

Aggregated Scan Result

Vulnerability Scan Results

Summary

Overall risk level:**Low****Risk ratings:**High: **0**Medium: **0**Low: **5**Info: **39****Scan information:**

This is an aggregated report from 3 scans.

Start time: Oct 20, 2023 / 09:03:06

Finish time: Oct 20, 2023 / 09:05:48

Findings (by target)

1. Target: <https://conductionnl.github.io/woo-website-xxlInc> - Demo omgeving voor OpenWOO APP

🚩 Missing security header: X-Content-Type-Options OPEN

CONFIRMED

URL	Evidence
https://conductionnl.github.io/woo-website-xxlInc	Response headers do not include the X-Content-Type-Options HTTP security header

▼ Details**Risk description:**

The HTTP header **X-Content-Type-Options** is addressed to the Internet Explorer browser and prevents it from reinterpreting the content of a web page (MIME-sniffing) and thus overriding the value of the Content-Type header). Lack of this header could lead to attacks such as Cross-Site Scripting or phishing.

Recommendation:

We recommend setting the X-Content-Type-Options header such as **X-Content-Type-Options: nosniff**.

References:

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options>

Classification:

CWE : [CWE-693](#)

OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

🚩 Missing security header: Content-Security-Policy OPEN

CONFIRMED

URL	Evidence
https://conductionnl.github.io/woo-website-xxlInc	Response headers do not include the HTTP Content-Security-Policy security header

▼ Details**Risk description:**

The Content-Security-Policy (CSP) header activates a protection mechanism implemented in web browsers which prevents exploitation of Cross-Site Scripting vulnerabilities (XSS). If the target application is vulnerable to XSS, lack of this header makes it easily exploitable by attackers.

Recommendation:

Configure the Content-Security-Header to be sent with each HTTP response in order to apply the specific policies needed by the application.

References:

https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy>

Classification:

CWE : [CWE-693](#)

OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

Missing security header: X-Frame-Options

[OPEN](#)**CONFIRMED**

URL	Evidence
https://conductionnl.github.io/woo-website-xxlnc	Response headers do not include the HTTP X-Frame-Options security header

Details**Risk description:**

Because the **X-Frame-Options** header is not sent by the server, an attacker could embed this website into an iframe of a third party website. By manipulating the display attributes of the iframe, the attacker could trick the user into performing mouse clicks in the application, thus performing activities without user consent (ex: delete user, subscribe to newsletter, etc). This is called a Clickjacking attack and it is described in detail here:

<https://owasp.org/www-community/attacks/Clickjacking>

Recommendation:

We recommend you to add the **X-Frame-Options** HTTP header with the values **DENY** or **SAMEORIGIN** to every page that you want to be protected against Clickjacking attacks.

References:

https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

Classification:

CWE : [CWE-693](#)

OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

Missing security header: Referrer-Policy

[OPEN](#)**CONFIRMED**

URL	Evidence
https://conductionnl.github.io/woo-website-xxlnc	Response headers do not include the Referrer-Policy HTTP security header as well as the <meta> tag with name 'referrer' is not present in the response.

Details**Risk description:**

The Referrer-Policy HTTP header controls how much referrer information the browser will send with each request originated from the current web application.

For instance, if a user visits the web page "http://example.com/pricing/" and it clicks on a link from that page going to e.g. "https://www.google.com", the browser will send to Google the full originating URL in the **Referer** header, assuming the Referrer-Policy header is not set. The originating URL could be considered sensitive information and it could be used for user tracking.

Recommendation:

The Referrer-Policy header should be configured on the server side to avoid user tracking and inadvertent information leakage. The value **no-referrer** of this header instructs the browser to omit the Referer header entirely.

References:









https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns

Classification:

CWE : [CWE-693](#)

OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

Software / Version	Category
Fastly	CDN
 Webpack	Miscellaneous
 Module Federation	Miscellaneous
 Varnish	Caching
 React	JavaScript frameworks
 Gatsby 4.25.7	Static site generator, JavaScript frameworks
 GitHub Pages	PaaS
 HSTS	Security
 DigiCert	SSL/TLS certificate authorities

▼ Details

Risk description:

An attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:

We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

References:

https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html

Classification:

OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

Screenshot:

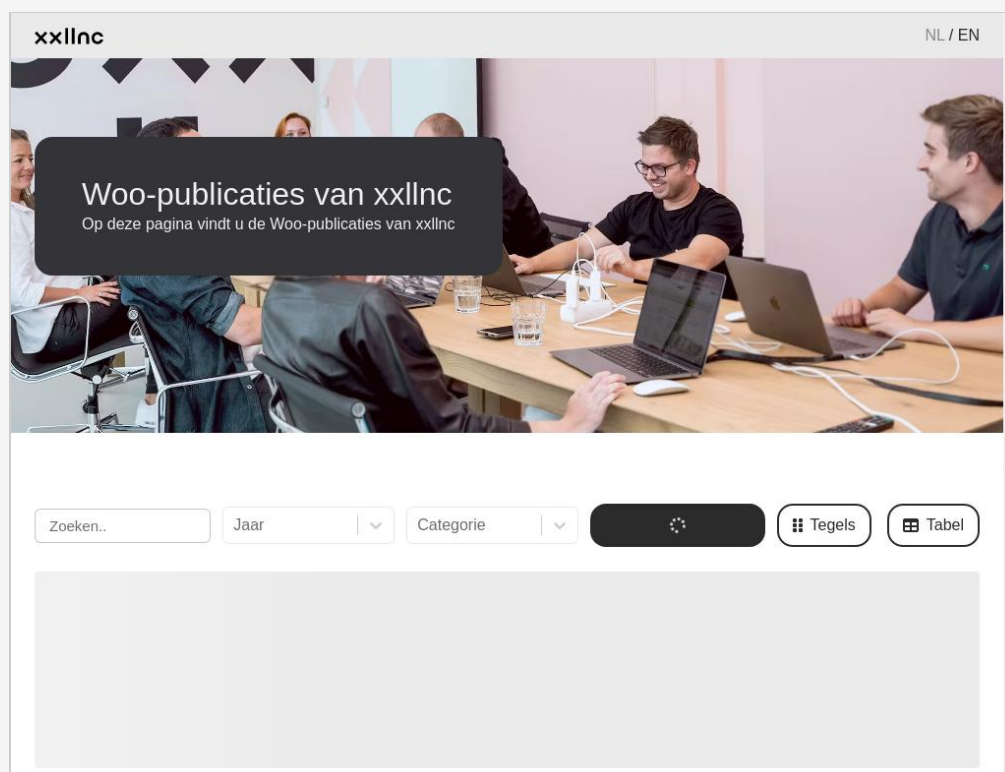


Figure 1. Website Screenshot

🚩 Website is accessible. [OPEN](#)

🚩 Spider results [OPEN](#)

URL	Method	Parameters
https://conductionnl.github.io/woo-website-xxllnc	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36

▼ Details

Risk description:

The table contains all the unique pages the scanner found. The duplicated URLs are not available here as scanning those is considered unnecessary

Recommendation:

We recommend to advanced users to make sure the scan properly detected most of the URLs in the application.

References:

[All the URLs the scanner found, including duplicates](#) (available for 90 days after the scan date)

🚩 Nothing was found for vulnerabilities of server-side software. [OPEN](#)

🚩 Nothing was found for client access policies. [OPEN](#)

🚩 Nothing was found for robots.txt file. [OPEN](#)

🚩 Nothing was found for outdated JavaScript libraries. [OPEN](#)

🚩 Nothing was found for use of untrusted certificates. [OPEN](#)

🚩 Nothing was found for enabled HTTP debug methods. [OPEN](#)

🚩 Nothing was found for secure communication. [OPEN](#)

🚩 Nothing was found for directory listing. [OPEN](#)

🚩 Nothing was found for passwords submitted unencrypted. [OPEN](#)

🚩 Nothing was found for Cross-Site Scripting. [OPEN](#)

🚩 Nothing was found for SQL Injection. [OPEN](#)

🚩 Nothing was found for Local File Inclusion. [OPEN](#)

🚩 Nothing was found for OS Command Injection. [OPEN](#)

🚩 Nothing was found for error messages. [OPEN](#)

🚩 Nothing was found for debug messages. [OPEN](#)

🚩 Nothing was found for code comments. [OPEN](#)

🚩 Nothing was found for missing HTTP header - Strict-Transport-Security. [OPEN](#)

🚩 Nothing was found for domain too loose set for cookies. [OPEN](#)

🚩 Nothing was found for mixed content between HTTP and HTTPS. [OPEN](#)

🚩 Nothing was found for cross domain file inclusion. [OPEN](#)

🚩 Nothing was found for internal error code. [OPEN](#)

🚩 Nothing was found for HttpOnly flag of cookie. [OPEN](#)

🚩 Nothing was found for Secure flag of cookie. [OPEN](#)

🚩 Nothing was found for login interfaces. [OPEN](#)

🚩 Nothing was found for secure password submission. [OPEN](#)

🚩 Nothing was found for sensitive data. [OPEN](#)

🚩 Nothing was found for Server Side Request Forgery. [OPEN](#)

🚩 Nothing was found for Open Redirect. [OPEN](#)

🚩 Nothing was found for PHP Code Injection. [OPEN](#)

🚩 Nothing was found for JavaScript Code Injection. [OPEN](#)

🚩 Nothing was found for unsafe HTTP header Content Security Policy. [OPEN](#)

🚩 Website is accessible. [OPEN](#)

🚩 Spider results [OPEN](#)

URL	Method	Parameters
https://conductionnl.github.io/woo-website-xxlnc/	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
https://conductionnl.github.io/woo-website-xxlnc/	GET	Query: _search= Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
https://conductionnl.github.io/woo-website-xxlnc/page-data/app-data.json	GET	Headers: Referer= https://conductionnl.github.io/woo-website-xxlnc/ User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
https://conductionnl.github.io/woo-website-xxlnc/page-data/index/page-data.json	GET	Query: _search= Headers: referer= https://conductionnl.github.io/woo-website-xxlnc/?_search= user-agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
https://conductionnl.github.io/woo-website-xxlnc/page-data/quot;https://uploads.magnetme-images.com/bf3b2064d7a7c8a51b2c66608b62160f01ee478ab2df8a493635c92069405d35/page-data.json	GET	Query: amp:auto=format amp;fit=crop amp:frame=0 amp;h=1125 amp;w=2000 auto=compress quot;= Headers: user-agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
https://conductionnl.github.io/woo-website-xxlnc/quot;https://	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36

https://conductionnl.github.io/woo-website-xxlnc/quot;https/uploads.magnetme-images.com/bf3b2064d7a7c8a51b2c66608b62160f01ee478ab2df8a493635c92069405d35	GET	Query: amp:auto=format amp;fit=crop amp;frame=0 amp;h=1125 amp;w=2000 auto=compress quot;= Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
https://conductionnl.github.io/woo-website-xxlnc/woo-website-xxlnc/static/	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
https://conductionnl.github.io/woo-website-xxlnc/woo-website-xxlnc/static/woo-website-xxlnc	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
https://conductionnl.github.io/woo-website-xxlnc/woo-website-xxlnc/static	GET	Headers: user-agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
https://conductionnl.github.io/woo-website-xxlnc/woo-website-xxlnc/woo-website-xxlnc	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
https://conductionnl.github.io/woo-website-xxlnc	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36

▼ Details

Risk description:

The table contains all the unique pages the scanner found. The duplicated URLs are not available here as scanning those is considered unnecessary

Recommendation:

We recommend to advanced users to make sure the scan properly detected most of the URLs in the application.

References:

[All the URLs the scanner found, including duplicates](#) (available for 90 days after the scan date)

🚩 Nothing was found for Cross-Site Scripting. [OPEN](#)

🚩 Website is accessible. [OPEN](#)

🚩 Spider results [OPEN](#)

URL	Method	Parameters
-----	--------	------------

https://conductionnl.github.io/woo-website-xxlnc/page-data/app-data.json	GET	Headers: Referer=https://conductionnl.github.io/woo-website-xxlnc/ User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
https://conductionnl.github.io/woo-website-xxlnc/woo-website-xxlnc/static/	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
https://conductionnl.github.io/woo-website-xxlnc/woo-website-xxlnc/static/woo-website-xxlnc/	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
https://conductionnl.github.io/woo-website-xxlnc/woo-website-xxlnc/static	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
https://conductionnl.github.io/woo-website-xxlnc	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36

▼ Details

Risk description:

The table contains all the unique pages the scanner found. The duplicated URLs are not available here as scanning those is considered unnecessary

Recommendation:

We recommend to advanced users to make sure the scan properly detected most of the URLs in the application.

References:

[All the URLs the scanner found, including duplicates](#) (available for 90 days after the scan date)

🚩 Nothing was found for SQL Injection. [OPEN](#)

Tool configuration details

The following tools were run to obtain the findings above:

Website Vulnerability Scanner

Scan parameters

Target https://conductionnl.github.io/woo-website-xxlInc
Scan type Ptt_engine
Authentication False

Scan information

Start time: Oct 20, 2023 / 09:03:09
Finish time: Oct 20, 2023 / 09:04:38
Scan duration: 1 min, 29 sec
Tests performed: 38/38
Scan status: Finished

XSS Scanner

Scan parameters

Target https://conductionnl.github.io/woo-website-xxlInc
Scan type Deep
Authentication False

Scan information

Start time: Oct 20, 2023 / 09:03:06
Finish time: Oct 20, 2023 / 09:05:12
Scan duration: 2 min, 6 sec
Tests performed: 3/3
Scan status: Finished

SQL Injection Scanner

Scan parameters

Target https://conductionnl.github.io/woo-website-xxlInc
Scan type Deep
Authentication False

Scan information

Start time: Oct 20, 2023 / 09:04:43
Finish time: Oct 20, 2023 / 09:05:48
Scan duration: 1 min, 5 sec
Tests performed: 3/3
Scan status: Finished