

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://www.tesla.com/cybertruck>

! 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: 18


Scan information:

Start time: Sep 10, 2024 / 00:35:08 UTC+03
Finish time: Sep 10, 2024 / 00:35:26 UTC+03
Scan duration: 18 sec
Tests performed: 19/19
Scan status: **Finished**

Findings

Server software and technology found

UNCONFIRMED ⓘ

Software / Version	Category
 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://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](#)

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 enabled HTTP OPTIONS method.

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 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 domain too loose set for cookies.

🚩 Nothing was found for HttpOnly flag of cookie.

🚩 Nothing was found for Secure 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 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 missing HTTP header - Content Security Policy...
- ✓ Checking for missing HTTP header - X-Content-Type-Options...
- ✓ Checking for missing HTTP header - Referrer...
- ✓ Checking for domain too loose set for cookies...
- ✓ Checking for HttpOnly flag of cookie...
- ✓ Checking for Secure flag of cookie...
- ✓ Checking for unsafe HTTP header Content Security Policy...

Scan parameters

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

Scan stats

Unique Injection Points Detected: 1
URLs spidered: 1
Total number of HTTP requests: 10
Average time until a response was received: 35ms
