Pentest Tools

Website Vulnerability Scanner Report

✔ **https://www.tesla.com/**

⚠ 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:

High:	0
Medium:	0
Low:	1
Info:	37

Scan information:

Start time:	Oct 20, 2024 / 21:57:58 UTC-04
Finish time:	Oct 20, 2024 / 22:01:03 UTC-04
Scan duration:	3 min, 5 sec
Tests performed:	38/38
Scan status:	Finished

Findings

🚩 Server software and technology found

UNCONFIRMED ⓘ

Software / Version	Category
⌀ waf	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

Screenshot:

Access Denied

You don't have permission to access "http://www.tesla.com/" on this server.

Reference #18.64421202.1729475930.f116a15

https://errors.edgesuite.net/18.64421202.1729475930.f116a15

Figure 1. Website Screenshot

🚩 Security.txt file is missing

URL
Missing: https://www.tesla.com/.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

🚩 Spider results

URL	Method	Page Title	Page Size	Status Code
https://www.tesla.com/	GET		365 B	403

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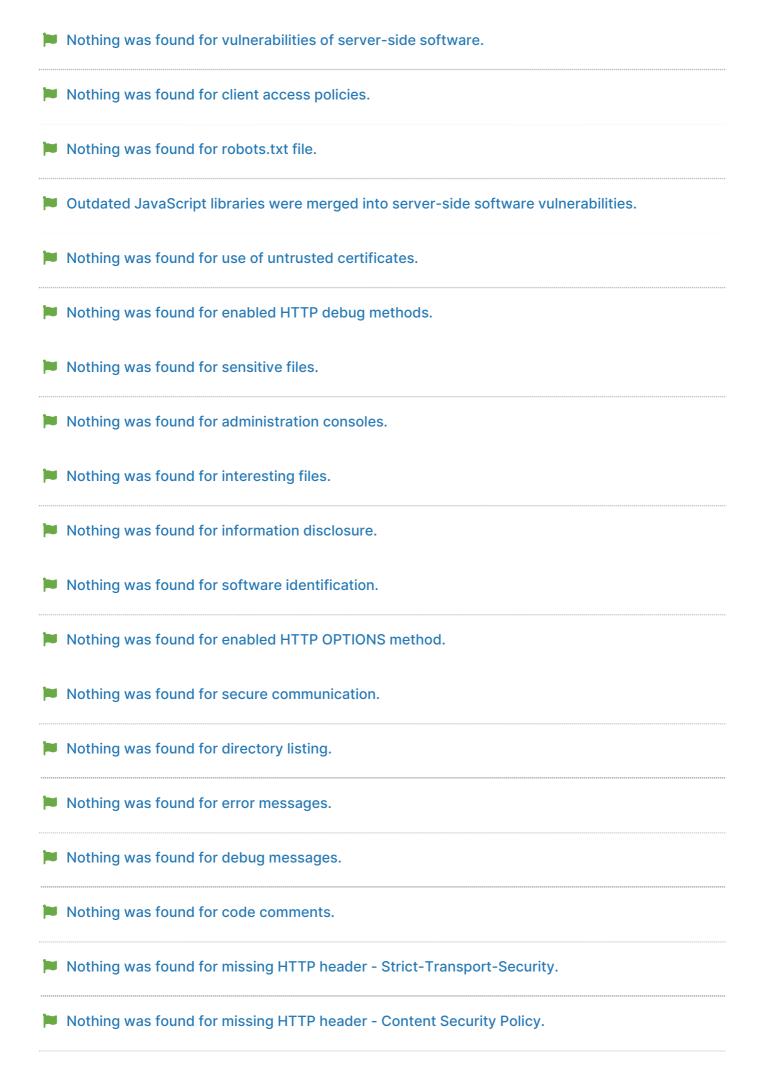
Recommendation:
We recommend to advanced users to make sure the scan properly detected most of the URLs in the application.

References:
All the URLs the scanner found, including duplicates (available for 90 days after the scan date)

🚩 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.

⚑ Outdated JavaScript libraries were merged into server-side software vulnerabilities.

⚑ Nothing was found for use of untrusted certificates.

⚑ Nothing was found for enabled HTTP debug methods.

⚑ Nothing was found for sensitive files.

⚑ Nothing was found for administration consoles.

⚑ Nothing was found for interesting files.

⚑ Nothing was found for information disclosure.

⚑ Nothing was found for software identification.

⚑ Nothing was found for enabled HTTP OPTIONS method.

⚑ Nothing was found for secure communication.

⚑ Nothing was found for directory listing.

⚑ 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 Insecure Direct Object Reference.

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

⚑ Nothing was found for mixed content between HTTP and HTTPS.

⚑ 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 Server Side Request Forgery.

⚑ Nothing was found for Open Redirect.

⚑ Nothing was found for Exposed Backup Files.

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

⚑ Nothing was found for OpenAPI files.

⚑ Nothing was found for file upload.

Scan coverage information

List of tests performed (38/38)

- ✔ Starting the scan...
- ✔ Spidering target...
- ✔ 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 outdated JavaScript libraries...
- ✔ Checking for use of untrusted certificates...
- ✔ Checking for enabled HTTP debug methods...

- ✔ Checking for sensitive files...
- ✔ Checking for administration consoles...
- ✔ Checking for interesting files... (this might take a few hours)
- ✔ Checking for information disclosure... (this might take a few hours)
- ✔ Checking for software identification...
- ✔ Checking for enabled HTTP OPTIONS method...
- ✔ Checking for secure communication...
- ✔ Checking for directory listing...
- ✔ Checking for error messages...
- ✔ Checking for debug messages...
- ✔ Checking for code comments...
- ✔ Checking for missing HTTP header - Strict-Transport-Security...
- ✔ Checking for missing HTTP header - Content Security Policy...
- ✔ Checking for missing HTTP header - X-Content-Type-Options...
- ✔ Checking for missing HTTP header - Referrer...
- ✔ Checking for Insecure Direct Object Reference...
- ✔ Checking for domain too loose set for cookies...
- ✔ Checking for mixed content between HTTP and HTTPS...
- ✔ Checking for internal error code...
- ✔ Checking for HttpOnly flag of cookie...
- ✔ Checking for Secure flag of cookie...
- ✔ Checking for login interfaces...
- ✔ Checking for Server Side Request Forgery...
- ✔ Checking for Open Redirect...
- ✔ Checking for Exposed Backup Files...
- ✔ Checking for unsafe HTTP header Content Security Policy...
- ✔ Checking for OpenAPI files...
- ✔ Checking for file upload...

Scan parameters

Target:	https://www.tesla.com/
Scan type:	Light
Authentication:	False

Scan stats

Unique Injection Points Detected:	1
URLs spidered:	1
Total number of HTTP requests:	14934
Average time until a response was received:	0ms
Total number of HTTP request errors:	42