account/profile?lang=fr
- *********************/account/manage/user?lang=fr
- *********************/
- *********************/images/favicon.png
- *********************/account/transactions
- *********************/notifications/relaunch?lang=en
- *********************/sitemap.xml
- *********************/login
- *********************/plugins/dzsparallaxer/dzsparallaxer.css
- *********************
- *********************/account/transfer/bank?lang=fr

- *********************/account/transfer/bank/new?lang=fr
- *********************/account/recharges?lang=en
- *********************/plugins/bootstrap-table/bootstrap-table.min.css
- *********************/notifications/relaunch?lang=fr
- *********************/account/transactions?lang=en
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&type=All
- *********************/css/select2.min.css
- *********************/js/uikit.min.js
- *********************/account/transfer/bank?lang=en
- *********************/logout
- *********************/css/uikit.min.css
- *********************/notifications/relaunch?lang=en&lang=fr
- *********************/plugins/slick-carousel/slick/slick.js
- *********************/js/hs.mask.js
- *********************/plugins/bootstrap-table/locale/bootstrap-table-fr-FR.min.js
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&lang=fr&type=Tout
- *********************/account/transfer/bank?lang=en&lang=fr
- *********************/plugins/slick-carousel/slick/slick.css
- *********************/account/integration?lang=fr
- *********************/account/manage/role/store
- *********************/account/ticketing/liste?lang=en&lang=fr
- *********************/account/ticketing/nouveau?lang=en
- *********************/plugins/bootstrap-table/extensions/print/bootstrap-table-print.min.js
- *********************/js/hs.quill.js
- *********************/account/transfer/bank/new
- *********************/account/transfer/bank
- *********************/js/jquery.min.js
- *********************/replay-notification-model.xlsx
- *********************/account/manage/role?lang=en
- *********************/css/theme.css
- *********************/robots.txt
- *********************/account/recharges?df=2024-12-09&dt=2024-12-09
- *********************/js/hs.slick-carousel.js
- *********************/js/sweetalert2.all.js
- *********************/account/manage/user/create
- *********************/demo
- *********************/account/manage/role
- *********************/account/transfer/bank/new?lang=en
- *********************/account/recharges/new
- *********************/images/merchant_default.png
- *********************/account/transactions/quick-search
- *********************/account/integration?lang=en
- *********************/account/update
- *********************/account/manage/role?lang=fr
- *********************/account/transactions?lang=fr
- *********************/js/hs.core.js
- *********************/account/recharges
- *********************/plugins/bootstrap-table/bootstrap-table.min.js
- *********************/notifications/relaunch
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&type=Tout
- *********************/plugins/jquery-date-range-picker/daterangepicker.min.css
- *********************/js/bootstrap.bundle.min.js
- *********************/account/manage/user?lang=en
- *********************/account/manage/user?lang=en&lang=fr

- *********************/plugins/jquery-date-range-picker/moment.min.js
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchant_customer_id=Test&merchantid=Test&status=SUCCESS&transactionid=Test
- *********************/account?lang=en
- *********************/plugins/bootstrap-table/extensions/export/bootstrap-table-export.min.js
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&lang=en&type=Tout
- *********************/account/ticketing/nouveau?lang=fr
- *********************/js/uikit-icons.js
- *********************/plugins/jquery-date-range-picker/jquery.daterangepicker.min.js
- *********************/account/integration
- *********************/account/updatePassword
- *********************/account/transactions/quick-search?lang=fr
- *********************/css/custom.css
- *********************/account?lang=fr
- *********************/images/logo.png
- *********************/plugins/intl-tel-input/js/intlTelInput.min.js
- *********************/plugins/intl-tel-input/css/intlTelInput.min.css
- *********************/account/ticketing/nouveau

Findings Summary

Vulnerabilities by severity

The assessment was conducted using an automated security scanning tool aligned with the OWASP Web Application Testing Methodology, delivering the following results.

Severity	Critical	High	Medium	Low	Total
# of issues	0	1	4	8	13

Severity scoring:

- Critical - Immediate threat to key business processes.
- High - Direct threat to key business processes.
- Medium - Indirect threat to key business processes or partial threat to business processes.
- Low - No direct threat exists. Vulnerability may be exploited using other vulnerabilities.

S.No.	Issue Type	Severity	Count
1	Vulnerable JS Library	HIGH	1
2	Content Security Policy (CSP) Header Not Set	MEDIUM	64
3	Missing Anti-clickjacking Header	MEDIUM	52
4	Absence of Anti-CSRF Tokens	MEDIUM	2

S.No.	Issue Type	Severity	Count
5	Vulnerable JS Library	MEDIUM	1
6	Cookie Without Secure Flag	LOW	125
7	Strict-Transport-Security Header Not Set	LOW	99
8	Cross-Domain JavaScript Source File Inclusion	LOW	98
9	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	LOW	94
10	X-Content-Type-Options Header Missing	LOW	86
11	Cookie No HttpOnly Flag	LOW	61
12	Big Redirect Detected (Potential Sensitive Information Leak)	LOW	10
13	Application Error Disclosure	LOW	1

OWASP Top 10 Security Threats

S.No.	Criteria Label	Status
1	Broken Access Control	FAIL
2	Cryptographic Failures	FAIL
3	Identification and Authentication Failures	PASS
4	Injection	PASS
5	Insecure Design	FAIL
6	Security Logging and Monitoring Failures	PASS
7	Security Misconfiguration	FAIL
8	Server-Side Request Forgery (SSRF)	PASS
9	Software and Data Integrity Failures	FAIL
10	Vulnerable and Outdated Components	PASS

Network Port Mapping

S.No.	Port No	Protocol	State	Name	Product
1	21	tcp	filtered	ftp	-
2	22	tcp	filtered	ssh	-
3	25	tcp	open	smtp	Postfix smtpd
4	53	tcp	open	domain	Plesk Onyx BIND
5	80	tcp	open	http	nginx
6	106	tcp	open	tcpwrapped	-
7	110	tcp	open	pop3	Dovecot pop3d
8	143	tcp	open	imap	Dovecot imapd
9	443	tcp	open	http	nginx
10	465	tcp	open	smtp	Postfix smtpd
11	993	tcp	open	imap	Dovecot imapd
12	995	tcp	open	pop3	Dovecot pop3d
13	8443	tcp	filtered	https-alt	-

Findings Details

1. Vulnerable JS Library

There are 1 instances of this issue:

- **********************/plugins/jquery-date-range-picker/moment.min.js

Severity: HIGH

Vulnerability Id:CWE-829

Solutions

Please upgrade to the latest version of moment.js.

References

- https://github.com/moment/moment/security/advisories/GHSA-wc69-rhjr-hc9g
- https://security.snyk.io/vuln/SNYK-JS-MOMENT-2944238
- https://github.com/moment/moment/security/advisories/GHSA-8hfj-j24r-96c4
-

Tags

- https://nvd.nist.gov/vuln/detail/CVE-2022-24785

- https://nvd.nist.gov/vuln/detail/CVE-2022-31129
- https://nvd.nist.gov/vuln/detail/CVE-2023-22467
- https://cwe.mitre.org/data/definitions/829.html
- https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html
- https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

2. Content Security Policy (CSP) Header Not Set

There are 64 instances of this issue:

- *********************/account/transactions
- *********************/sitemap.xml
- *********************/account
- *********************/account/recharges
- *********************/account/transactions?lang=en
- *********************/logout
- *********************/notifications/relaunch
- *********************/account/integration
- *********************/account/transfer/bank
- *********************/account/profile
- *********************/account/transactions?lang=fr
- *********************/account/manage/user
- *********************/demo
- *********************/account/ticketing/liste
- *********************/logout
- *********************/account/updatePassword
- *********************/account/transactions/quick-search
- *********************/account/recharges?lang=en
- *********************/account/recharges/new
- *********************/account/recharges?df=2024-12-09&dt=2024-12-09
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchantid=Test&status=SUCCESS&transactionid=Test&type=payments
- *********************/account?lang=en
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchant_customer_id=Test&merchantid=Test&status=SUCCESS&transactionid=Test
- *********************/notifications/relaunch
- *********************/notifications/relaunch?lang=fr
- *********************/account/recharges?lang=fr
- *********************/account/integration?lang=fr
- *********************/account?lang=fr
- *********************/notifications/relaunch?lang=en
- *********************/account/integration?lang=en
- *********************/account/update
- *********************/account/manage/user
- *********************/account/integration
- *********************/account/profile?lang=fr
- *********************/account/transactions?lang=en&lang=fr
- *********************/account/profile?lang=en
- *********************/account/manage/role
- *********************/account/manage/user?lang=fr
- *********************/account/manage/user?lang=en
- *********************/account/manage/user/create
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&type=Tout
- *********************/account/ticketing/nouveau
- *********************/account/transfer/bank?lang=en

- ********************/account/ticketing/liste?lang=fr
- ********************/account/transfer/bank/new
- ********************/notifications/relaunch?lang=en&lang=fr
- ********************/account/ticketing/liste?lang=en
- ********************/account/manage/role?lang=en
- ********************/account/manage/role
- ********************/account/manage/user?lang=fr
- ********************/account/manage/user?lang=en
- ********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&lang=en&type=Tout
- ********************/account/manage/role?lang=fr
- ********************/account/manage/user?lang=en&lang=fr
- ********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&lang=fr&type=Tout
- ********************/account/ticketing/nouveau?lang=en
- ********************/account/transfer/bank?lang=en&lang=fr
- ********************/account/transfer/bank/new?lang=en
- ********************/account/ticketing/nouveau?lang=fr
- ********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&type=All
- ********************/account/ticketing/liste?lang=en&lang=fr
- ********************/account/transactions/quick-search?lang=en
- ********************/account/transfer/bank/new?lang=fr
- ********************/account/transactions/quick-search?lang=fr

Severity: MEDIUM

Vulnerability Id:CWE-693

Solutions

Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

References

- 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/

Tags

- https://cwe.mitre.org/data/definitions/693.html
- https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html
- https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

3. Missing Anti-clickjacking Header

There are 52 instances of this issue:

- ********************/account/transactions
- ********************/account
- ********************/account/recharges
- ********************/account/transactions?lang=en
- ********************/notifications/relaunch
- ********************/account/integration
- ********************/account/profile
- ********************/account/transfer/bank
- ********************/account/transactions?lang=fr

- *********************/account/manage/user
- *********************/demo
- *********************/account/ticketing/liste
- *********************/account/recharges/new
- *********************/account/recharges?lang=en
- *********************/account/recharges?df=2024-12-09&dt=2024-12-09
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchantid=Test&status=SUCCESS&transactionid=Test&type=payments
- *********************/account?lang=en
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchant_customer_id=Test&merchantid=Test&status=SUCCESS&transactionid=Test
- *********************/notifications/relaunch?lang=fr
- *********************/account/recharges?lang=fr
- *********************/account?lang=fr
- *********************/notifications/relaunch?lang=en
- *********************/account/integration?lang=fr
- *********************/account/integration?lang=en
- *********************/account/profile?lang=fr
- *********************/account/transactions?lang=en&lang=fr
- *********************/account/profile?lang=en
- *********************/account/manage/role
- *********************/account/manage/user?lang=fr
- *********************/account/manage/user?lang=en
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&type=Tout
- *********************/account/ticketing/nouveau
- *********************/account/transfer/bank?lang=en
- *********************/account/transfer/bank/new
- *********************/account/ticketing/liste?lang=fr
- *********************/notifications/relaunch?lang=en&lang=fr
- *********************/account/ticketing/liste?lang=en
- *********************/account/transactions/quick-search
- *********************/account/manage/role?lang=en
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&lang=en&type=Tout
- *********************/account/manage/user?lang=en&lang=fr
- *********************/account/manage/role?lang=fr
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&lang=fr&type=Tout
- *********************/account/ticketing/nouveau?lang=en
- *********************/account/transfer/bank?lang=en&lang=fr
- *********************/account/transfer/bank/new?lang=en
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&type=All
- *********************/account/ticketing/liste?lang=en&lang=fr
- *********************/account/ticketing/nouveau?lang=fr
- *********************/account/transactions/quick-search?lang=en
- *********************/account/transfer/bank/new?lang=fr
- *********************/account/transactions/quick-search?lang=fr

Severity: MEDIUM

Vulnerability Id:CWE-1021

Solutions

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.

References

- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Tags

- https://cwe.mitre.org/data/definitions/1021.html
- https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html
- https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
- https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testing_for_Clickjacking

4. Absence of Anti-CSRF Tokens

There are 2 instances of this issue:

- ********************/account/transactions/quick-search
- ********************/account/transactions/quick-search

Severity: MEDIUM

Vulnerability Id:CWE-352

Solutions

Phase: Architecture and Design
Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.
For example, use anti-CSRF packages such as the OWASP CSRFGuard.

Phase: Implementation
Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.

Phase: Architecture and Design
Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).
Note that this can be bypassed using XSS.

Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.
Note that this can be bypassed using XSS.

Use the ESAPI Session Management control.
This control includes a component for CSRF.

Do not use the GET method for any request that triggers a state change.

Phase: Implementation
Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

References

- https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html
- https://cwe.mitre.org/data/definitions/352.html

Tags

- https://cwe.mitre.org/data/definitions/352.html
- https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html
- https://owasp.org/Top10/A01_2021-Broken_Access_Control/
- https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery

5. Vulnerable JS Library

There are 1 instances of this issue:

- *********************/js/bootstrap.bundle.min.js

Severity: MEDIUM

Vulnerability Id:CWE-829

Solutions

Please upgrade to the latest version of bootstrap.

References

- https://www.herodevs.com/vulnerability-directory/cve-2024-6531
- https://github.com/advisories/GHSA-vc8w-jr9v-vj7f
- https://nvd.nist.gov/vuln/detail/CVE-2024-6531
- https://github.com/rubysec/ruby-advisory-db/blob/master/gems/bootstrap/CVE-2024-6531.yml
- https://github.com/twbs/bootstrap
-

Tags

- https://nvd.nist.gov/vuln/detail/CVE-2024-6531
- https://cwe.mitre.org/data/definitions/829.html
- https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html
- https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

6. Cookie Without Secure Flag

There are 125 instances of this issue:

- *********************/account/transactions
- *********************/account/transactions
- *********************
- *********************
- *********************/login
- *********************/login
- *********************/account
- *********************/account
- *********************/account/recharges
- *********************/account/recharges
- *********************/account/transactions?lang=en
- *********************/account/transactions?lang=en
- *********************/notifications/relaunch
- *********************/notifications/relaunch
- *********************/account/transfer/bank
- *********************/account/transfer/bank
- *********************/account/integration
- *********************/account/integration
- *********************/account/profile
- *********************/account/profile
- *********************/account/transactions?lang=fr

- *********************/account/transactions?lang=fr
- *********************/account/manage/user
- *********************/account/manage/user
- *********************/
- *********************/
- *********************/demo
- *********************/demo
- *********************/account/ticketing/liste
- *********************/account/ticketing/liste
- *********************/logout
- *********************/account/updatePassword
- *********************/account/transactions/quick-search
- *********************/account/recharges/new
- *********************/account/recharges?lang=en
- *********************/account/recharges?lang=en
- *********************/account/recharges/new
- *********************/account/recharges?df=2024-12-09&dt=2024-12-09
- *********************/account/recharges?df=2024-12-09&dt=2024-12-09
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchantid=Test&status=SUCCESS&transactionid=Test&type=payments
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchantid=Test&status=SUCCESS&transactionid=Test&type=payments
- *********************/account?lang=en
- *********************/account?lang=en
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchant_customer_id=Test&merchantid=Test&status=SUCCESS&transactionid=Test
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchant_customer_id=Test&merchantid=Test&status=SUCCESS&transactionid=Test
- *********************/notifications/relaunch
- *********************/notifications/relaunch
- *********************/notifications/relaunch?lang=fr
- *********************/notifications/relaunch?lang=fr
- *********************/account/recharges?lang=fr
- *********************/account/recharges?lang=fr
- *********************/account/integration?lang=fr
- *********************/account/integration?lang=fr
- *********************/account?lang=fr
- *********************/account?lang=fr
- *********************/notifications/relaunch?lang=en
- *********************/notifications/relaunch?lang=en
- *********************/account/integration?lang=en
- *********************/account/integration?lang=en
- *********************/account/integration
- *********************/account/update
- *********************/account/profile?lang=fr
- *********************/account/profile?lang=fr
- *********************/account/transactions?lang=en&lang=fr
- *********************/account/transactions?lang=en&lang=fr
- *********************/account/profile?lang=en
- *********************/account/profile?lang=en
- *********************/account/manage/role
- *********************/account/manage/role
- *********************/account/manage/user?lang=fr
- *********************/account/manage/user?lang=fr

- *********************/account/manage/user?lang=en
- *********************/account/manage/user?lang=en
- *********************/account/manage/user/create
- *********************/account/updatePassword
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&type=Tout
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&type=Tout
- *********************/account/ticketing/nouveau
- *********************/account/ticketing/nouveau
- *********************/account/transfer/bank?lang=en
- *********************/account/transfer/bank?lang=en
- *********************/account/ticketing/liste?lang=fr
- *********************/account/ticketing/liste?lang=fr
- *********************/account/transfer/bank/new
- *********************/account/transfer/bank/new
- *********************/account/manage/role/store
- *********************/account/manage/role/store
- *********************/account/transactions/quick-search
- *********************/account/ticketing/liste?lang=en
- *********************/notifications/relaunch?lang=en&lang=fr
- *********************/account/ticketing/liste?lang=en
- *********************/notifications/relaunch?lang=en&lang=fr
- *********************/account/manage/role?lang=en
- *********************/account/manage/role?lang=en
- *********************/account/manage/user/create
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&lang=en&type=Tout
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&lang=en&type=Tout
- *********************/account/manage/role?lang=fr
- *********************/account/manage/role?lang=fr
- *********************/account/manage/user?lang=en&lang=fr
- *********************/account/manage/user?lang=en&lang=fr
- *********************/account/ticketing/store
- *********************/account/ticketing/store
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&lang=fr&type=Tout
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&lang=fr&type=Tout
- *********************/account/ticketing/nouveau?lang=en
- *********************/account/ticketing/nouveau?lang=en
- *********************/account/transfer/bank?lang=en&lang=fr
- *********************/account/transfer/bank?lang=en&lang=fr
- *********************/account/transfer/bank/new?lang=en
- *********************/account/transfer/bank/new?lang=en
- *********************/account/ticketing/nouveau?lang=fr
- *********************/account/ticketing/nouveau?lang=fr
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&type=All
- *********************/account/ticketing/liste?lang=en&lang=fr
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&type=All
- *********************/account/ticketing/liste?lang=en&lang=fr
- *********************/account/transfer/bank
- *********************/account/transfer/bank
- *********************/account/transactions/quick-search?lang=en
- *********************/account/transactions/quick-search?lang=en
- *********************/account/transfer/bank/new?lang=fr
- *********************/account/transfer/bank/new?lang=fr
- *********************/account/transactions/quick-search?lang=fr
- *********************/account/transactions/quick-search?lang=fr

Severity: LOW

Vulnerability Id:CWE-614

Solutions

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.

References

- 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

Tags

- https://cwe.mitre.org/data/definitions/614.html
- https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html
- https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
- https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes

7. Strict-Transport-Security Header Not Set

There are 99 instances of this issue:

- *********************/account/transactions
- *********************/sitemap.xml
- *********************/account
- *********************/account/recharges
- *********************/account/transactions?lang=en
- *********************/logout
- *********************/notifications/relaunch
- *********************/account/transfer/bank
- *********************/account/integration
- *********************/account/profile
- *********************/account/transactions?lang=fr
- *********************/account/manage/user
- *********************/plugins/bootstrap-table/bootstrap-table.min.css
- *********************/plugins/dzsparallaxer/dzsparallaxer.css
- *********************/plugins/intl-tel-input/css/intlTelInput.min.css
- *********************/plugins/jquery-date-range-picker/daterangepicker.min.css
- *********************/plugins/slick-carousel/slick/slick.css
- *********************/images/favicon.png
- *********************/js/jquery.min.js
- *********************/js/bootstrap.bundle.min.js
- *********************/css/uikit.min.css
- *********************/css/theme.css
- *********************/js/hs.mask.js
- *********************/js/hs.core.js
- *********************/js/hs.quill.js
- *********************/js/hs.select2.js
- *********************/plugins/font-awesome/css/all.css
- *********************/css/custom.css
- *********************/js/hs.validation.js
- *********************/demo
- *********************/account/ticketing/liste
- *********************/js/sweetalert2.all.js
- *********************/plugins/bootstrap-table/locale/bootstrap-table-fr-FR.min.js

- *********************/images/merchant_default.png
- *********************/js/hs.fancybox.js
- *********************/images/logo.png
- *********************/plugins/intl-tel-input/js/intlTelInput.min.js
- *********************/plugins/jquery-date-range-picker/jquery.daterangepicker.min.js
- *********************/logout
- *********************/plugins/jquery-date-range-picker/moment.min.js
- *********************/plugins/slick-carousel/slick/slick.js
- *********************/account/updatePassword
- *********************/account/transactions/quick-search
- *********************/plugins/bootstrap-table/extensions/export/bootstrap-table-export.min.js
- *********************/plugins/bootstrap-table/extensions/print/bootstrap-table-print.min.js
- *********************/js/uikit-icons.js
- *********************/js/uikit.min.js
- *********************/plugins/bootstrap-table/bootstrap-table.min.js
- *********************/js/hs.slick-carousel.js
- *********************/account/recharges/new
- *********************/account/recharges?lang=en
- *********************/account/recharges?df=2024-12-09&dt=2024-12-09
- *********************/account?lang=en
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchant_customer_id=Test&merchantid=Test&status=SUCCESS&transactionid=Test
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchantid=Test&status=SUCCESS&transactionid=Test&type=payments
- *********************/replay-notification-model.xlsx
- *********************/notifications/relaunch
- *********************/notifications/relaunch?lang=fr
- *********************/account/recharges?lang=fr
- *********************/account?lang=fr
- *********************/account/integration?lang=fr
- *********************/notifications/relaunch?lang=en
- *********************/account/integration?lang=en
- *********************/images/flyers.jpg
- *********************/js/phone.js
- *********************/account/manage/user
- *********************/account/integration
- *********************/account/update
- *********************/css/select2.min.css
- *********************/account/profile?lang=fr
- *********************/account/transactions?lang=en&lang=fr
- *********************/account/profile?lang=en
- *********************/account/manage/role
- *********************/account/manage/user?lang=fr
- *********************/account/manage/user?lang=en
- *********************/account/manage/user/create
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&type=Tout
- *********************/account/ticketing/nouveau
- *********************/account/ticketing/liste?lang=fr
- *********************/account/transfer/bank/new
- *********************/account/transfer/bank?lang=en
- *********************/notifications/relaunch?lang=en&lang=fr
- *********************/account/ticketing/liste?lang=en
- *********************/account/manage/role?lang=en
- *********************/account/manage/role

- *********************/account/manage/user?lang=en
- *********************/account/manage/user?lang=fr
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&lang=en&type=Tout
- *********************/account/manage/role?lang=fr
- *********************/account/manage/user?lang=en&lang=fr
- *********************/account/transfer/bank?lang=en&lang=fr
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&lang=fr&type=Tout
- *********************/account/ticketing/nouveau?lang=en
- *********************/account/transfer/bank/new?lang=en
- *********************/account/ticketing/liste?lang=en&lang=fr
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&type=All
- *********************/account/ticketing/nouveau?lang=fr
- *********************/account/transactions/quick-search?lang=en
- *********************/account/transfer/bank/new?lang=fr

Severity: LOW

Vulnerability Id:CWE-319

Solutions

Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

References

- 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

Tags

- https://cwe.mitre.org/data/definitions/319.html
- https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html
- https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

8. Cross-Domain JavaScript Source File Inclusion

There are 98 instances of this issue:

- *********************/account/transactions
- *********************/account/transactions
- *********************/account/transactions
- *********************/account/transactions
- *********************/account
- *********************/account/recharges
- *********************/account/transactions?lang=en
- *********************/account/transactions?lang=en
- *********************/account/transactions?lang=en
- *********************/account/transactions?lang=en
- *********************/notifications/relaunch
- *********************/account/transfer/bank
- *********************/account/integration
- *********************/account/profile
- *********************/account/transactions?lang=fr
- *********************/account/transactions?lang=fr
- *********************/account/transactions?lang=fr
- *********************/account/transactions?lang=fr

- *********************/account/manage/user
- *********************/account/manage/user
- *********************/account/manage/user
- *********************/account/manage/user
- *********************/demo
- *********************/account/ticketing/liste
- *********************/account/recharges?lang=en
- *********************/account/recharges/new
- *********************/account/recharges?df=2024-12-09&dt=2024-12-09
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchantid=Test&status=SUCCESS&transactionid=Test&type=payments
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchantid=Test&status=SUCCESS&transactionid=Test&type=payments
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchantid=Test&status=SUCCESS&transactionid=Test&type=payments
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchantid=Test&status=SUCCESS&transactionid=Test&type=payments
- *********************/account?lang=en
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchant_customer_id=Test&merchantid=Test&status=SUCCESS&transactionid=Test
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchant_customer_id=Test&merchantid=Test&status=SUCCESS&transactionid=Test
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchant_customer_id=Test&merchantid=Test&status=SUCCESS&transactionid=Test
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchant_customer_id=Test&merchantid=Test&status=SUCCESS&transactionid=Test
- *********************/notifications/relaunch?lang=fr
- *********************/account/recharges?lang=fr
- *********************/account/integration?lang=fr
- *********************/account?lang=fr
- *********************/notifications/relaunch?lang=en
- *********************/account/integration?lang=en
- *********************/account/profile?lang=fr
- *********************/account/transactions?lang=en&lang=fr
- *********************/account/transactions?lang=en&lang=fr
- *********************/account/transactions?lang=en&lang=fr
- *********************/account/transactions?lang=en&lang=fr
- *********************/account/profile?lang=en
- *********************/account/manage/role
- *********************/account/manage/role
- *********************/account/manage/role
- *********************/account/manage/role
- *********************/account/manage/user?lang=fr
- *********************/account/manage/user?lang=fr
- *********************/account/manage/user?lang=fr
- *********************/account/manage/user?lang=fr
- *********************/account/manage/user?lang=en
- *********************/account/manage/user?lang=en
- *********************/account/manage/user?lang=en
- *********************/account/manage/user?lang=en
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&type=Tout
- *********************/account/ticketing/nouveau
- *********************/account/transfer/bank?lang=en
- *********************/account/ticketing/liste?lang=fr

- *********************/account/transfer/bank/new
- *********************/account/ticketing/liste?lang=en
- *********************/notifications/relaunch?lang=en&lang=fr
- *********************/account/transactions/quick-search
- *********************/account/transactions/quick-search
- *********************/account/transactions/quick-search
- *********************/account/transactions/quick-search
- *********************/account/transactions/quick-search
- *********************/account/manage/role?lang=en
- *********************/account/manage/role?lang=en
- *********************/account/manage/role?lang=en
- *********************/account/manage/role?lang=en
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&lang=en&type=Tout
- *********************/account/manage/role?lang=fr
- *********************/account/manage/role?lang=fr
- *********************/account/manage/role?lang=fr
- *********************/account/manage/role?lang=fr
- *********************/account/manage/user?lang=en&lang=fr
- *********************/account/manage/user?lang=en&lang=fr
- *********************/account/manage/user?lang=en&lang=fr
- *********************/account/manage/user?lang=en&lang=fr
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&lang=fr&type=Tout
- *********************/account/transfer/bank?lang=en&lang=fr
- *********************/account/ticketing/nouveau?lang=en
- *********************/account/transfer/bank/new?lang=en
- *********************/account/ticketing/nouveau?lang=fr
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&type=All
- *********************/account/ticketing/liste?lang=en&lang=fr
- *********************/account/transactions/quick-search?lang=en
- *********************/account/transactions/quick-search?lang=en
- *********************/account/transactions/quick-search?lang=en
- *********************/account/transactions/quick-search?lang=en
- *********************/account/transactions/quick-search?lang=en
- *********************/account/transfer/bank/new?lang=fr

Severity: LOW

Vulnerability Id:CWE-829

Solutions

Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

References

Tags

- https://cwe.mitre.org/data/definitions/829.html
- https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/

9. Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

There are 94 instances of this issue:

- *********************/account/transactions
- *********************
- *********************/login
- *********************/account

- *********************/account/recharges
- *********************/account/transactions?lang=en
- *********************/notifications/relaunch
- *********************/account/transfer/bank
- *********************/account/integration
- *********************/account/profile
- *********************/account/transactions?lang=fr
- *********************/account/manage/user
- *********************/plugins/bootstrap-table/bootstrap-table.min.css
- *********************/plugins/jquery-date-range-picker/daterangepicker.min.css
- *********************/plugins/intl-tel-input/css/intlTelInput.min.css
- *********************/plugins/dzsparallaxer/dzsparallaxer.css
- *********************/plugins/slick-carousel/slick/slick.css
- *********************/images/favicon.png
- *********************/
- *********************/js/jquery.min.js
- *********************/js/bootstrap.bundle.min.js
- *********************/css/uikit.min.css
- *********************/css/theme.css
- *********************/js/hs.mask.js
- *********************/js/hs.core.js
- *********************/js/hs.quill.js
- *********************/js/hs.select2.js
- *********************/css/custom.css
- *********************/plugins/font-awesome/css/all.css
- *********************/js/hs.validation.js
- *********************/account/ticketing/liste
- *********************/demo
- *********************/js/sweetalert2.all.js
- *********************/plugins/bootstrap-table/locale/bootstrap-table-fr-FR.min.js
- *********************/images/merchant_default.png
- *********************/js/hs.fancybox.js
- *********************/images/logo.png
- *********************/plugins/jquery-date-range-picker/jquery.daterangepicker.min.js
- *********************/plugins/intl-tel-input/js/intlTelInput.min.js
- *********************/plugins/jquery-date-range-picker/moment.min.js
- *********************/plugins/slick-carousel/slick/slick.js
- *********************/plugins/bootstrap-table/extensions/export/bootstrap-table-export.min.js
- *********************/plugins/bootstrap-table/extensions/print/bootstrap-table-print.min.js
- *********************/js/uikit-icons.js
- *********************/js/uikit.min.js
- *********************/plugins/bootstrap-table/bootstrap-table.min.js
- *********************/js/hs.slick-carousel.js
- *********************/account/recharges/new
- *********************/account/recharges?df=2024-12-09&dt=2024-12-09
- *********************/account/recharges?lang=en
- *********************/account?lang=en
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchant_customer_id=Test&merchantid=Test&status=SUCCESS&transactionid=Test
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchantid=Test&status=SUCCESS&transactionid=Test&type=payments
- *********************/replay-notification-model.xlsx
- *********************/notifications/relaunch?lang=fr
- *********************/account/recharges?lang=fr

- *********************/account?lang=fr
- *********************/account/integration?lang=fr
- *********************/notifications/relaunch?lang=en
- *********************/account/integration?lang=en
- *********************/images/flyers.jpg
- *********************/js/phone.js
- *********************/css/select2.min.css
- *********************/account/profile?lang=fr
- *********************/account/profile?lang=en
- *********************/account/transactions?lang=en&lang=fr
- *********************/account/manage/role
- *********************/account/manage/user?lang=fr
- *********************/account/manage/user?lang=en
- *********************/account/updatePassword
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&type=Tout
- *********************/account/ticketing/nouveau
- *********************/account/ticketing/liste?lang=fr
- *********************/account/transfer/bank/new
- *********************/account/transfer/bank?lang=en
- *********************/account/manage/role/store
- *********************/account/transactions/quick-search
- *********************/notifications/relaunch?lang=en&lang=fr
- *********************/account/ticketing/liste?lang=en
- *********************/account/manage/role?lang=en
- *********************/account/manage/user/create
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&lang=en&type=Tout
- *********************/account/manage/role?lang=fr
- *********************/account/manage/user?lang=en&lang=fr
- *********************/account/ticketing/store
- *********************/account/transfer/bank?lang=en&lang=fr
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&lang=fr&type=Tout
- *********************/account/transfer/bank/new?lang=en
- *********************/account/ticketing/nouveau?lang=en
- *********************/account/transfer/bank
- *********************/account/ticketing/nouveau?lang=fr
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&type=All
- *********************/account/ticketing/liste?lang=en&lang=fr
- *********************/account/transactions/quick-search?lang=en

Severity: LOW

Vulnerability Id:CWE-200

Solutions

Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.

References

- https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework
- https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

Tags

- https://cwe.mitre.org/data/definitions/200.html
- https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html
- https://owasp.org/Top10/A01_2021-Broken_Access_Control/

- https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework

10. X-Content-Type-Options Header Missing

There are 86 instances of this issue:

- *********************/account/transactions
- *********************/account
- *********************/account/recharges
- *********************/account/transactions?lang=en
- *********************/notifications/relaunch
- *********************/account/transfer/bank
- *********************/account/integration
- *********************/account/profile
- *********************/account/transactions?lang=fr
- *********************/account/manage/user
- *********************/plugins/bootstrap-table/bootstrap-table.min.css
- *********************/plugins/intl-tel-input/css/intlTelInput.min.css
- *********************/plugins/jquery-date-range-picker/daterangepicker.min.css
- *********************/plugins/dzsparallaxer/dzsparallaxer.css
- *********************/plugins/slick-carousel/slick/slick.css
- *********************/images/favicon.png
- *********************/js/jquery.min.js
- *********************/js/bootstrap.bundle.min.js
- *********************/css/uikit.min.css
- *********************/css/theme.css
- *********************/js/hs.mask.js
- *********************/js/hs.core.js
- *********************/js/hs.quill.js
- *********************/js/hs.select2.js
- *********************/css/custom.css
- *********************/js/hs.validation.js
- *********************/plugins/font-awesome/css/all.css
- *********************/account/ticketing/liste
- *********************/demo
- *********************/js/sweetalert2.all.js
- *********************/plugins/bootstrap-table/locale/bootstrap-table-fr-FR.min.js
- *********************/images/merchant_default.png
- *********************/js/hs.fancybox.js
- *********************/images/logo.png
- *********************/plugins/jquery-date-range-picker/jquery.daterangepicker.min.js
- *********************/plugins/intl-tel-input/js/intlTelInput.min.js
- *********************/plugins/jquery-date-range-picker/moment.min.js
- *********************/plugins/slick-carousel/slick/slick.js
- *********************/plugins/bootstrap-table/extensions/export/bootstrap-table-export.min.js
- *********************/plugins/bootstrap-table/extensions/print/bootstrap-table-print.min.js
- *********************/js/uikit-icons.js
- *********************/js/uikit.min.js
- *********************/plugins/bootstrap-table/bootstrap-table.min.js
- *********************/js/hs.slick-carousel.js
- *********************/account/recharges/new
- *********************/account/recharges?df=2024-12-09&dt=2024-12-09
- *********************/account/recharges?lang=en
- *********************/account?lang=en

- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchant_customer_id=Test&merchantid=Test&status=SUCCESS&transactionid=Test
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchantid=Test&status=SUCCESS&transactionid=Test&type=payments
- *********************/replay-notification-model.xlsx
- *********************/notifications/relaunch?lang=fr
- *********************/account/recharges?lang=fr
- *********************/account?lang=fr
- *********************/account/integration?lang=fr
- *********************/notifications/relaunch?lang=en
- *********************/account/integration?lang=en
- *********************/images/flyers.jpg
- *********************/js/phone.js
- *********************/css/select2.min.css
- *********************/account/profile?lang=fr
- *********************/account/profile?lang=en
- *********************/account/transactions?lang=en&lang=fr
- *********************/account/manage/role
- *********************/account/manage/user?lang=fr
- *********************/account/manage/user?lang=en
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&type=Tout
- *********************/account/ticketing/nouveau
- *********************/account/ticketing/liste?lang=fr
- *********************/account/transfer/bank/new
- *********************/account/transfer/bank?lang=en
- *********************/notifications/relaunch?lang=en&lang=fr
- *********************/account/ticketing/liste?lang=en
- *********************/account/transactions/quick-search
- *********************/account/manage/role?lang=en
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&lang=en&type=Tout
- *********************/account/manage/role?lang=fr
- *********************/account/manage/user?lang=en&lang=fr
- *********************/account/transfer/bank?lang=en&lang=fr
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&lang=fr&type=Tout
- *********************/account/transfer/bank/new?lang=en
- *********************/account/ticketing/nouveau?lang=en
- *********************/account/ticketing/nouveau?lang=fr
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&type=All
- *********************/account/ticketing/liste?lang=en&lang=fr
- *********************/account/transactions/quick-search?lang=en

Severity: LOW

Vulnerability Id:CWE-693

Solutions

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.

References

- 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

Tags

- https://cwe.mitre.org/data/definitions/693.html
- https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html
- https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

11. Cookie No HttpOnly Flag

There are 61 instances of this issue:

- *********************/account/transactions
- *********************
- *********************/login
- *********************/account
- *********************/account/recharges
- *********************/account/transactions?lang=en
- *********************/notifications/relaunch
- *********************/account/integration
- *********************/account/transfer/bank
- *********************/account/profile
- *********************/account/transactions?lang=fr
- *********************/account/manage/user
- *********************/
- *********************/demo
- *********************/account/ticketing/liste
- *********************/account/recharges/new
- *********************/account/recharges?lang=en
- *********************/account/recharges?df=2024-12-09&dt=2024-12-09
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchantid=Test&status=SUCCESS&transactionid=Test&type=payments
- *********************/account?lang=en
- *********************/account/transactions?df=2024-12-09&dt=2024-12-09&merchant_customer_id=Test&merchantid=Test&status=SUCCESS&transactionid=Test
- *********************/notifications/relaunch
- *********************/notifications/relaunch?lang=fr
- *********************/account/recharges?lang=fr
- *********************/account/integration?lang=fr
- *********************/account?lang=fr
- *********************/notifications/relaunch?lang=en
- *********************/account/integration?lang=en
- *********************/account/profile?lang=fr
- *********************/account/transactions?lang=en&lang=fr
- *********************/account/profile?lang=en
- *********************/account/manage/role
- *********************/account/manage/user?lang=fr
- *********************/account/manage/user?lang=en
- *********************/account/updatePassword
- *********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&type=Tout
- *********************/account/ticketing/nouveau
- *********************/account/transfer/bank?lang=en
- *********************/account/ticketing/liste?lang=fr
- *********************/account/transfer/bank/new
- *********************/account/manage/role/store
- *********************/account/transactions/quick-search
- *********************/notifications/relaunch?lang=en&lang=fr

- ********************/account/ticketing/liste?lang=en
- ********************/account/manage/role?lang=en
- ********************/account/manage/user/create
- ********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&lang=en&type=Tout
- ********************/account/manage/role?lang=fr
- ********************/account/manage/user?lang=en&lang=fr
- ********************/account/ticketing/store
- ********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&lang=fr&type=Tout
- ********************/account/ticketing/nouveau?lang=en
- ********************/account/transfer/bank?lang=en&lang=fr
- ********************/account/transfer/bank/new?lang=en
- ********************/account/ticketing/nouveau?lang=fr
- ********************/account/transfer/bank?df=2024-12-09&dt=2024-12-09&type=All
- ********************/account/ticketing/liste?lang=en&lang=fr
- ********************/account/transfer/bank
- ********************/account/transactions/quick-search?lang=en
- ********************/account/transfer/bank/new?lang=fr
- ********************/account/transactions/quick-search?lang=fr

Severity: LOW

Vulnerability Id:CWE-1004

Solutions

Ensure that the HttpOnly flag is set for all cookies.

References

- https://owasp.org/www-community/HttpOnly

Tags

- https://cwe.mitre.org/data/definitions/1004.html
- https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html
- https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
- https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes

12. Big Redirect Detected (Potential Sensitive Information Leak)

There are 10 instances of this issue:

- ********************
- ********************/login
- ********************/
- ********************/account/updatePassword
- ********************/account/manage/role/store
- ********************/account/transactions/quick-search
- ********************/account/manage/user/create
- ********************/account/manage/user/create
- ********************/account/ticketing/store
- ********************/account/transfer/bank

Severity: LOW

Vulnerability Id:CWE-201

Solutions

Ensure that no sensitive information is leaked via redirect responses. Redirect responses should have almost no content.

References

Tags

- https://cwe.mitre.org/data/definitions/201.html
- https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html
- https://owasp.org/Top10/A04_2021-Insecure_Design/
- https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage

13. Application Error Disclosure

There are 1 instances of this issue:

- *********************/notifications/relaunch

Severity: LOW

Vulnerability Id:CWE-200

Solutions

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.

References

Tags

- https://cwe.mitre.org/data/definitions/200.html
- https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html
- https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
- https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/08-Testing_for_Error_Handling/01-Testing_For_Improper_Error_Handling
- https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/08-Testing_for_Error_Handling/02-Testing_for_Stack_Traces