

# 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://djswebserver.com/>

Target added due to a redirect from <https://djswebserver.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:

Medium

### Risk ratings:



### Scan information:

Start time: Sep 20, 2025 / 17:59:13 UTC+03  
 Finish time: Sep 20, 2025 / 17:59:38 UTC+03  
 Scan duration: 25 sec  
 Tests performed: 39/39  
 Scan status: **Finished**

## Findings

### Directory listing is enabled

port 443/tcp

CONFIRMED

URL	Evidence
<a href="https://djswebserver.com/WEFiles/Css">https://djswebserver.com/WEFiles/Css</a>	Found output resembling directory listing. <a href="#">Request / Response</a>
<a href="https://djswebserver.com/WEFiles/Css/v02/">https://djswebserver.com/WEFiles/Css/v02/</a>	Found output resembling directory listing. <a href="#">Request / Response</a>

Details

**Risk description:**

The risk is that it's often the case that sensitive files are "hidden" among public files in that location and attackers can use this vulnerability to access them.

**Recommendation:**

We recommend reconfiguring the web server in order to deny directory listing. Furthermore, you should verify that there are no sensitive files at the mentioned URLs.

**References:**

<http://projects.webappsec.org/w/page/13246922/Directory%20Indexing>

**Classification:**

CWE : [CWE-548](#)  
OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)  
OWASP Top 10 - 2021 : [A1 - Broken Access Control](#)

**Screenshot:**

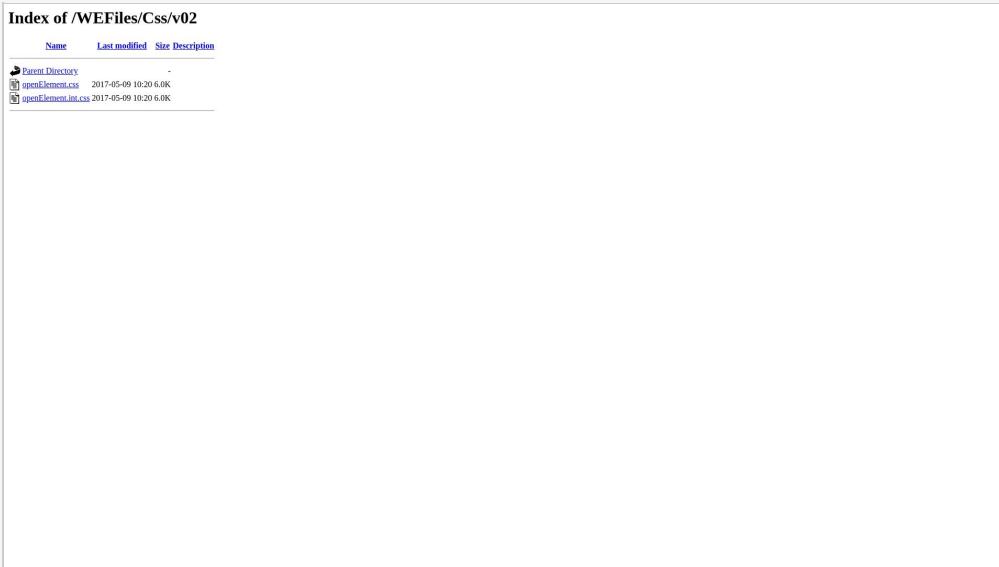


Figure 1. Directory Listing

**Missing security header: Content-Security-Policy**  
port 443/tcp

CONFIRMED

URL	Evidence
<a href="https://djswebserver.com/">https://djswebserver.com/</a>	Response does not include the HTTP Content-Security-Policy security header or meta tag <a href="#">Request / Response</a>

▼ 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://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**  
port 443/tcp

CONFIRMED

<b>URL</b>
<a href="https://djswebserver.com/robots.txt">https://djswebserver.com/robots.txt</a>


▼ 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
 Google Hosted Libraries	CDN
 Apache HTTP Server	Web servers
 jQuery 3.7.1	JavaScript libraries
 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](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

<b>URL</b>
Missing: <a href="https://djswebserver.com/.well-known/security.txt">https://djswebserver.com/.well-known/security.txt</a>

▼ 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 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 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 - 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 unsafe HTTP header Content Security Policy.

---

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 initial connection
- ✓ Scanned for missing HTTP header - Content Security Policy

- ✓ Scanned for directory listing
- ✓ 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 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 - 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 unsafe HTTP header Content Security Policy
- ✓ 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://djswebserver.com/  
scan\_type: Light  
authentication: False

### Scan stats

Unique Injection Points Detected: 87  
URLs spidered: 13  
Total number of HTTP requests: 23  
Average time until a response was received: 231ms