Pentest-Tools.com

Website Vulnerability Scanner Report

Full Security Scan Report

✔ https://dbtestdrive.cf/docsprs/public

Summary

Overall risk level:

Low

Risk ratings:

High:	0
Medium:	0
Low:	5
Info:	12

Scan information:

Start time:	2021-03-30 10:16:30 UTC+03
Finish time:	2021-03-30 10:17:01 UTC+03
Scan duration:	31 sec
Tests performed:	17/17
Scan status:	Finished

Findings

Missing security header: Strict-Transport-Security

URL	Evidence
https://dbtestdrive.cf/docsprs/public	Response headers do not include the HTTP Strict-Transport-Security header

Details

Risk description:
The HTTP Strict-Transport-Security header instructs the browser to initiate only secure (HTTPS) connections to the web server and deny any unencrypted HTTP connection attempts. Lack of this header permits an attacker to force a victim user to initiate a clear-text HTTP connection to the server, thus opening the possibility to eavesdrop on the network traffic and extract sensitive information (e.g. session cookies).

Recommendation:
The Strict-Transport-Security HTTP header should be sent with each HTTPS response. The syntax is as follows:

```
Strict-Transport-Security: max-age=<seconds>[; includeSubDomains]
```

The parameter `max-age` gives the time frame for requirement of HTTPS in seconds and should be chosen quite high, e.g. several months. A value below 7776000 is considered as too low by this scanner check.
The flag `includeSubDomains` defines that the policy applies also for sub domains of the sender of the response.

Missing security header: Content-Security-Policy

URL	Evidence
https://dbtestdrive.cf/docsprs/public	Response headers do not include the HTTP Content-Security-Policy security header

Details

Risk description:
The Content-Security-Policy (CSP) header activates a protection mechanism implemented in web browsers which prevents exploitation of Cross-Site Scripting vulnerabilities (XSS). 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.

Read more about CSP:
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

Missing security header: X-Frame-Options

URL	Evidence
https://dbtestdrive.cf/docsprs/public	Response headers do not include the HTTP X-Frame-Options security header

Details

Risk description:
Because the `X-Frame-Options` header is not sent by the server, an attacker could embed this website into an iframe of a third party website. By manipulating the display attributes of the iframe, the attacker could trick the user into performing mouse clicks in the application, thus performing activities without user's consent (ex: delete user, subscribe to newsletter, etc). This is called a Clickjacking attack and it is described in detail here:
https://owasp.org/www-community/attacks/Clickjacking

Recommendation:
We recommend you to add the `X-Frame-Options` HTTP header with the values `DENY` or `SAMEORIGIN` to every page that you want to be protected against Clickjacking attacks.

More information about this issue:
https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

Missing security header: Referrer-Policy

URL	Evidence
https://dbtestdrive.cf/docsprs/public	Response headers do not include the Referrer-Policy HTTP security header

Details

Risk description:
The Referrer-Policy HTTP header controls how much referrer information the browser will send with each request originated from the current web application.
For instance, if a user visits the web page "http://example.com/pricing/" and it 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.

Read more:
https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns

Server software and technology found

Software / Version	Category
Nginx	Web Servers
Twitter Bootstrap	Web Frameworks
Font Awesome	Font Scripts
OWL Carousel	Widgets
SweetAlert	JavaScript Frameworks
TinyMCE	Rich Text Editors
jQuery 3.3.1	JavaScript Frameworks

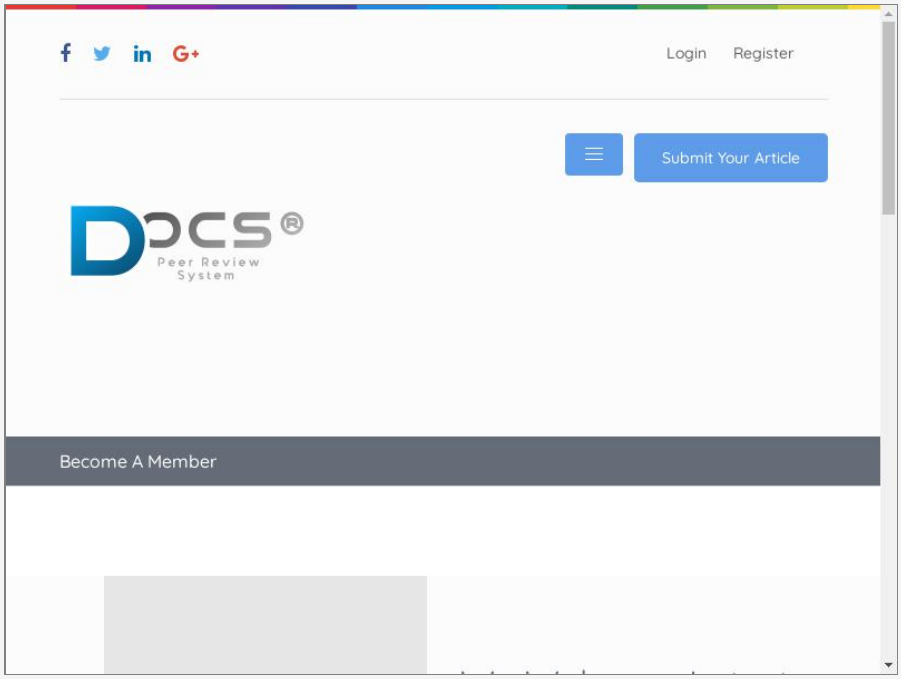
Details

Risk description:
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.

More information about this issue:
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html.

Screenshot:



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 missing HTTP header - X-XSS-Protection.

Nothing was found for domain too loose set for cookies.

Nothing was found for Secure flag of cookie.

Nothing was found for directory listing.

Nothing was found for secure communication.

Nothing was found for missing HTTP header - X-Content-Type-Options.

Nothing was found for HttpOnly flag of cookie.

Scan coverage information

List of tests performed (17/17)

- Checking for website accessibility...
- Checking for missing HTTP header - Strict-Transport-Security...
- Checking for missing HTTP header - Content Security Policy...
- Checking for missing HTTP header - X-Frame-Options...
- Checking for missing HTTP header - Referrer...
- Checking for website technologies...
- Checking for vulnerabilities of server-side software...
- Checking for client access policies...
- Checking for robots.txt file...
- Checking for use of untrusted certificates...
- Checking for missing HTTP header - X-XSS-Protection...
- Checking for domain too loose set for cookies...
- Checking for Secure flag of cookie...
- Checking for directory listing...
- Checking for secure communication...
- Checking for missing HTTP header - X-Content-Type-Options...
- Checking for HttpOnly flag of cookie...

Scan parameters

Website URL:	https://dbtestdrive.cf/docsprs/public
Scan type:	Light
Authentication:	False