FULL SCOPE SECURITY

Website Vulnerability Report

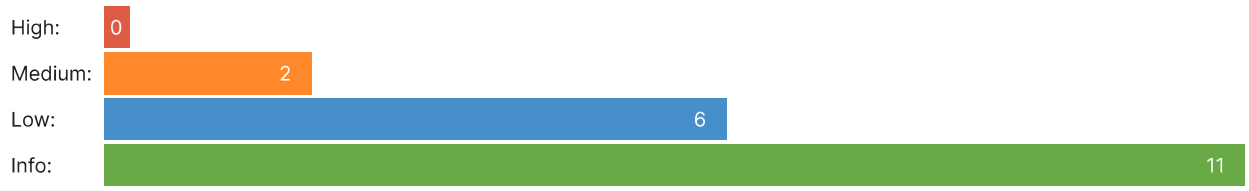
✔ **Target: https://fullscopesec.com/**

Summary

Overall risk level:

Medium

Risk ratings:



Scan information:

Tests performed: 19/19

Scan status: Finished

Findings

Insecure cookie setting: missing HttpOnly flag

CONFIRMED

URL	Cookie Name	Evidence
https://fullscopesec.com/	dps_site_id	The server responded with Set-Cookie header(s) that does not specify the HttpOnly flag: Set-Cookie: dps_site_id=eu-west-2 Request / Response

Details

Risk description:
The risk is that an attacker who injects malicious JavaScript code on the page (e.g. by using an XSS attack) can access the cookie and can send it to another site. In case of a session cookie, this could lead to session hijacking.

Recommendation:
Ensure that the HttpOnly flag is set for all cookies.

References:
https://owasp.org/www-community/HttpOnly

Classification:
CWE : CWE-1004
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Vulnerabilities found for server-side software

UNCONFIRMED

Risk Level	CVSS	CVE	Summary	Affected software
●	6.5	CVE-2021-23337	Lodash versions prior to 4.17.21 are vulnerable to Command Injection via the template function.	lodash 4.17.15
●	5.8	CVE-2020-8203	Prototype pollution attack when using _.zipObjectDeep in lodash before 4.17.20.	lodash 4.17.15
●	5	CVE-2020-28500	Lodash versions prior to 4.17.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the toNumber, trim and trimEnd functions.	lodash 4.17.15

Details

Risk description:
The risk is that an attacker could search for an appropriate exploit (or create one himself) for any of these vulnerabilities and use it to attack the system.

Recommendation:
We recommend you to upgrade the affected software to the latest version in order to eliminate the risk of these vulnerabilities.

Classification:
CWE : CWE-1026
OWASP Top 10 - 2017 : A9 - Using Components with Known Vulnerabilities
OWASP Top 10 - 2021 : A6 - Vulnerable and Outdated Components

Missing security header: Strict-Transport-Security

CONFIRMED

URL	Evidence
https://fullscopesec.com/	Response headers do not include the HTTP Strict-Transport-Security header Request / Response

Details

Risk description:
The risk is that 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.

Classification:
CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Missing security header: Referrer-Policy

CONFIRMED

URL	Evidence
https://fullscopesec.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. Request / Response

Details

Risk description:
The risk is that if a user visits a web page (e.g. "http://example.com/pricing/") and 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 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Missing security header: X-Content-Type-Options

CONFIRMED

URL	Evidence
https://fullscopesec.com/	Response headers do not include the X-Content-Type-Options HTTP security header Request / Response

Details

Risk description:

The risk is that lack of this header could make possible attacks such as Cross-Site Scripting or phishing in Internet Explorer browsers.

Recommendation:

We recommend setting the X-Content-Type-Options header such as `X-Content-Type-Options: nosniff` .

References:

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

Classification:

CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Unsafe security header: Content-Security-Policy

CONFIRMED

URL	Evidence

https://fullscopesec.com/	Response headers include the HTTP Content-Security-Policy security header with the following security issues:
	`frame-ancestors: This directive tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. The recommended value is 'none' or 'self'.`
	`frame-ancestors: This directive tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. The recommended value is 'none' or 'self'.`
	`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.`
	`object-src: Missing object-src allows the injection of plugins which can execute JavaScript. We recommend setting it to 'none'.`
	`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'.`
	Request / Response

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

CONFIRMED

URL
https://fullscopesec.com/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

UNCONFIRMED

Software / Version	Category
Facebook Pixel	Analytics
Google Analytics	Analytics
RequireJS	JavaScript frameworks
Lodash 4.17.15	JavaScript libraries
core-js 3.0.0	JavaScript libraries
Open Graph	Miscellaneous
React 17.0.2	JavaScript frameworks
PWA	Miscellaneous
GoDaddy Website Builder 8.0.0000	CMS
Re:amaze	Live chat

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://fullscopesec.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 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 directory listing.

Nothing was found for missing HTTP header - Content Security Policy.

Nothing was found for domain too loose set for cookies.

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 - Strict-Transport-Security...
- Checking for missing HTTP header - Referrer...
- Checking for HttpOnly flag of cookie...
- Checking for missing HTTP header - X-Content-Type-Options...
- 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 directory listing...
- Checking for missing HTTP header - Content Security Policy...
- Checking for domain too loose set for cookies...
- Checking for Secure flag of cookie...

Scan parameters

Target:	https://fullscopesec.com/
Scan type:	Light
Authentication:	False

Scan stats

Unique Injection Points Detected:	10

URLs spidered:	3
Total number of HTTP requests:	12
Average time until a response was received:	29ms