

Website Vulnerability Scanner Report

✓ <https://www.dat.com/>

Summary

Overall risk level:

Low

Risk ratings:

High: 0

Medium: 0

Low: 4

Info: 15

Scan information:

Start time: Oct 23, 2023 / 18:49:06

Finish time: Oct 23, 2023 / 18:50:12

Scan duration: 1 min, 6 sec

Tests performed: 19/19

Scan status: **Finished**

Findings

Missing security header: Referrer-Policy

CONFIRMED

URL	Evidence
https://www.dat.com/	Response headers do not include the Referrer-Policy HTTP security header as well as the <meta> tag with name 'referrer' is not present in the response.

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.

References:

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

Classification:

CWE : [CWE-693](#)

OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

Missing security header: X-Frame-Options

CONFIRMED

URL	Evidence
https://www.dat.com/	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 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.

References:

https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

Classification:

CWE : [CWE-693](#)

OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

Robots.txt file found

CONFIRMED

URL

<https://www.dat.com/robots.txt>

▼ Details

Risk description:

There is no particular security risk in having a robots.txt file. However, this file is often misused by website administrators to try to hide some web pages from the users. This should not be considered a security measure because these URLs can be easily read directly from the robots.txt file.

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 - 2013 : [A5 - Security Misconfiguration](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

Server software and technology found

UNCONFIRMED ⓘ

Software / Version	Category
 PHP	Programming languages
 WordPress	CMS, Blogs
 MySQL	Databases
 Unpkg	CDN
 cdnjs	CDN
 Cloudflare	CDN
 Webpack	Miscellaneous
 Module Federation	Miscellaneous
 HTTP/3	Miscellaneous
 Hello Elementor	WordPress themes
 Bootstrap	UI frameworks
 WPMU DEV Smush	WordPress plugins

 Elementor 3.16.6	Page builders, WordPress plugins
 Yoast SEO Premium 21.4	SEO
 Yoast SEO 21.4	SEO, WordPress plugins
 Swiper	JavaScript libraries
 Sumo	Widgets, Marketing automation
 Pingdom	RUM
 OneTrust	Cookie compliance
 OWL Carousel	JavaScript libraries
 jQuery 3.7.6	JavaScript libraries
 Google Analytics	Analytics
 Font Awesome	Font scripts
 WP Engine	PaaS, Hosting
 HSTS	Security

▼ 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.

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 - 2013 : [A5 - Security Misconfiguration](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

Security.txt file is missing

CONFIRMED

URL

Missing: <https://www.dat.com/.well-known/security.txt>

▼ Details

Risk description:

We have detected that the server is missing the security.txt file. There is no particular risk in not creating a valid 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 - 2013 : [A5 - Security Misconfiguration](#)

OWASP Top 10 - 2017 : [A6 - 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 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 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)

- ✓ Checking for website accessibility...
- ✓ Checking for missing HTTP header - Referrer...
- ✓ Checking for missing HTTP header - X-Frame-Options...
- ✓ 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 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 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.dat.com/
Scan type: Light
Authentication: False

Scan stats

Unique Injection Points Detected: 114
URLs spidered: 2
Total number of HTTP requests: 12
Average time until a response was received: 306ms
Total number of HTTP request errors: 4