Website Vulnerability Scanner Report (Light)

Unlock the full capabilities of this scanner

See what the DEEP scanner can do

Perform in-depth website scanning and discover high risk vulnerabilities.

Testing areas	Light scan	Deep scan
Website fingerprinting	✔	✔
Version-based vulnerability detection	✔	✔
Common configuration issues	✔	✔
SQL injection	–	✔
Cross-Site Scripting	–	✔
Local/Remote File Inclusion	–	✔
Remote command execution	–	✔
Discovery of sensitive files	–	✔

✔ **https://kamarleyj.co.uk/**

Target added due to a redirect from https://kamarleyj.co.uk

The Light Website Scanner didn't check for critical issues like SQLi, XSS, Command Injection, XXE, etc.
Upgrade to run Deep scans with 40+ tests and detect more vulnerabilities.

Summary

Overall risk level:

Low

Risk ratings:

Critical:	0
High:	0
Medium:	0
Low:	5
Info:	34

Scan information:

Start time:	Jan 19, 2026 / 04:21:35 UTC+02
Finish time:	Jan 19, 2026 / 04:22:04 UTC+02
Scan duration:	29 sec
Tests performed:	39/39
Scan status:	Finished

Findings

Missing security header: Referrer-Policy

CONFIRMED

port 443/tcp

URL	Evidence
https://kamarleyj.co.uk/	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. Request / Response

Details

Risk description:

The risk is that if a user visits a web page (e.g. "http://example.com/pricing/") and 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 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Unsafe security header: Content-Security-Policy

CONFIRMED

port 443/tcp

URL	Evidence

https://kamarleyj.co.uk/	Response headers include the HTTP Content-Security-Policy security header with the following security issues:
	`script-src: 'self' can be problematic if you host JSONP, Angular or user uploaded files.`
	`script-src: ''unsafe-inline'' allows the execution of unsafe in-page scripts and event handlers.`
	Request / Response

Details

Risk description:

For example, if the unsafe-inline directive is present in the CSP header, the execution of inline scripts and event handlers is allowed. This can be exploited by an attacker to execute arbitrary JavaScript code in the context of the vulnerable application.

Recommendation:

Remove the unsafe values from the directives, adopt nonces or hashes for safer inclusion of inline scripts if they are needed, and explicitly define the sources from which scripts, styles, images or other resources can be loaded.

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 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Missing security header: X-Content-Type-Options

CONFIRMED

port 443/tcp

URL	Evidence
https://kamarleyj.co.uk/	Response headers do not include the X-Content-Type-Options HTTP security header Request / Response

Details

Risk description:

The risk is that lack of this header could make possible attacks such as Cross-Site Scripting or phishing in Internet Explorer browsers.

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 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Robots.txt file found

port 443/tcp

CONFIRMED

URL
https://kamarleyj.co.uk/robots.txt

Details

Risk description:
There is no particular security risk in having a robots.txt file. However, it's important to note that adding endpoints in it should not be considered a security measure, as this file can be directly accessed and read by anyone.

Recommendation:
We recommend you to manually review the entries from robots.txt and remove the ones which lead to sensitive locations in the website (ex. administration panels, configuration files, etc).

References:
https://www.theregister.co.uk/2015/05/19/robotstxt/

Classification:
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Server software and technology found

port 443/tcp

UNCONFIRMED

Software / Version	Category
Lenis 1.3.17	JavaScript libraries
Astro 5.16.6	Static site generator, JavaScript frameworks
Google Analytics	Analytics
Google Font API	Font scripts
GSAP	JavaScript frameworks
HTTP/3	Miscellaneous
Nginx	Web servers, Reverse proxies
Open Graph	Miscellaneous
PHP	Programming languages
Three.js 182	JavaScript graphics
Cloudflare Turnstile	Security
Google Tag Manager	Tag managers
HSTS	Security
Zabbix	Miscellaneous

Details

Risk description:
The risk is that 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 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Security.txt file is missing

CONFIRMED

port 443/tcp

URL
Missing: https://kamarleyj.co.uk/.well-known/security.txt

Details

Risk description:
There is no particular risk in not having a security.txt file for your server. However, this file is important because it offers a designated channel for reporting vulnerabilities and security issues.

Recommendation:
We recommend you to implement the security.txt file according to the standard, in order to allow researchers or users report any security issues they find, improving the defensive mechanisms of your server.

References:
https://securitytxt.org/

Classification:
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

CONFIRMED

Nothing was found for vulnerabilities of server-side software.

Nothing was found for client access policies.

Nothing was found for use of untrusted certificates.

Nothing was found for enabled HTTP debug methods.

Nothing was found for enabled HTTP OPTIONS method.

Nothing was found for secure communication.

Nothing was found for directory listing.

Nothing was found for passwords submitted unencrypted.

Nothing was found for error messages.

Nothing was found for debug messages.

- Nothing was found for code comments.
- Nothing was found for missing HTTP header - Strict-Transport-Security.
- Nothing was found for missing HTTP header - Content Security Policy.
- Nothing was found for passwords submitted in URLs.
- Nothing was found for domain too loose set for cookies.
- Nothing was found for mixed content between HTTP and HTTPS.
- Nothing was found for cross domain file inclusion.
- Nothing was found for internal error code.
- Nothing was found for HttpOnly flag of cookie.
- Nothing was found for Secure flag of cookie.
- Nothing was found for login interfaces.
- Nothing was found for secure password submission.
- Nothing was found for sensitive data.
- Nothing was found for OpenAPI files.
- Nothing was found for file upload.
- Nothing was found for SQL statement in request parameter.
- Nothing was found for password returned in later response.
- Nothing was found for Path Disclosure.
- Nothing was found for Session Token in URL.

Nothing was found for API endpoints.

Nothing was found for emails.

Nothing was found for missing HTTP header - Rate Limit.

Scan coverage information

List of tests performed (39/39)

- Test connection
- Scanned for missing HTTP header - Referrer
- Scanned for unsafe HTTP header Content Security Policy
- Scanned for missing HTTP header - X-Content-Type-Options
- Scanned for website technologies
- Scanned for version-based vulnerabilities of server-side software
- Scanned for client access policies
- Scanned for robots.txt file
- Scanned for absence of the security.txt file
- Scanned for use of untrusted certificates
- Scanned for enabled HTTP debug methods
- Scanned for enabled HTTP OPTIONS method
- Scanned for secure communication
- Scanned for directory listing
- Scanned for passwords submitted unencrypted
- Scanned for error messages
- Scanned for debug messages
- Scanned for code comments
- Scanned for missing HTTP header - Strict-Transport-Security
- Scanned for missing HTTP header - Content Security Policy
- Scanned for passwords submitted in URLs
- Scanned for domain too loose set for cookies
- Scanned for mixed content between HTTP and HTTPS
- Scanned for cross domain file inclusion
- Scanned for internal error code
- Scanned for HttpOnly flag of cookie
- Scanned for Secure flag of cookie
- Scanned for login interfaces
- Scanned for secure password submission
- Scanned for sensitive data
- Scanned for OpenAPI files
- Scanned for file upload
- Scanned for SQL statement in request parameter
- Scanned for password returned in later response
- Scanned for Path Disclosure
- Scanned for Session Token in URL
- Scanned for API endpoints
- Scanned for emails
- Scanned for missing HTTP header - Rate Limit

Scan parameters

target:	https://kamarleyj.co.uk/
scan_type:	Light
authentication:	False

Scan stats

Unique Injection Points Detected:	3
URLs spidered:	7
Total number of HTTP requests:	21
Average time until a response was received:	146ms