Pentest Tools

Website Vulnerability Scanner Report

✓ **https://fontein-si-umkm-1-3.vercel.app/**

⚠ 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:

Medium

Risk ratings:

High:	0
Medium:	1
Low:	4
Info:	14

Scan information:

Start time:	Jul 17, 2024 / 11:47:41
Finish time:	Jul 17, 2024 / 11:48:06
Scan duration:	25 sec
Tests performed:	19/19
Scan status:	Finished

Findings

🚩 Insecure cookie setting: missing Secure flag   CONFIRMED

URL	Cookie Name	Evidence
https://fontein-si-umkm-1-3.vercel.app/	fontein	Set-Cookie: fontein=s%3AWW0r96VwgqM1Usyg5bYRi91SiOueRP0V.zbi9cHyM0Alb5THUouFt85tM8wqn41eUJcYFyYntN2k; Path=/; HttpOnly Request / Response

⌄ Details

Risk description:
The risk exists that an attacker will intercept the clear-text communication between the browser and the server and he will steal the cookie of the user. If this is a session cookie, the attacker could gain unauthorized access to the victim's web session.

Recommendation:
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/stable/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html

Classification:
CWE : CWE-614
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

🚩 Missing security header: Referrer-Policy   CONFIRMED

URL	Evidence
https://fontein-si-umkm-1-3.vercel.app/	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

🚩 Missing security header: Content-Security-Policy   CONFIRMED

URL	Evidence
https://fontein-si-umkm-1-3.vercel.app/	Response does not include the HTTP Content-Security-Policy security header or meta tag Request / Response

❯ Details

Risk description:

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

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

URL	Evidence
https://fontein-si-umkm-1-3.vercel.app/	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

🚩 Server software and technology found   UNCONFIRMED ⓘ

Software / Version	Category
ex Express	Web frameworks, Web servers
Node.js	Programming languages
Cloudflare	CDN
cdnjs	CDN
jQuery CDN	CDN
Font Awesome	Font scripts
Bootstrap 5.3.3	UI frameworks
jQuery 3.6.0	JavaScript libraries
Vercel	PaaS
jsDelivr	CDN
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   CONFIRMED

URL
Missing: https://fontein-si-umkm-1-3.vercel.app/.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   CONFIRMED

URL	Method	Summary

https://fontein-si-umkm-1-3.vercel.app/	OPTIONS	We did a HTTP OPTIONS request. The server responded with a 200 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

🚩 Website is accessible.

🚩 Nothing was found for vulnerabilities of server-side software.

🚩 Nothing was found for client access policies.

🚩 Nothing was found for robots.txt file.

🚩 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 missing HTTP header - Strict-Transport-Security.

🚩 Nothing was found for domain too loose set for cookies.

🚩 Nothing was found for HttpOnly flag of cookie.

🚩 Nothing was found for unsafe HTTP header Content Security Policy.

Scan coverage information

List of tests performed (19/19)

- ✔ Starting the scan...
- ✔ Checking for Secure flag of cookie...
- ✔ Checking for missing HTTP header - Referrer...
- ✔ Checking for missing HTTP header - Content Security Policy...
- ✔ Checking for missing HTTP header - X-Content-Type-Options...
- ✔ Checking for website technologies...
- ✔ Checking for vulnerabilities of server-side software...
- ✔ Checking for client access policies...
- ✔ Checking for robots.txt file...
- ✔ Checking for absence of the security.txt file...
- ✔ Checking for use of untrusted certificates...
- ✔ Checking for enabled HTTP debug methods...
- ✔ Checking for enabled HTTP OPTIONS method...
- ✔ Checking for secure communication...
- ✔ Checking for directory listing...
- ✔ Checking for missing HTTP header - Strict-Transport-Security...
- ✔ Checking for domain too loose set for cookies...
- ✔ Checking for HttpOnly flag of cookie...
- ✔ Checking for unsafe HTTP header Content Security Policy...

Scan parameters

Target:	https://fontein-si-umkm-1-3.vercel.app/
Scan type:	Light
Authentication:	False

Scan stats

Unique Injection Points Detected:	3
URLs spidered:	8
Total number of HTTP requests:	18
Average time until a response was received:	422ms