Pentest Tools

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://stamet-samarinda.devbmkg.my.id/**

Target added due to a redirect from https://stamet-samarinda.devbmkg.my.id

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:	3
Info:	35

Scan information:

Start time:	Feb 19, 2026 / 06:00:02 UTC+02
Finish time:	Feb 19, 2026 / 06:00:32 UTC+02
Scan duration:	30 sec
Tests performed:	38/38
Scan status:	Finished

Findings

Unsafe security header: Content-Security-Policy

CONFIRMED

port 443/tcp

URL	Evidence

<table>
<tr><td>https://stamet-samarinda.devbmkg.my.id/</td><td>Response headers include the HTTP Content-Security-Policy security header with the following security issues:
<pre>
script-src: 'unsafe-eval' allows the execution of code injected into DOM APIs such as eval().
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.
object-src: We recommend restricting object-src to 'none'.
base-uri: Missing base-uri allows the injection of base tags. They can be used to set the base URL for
all relative (script) URLs to an attacker controlled domain. We recommend setting it to 'none' or 'self'
.
</pre>
Request / Response</td></tr>
</table>

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

Robots.txt file found

CONFIRMED

port 443/tcp

URL
https://stamet-samarinda.devbmkg.my.id/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

UNCONFIRMED

port 443/tcp

Software / Version	Category
HTTP/3	Miscellaneous
Lucide	Font scripts
Google Maps	Maps
Next.js 15.5.7	JavaScript frameworks, Web frameworks, Web servers, Static site generator
Open Graph	Miscellaneous

React	JavaScript frameworks
Supabase	Development
Webpack	Miscellaneous
Priority Hints	Performance
Cloudflare	CDN
PostgreSQL	Databases
HSTS	Security

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

port 443/tcp

CONFIRMED

URL
Missing: https://stamet-samarinda.devbmkg.my.id/.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

HTTP OPTIONS enabled

port 443/tcp

CONFIRMED

URL	Method	Summary
https://stamet-samarinda.devbmkg.my.id/	OPTIONS	We did a HTTP OPTIONS request. The server responded with a 405 status code and the header: `Allow: GET, HEAD` Request / Response

Details

Risk description:

The only risk this might present nowadays is revealing debug HTTP methods that can be used on the server. This can present a danger if any of those methods can lead to sensitive information, like authentication information, secret keys.

Recommendation:
We recommend that you check for unused HTTP methods or even better, disable the OPTIONS method. This can be done using your webserver configuration.

References:
https://techcommunity.microsoft.com/t5/iis-support-blog/http-options-and-default-page-vulnerabilities/ba-p/1504845
https://docs.nginx.com/nginx-management-suite/acm/how-to/policies/allowed-http-methods/

Classification:
CWE : CWE-16
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

⚑ Email Address Exposure

port 443/tcp

UNCONFIRMED

URL	Method	Parameters	Evidence
https://stamet-samarinda.devbmkg.my.id/	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	Email Address: stamet.samarinda@bmkg.go.id Request / Response

Details

Risk description:
The risk is that exposed email addresses within the application could be accessed by unauthorized parties. This could lead to privacy violations, spam, phishing attacks, or other forms of misuse.

Recommendation:
Compartmentalize the application to have 'safe' areas where trust boundaries can be unambiguously drawn. Do not allow email addresses to go outside of the trust boundary, and always be careful when interfacing with a compartment outside of the safe area.

References:
https://owasp.org/Top10/A04_2021-Insecure_Design/

Classification:
CISA KEV: False
CVE : -1
CWE : CWE-200
OWASP Top 10 - 2017 : A6: Security Misconfiguration
OWASP Top 10 - 2021 : A4: Insecure Design

⚑ 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 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 missing HTTP header - X-Content-Type-Options.

Nothing was found for missing HTTP header - Referrer.

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 missing HTTP header - Rate Limit.

Scan coverage information

List of tests performed (38/38)

- ✓ Scanned for emails
- ✓ Scanned for unsafe HTTP header Content Security Policy
- ✓ 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 missing HTTP header - X-Content-Type-Options
- ✓ Scanned for missing HTTP header - Referrer
- ✓ 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 missing HTTP header - Rate Limit

Scan parameters

target:	https://stamet-samarinda.devbmkg.my.id/
scan_type:	Light
authentication:	False

Scan stats

Unique Injection Points Detected:	67
URLs spidered:	21
Total number of HTTP requests:	35
Average time until a response was received:	262ms