

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://djs-webserver.zanity.net/

Target added due to a redirect from https://djs-webserver.zanity.net

! 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: Apr 25, 2025 / 00:57:05 UTC+03
Finish time: Apr 25, 2025 / 00:57:24 UTC+03
Scan duration: 19 sec
Tests performed: 19/19
Scan status: **Finished**

Findings



Directory listing is enabled

port 443/tcp

CONFIRMED

URL	Evidence
https://djs-webserver.zanity.net/Templates	Found output resembling directory listing. Request / Response
https://djs-webserver.zanity.net/WEFiles/	Found output resembling directory listing. Request / Response

https://djs-webserver.zanity.net/WEFiles/Client/Common	Found output resembling directory listing. Request / Response
https://djs-webserver.zanity.net/WEFiles/Css/	Found output resembling directory listing. Request / Response
https://djs-webserver.zanity.net/WEFiles/Image	Found output resembling directory listing. Request / Response
https://djs-webserver.zanity.net/WEFiles/Image/WEImage	Found output resembling directory listing. Request / Response

▼ 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:

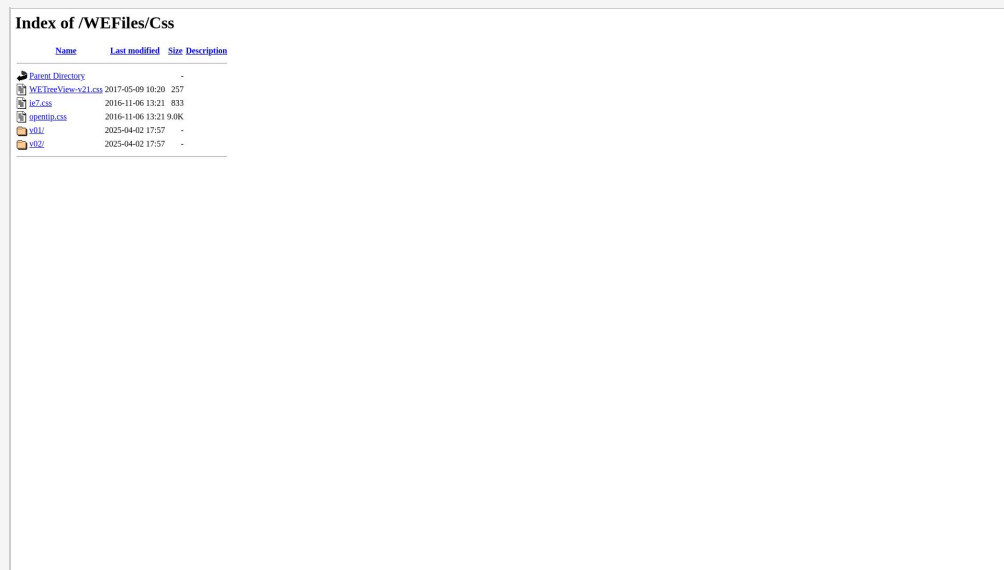


Figure 1. Directory Listing

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

CONFIRMED

URL	Evidence
https://djs-webserver.zanity.net/	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](#)

Unsafe security header: Content-Security-Policy

port 443/tcp

CONFIRMED

URL	Evidence
https://djs-webserver.zanity.net/forums/index.php	<p>Response headers include the HTTP Content-Security-Policy security header with the following security issues:</p> <pre>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'. object-src: Missing object-src allows the injection of plugins which can execute JavaScript. We recommend setting it to 'none'. default-src: The default-src directive should be set as a fall-back when other restrictions have not been specified. script-src: script-src directive is missing.</pre> <p>Request / Response</p>

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

port 443/tcp

CONFIRMED

URL
https://djs-webserver.zanity.net/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

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

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://djs-webserver.zanify.net/.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 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 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 domain too loose set for cookies.

🚩 Nothing was found for HttpOnly flag of cookie.

🚩 Nothing was found for Secure flag of cookie.

Scan coverage information

List of tests performed (19/19)

- ✓ Starting the scan...
- ✓ Checking for missing HTTP header - Content Security Policy...
- ✓ Checking for directory listing...
- ✓ Checking for unsafe HTTP header Content Security Policy...
- ✓ 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 missing HTTP header - Strict-Transport-Security...
- ✓ 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...

Scan parameters

target: https://djs-webserver.zanity.net/
scan_type: Light
authentication: False

Scan stats

Unique Injection Points Detected: 88
URLs spidered: 12

Total number of HTTP requests: 22
Average time until a response was received: 295ms
