

Website Vulnerability Scanner Report

✓ <https://www.irobot.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:

High: 0
Medium: 1
Low: 4
Info: 14

Scan information:

Start time: Jun 25, 2024 / 23:11:27
Finish time: Jun 25, 2024 / 23:12:19
Scan duration: 52 sec
Tests performed: 19/19
Scan status: **Finished**

Findings

🚩 Insecure cookie setting: missing HttpOnly flag

CONFIRMED

URL	Cookie Name	Evidence
https://www.irobot.com/	__cq_dnt, cqcid, cquid, dw_dnt, dwac_ddcb22018c454a1247eeba52a2	<p>The server responded with Set-Cookie header(s) that does not specify the HttpOnly flag:</p> <p>Set-Cookie: __cq_dnt=0 Set-Cookie: cqcid=abyHI5pi3DwaQsv2nNgeMQznSX Set-Cookie: cquid= Set-Cookie: dw_dnt=0 Set-Cookie: dwac_ddcb22018c454a1247eeba52a2=IC9K1k03FlonbsQ6UWqqZO0uQ9-k0Li7Omg%3D dw-only USD false US%2FEastern true</p> <p>Request / Response</p>

▼ 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 - 2013 : [A5 - Security Misconfiguration](#)
OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)
OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

🚩 Missing security header: Referrer-Policy

CONFIRMED

URL	Evidence
-----	----------

https://www.irobot.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 - 2013 : [A5 - Security Misconfiguration](#)

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

OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

🚩 Unsafe security header: Content-Security-Policy

CONFIRMED

URL	Evidence
https://www.irobot.com/	Response headers include the HTTP Content-Security-Policy security header with the following security issues: 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 - 2013 : [A5 - Security Misconfiguration](#)

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

OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

🚩 Robots.txt file found

CONFIRMED

URL
https://www.irobot.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 - 2013 : [A5 - Security Misconfiguration](#)

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

OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

🚩 Server software and technology found

UNCONFIRMED ⓘ

Software / Version	Category
 Salesforce Commerce Cloud	Ecommerce
 jQuery UI 1.12.1	JavaScript libraries
TrustArc	Cookie compliance
 Cloudflare	CDN
 Google Tag Manager	Tag managers
 Lodash 4.17.21	JavaScript libraries
 YouTube	Video players
 core-js 3.6.5	JavaScript libraries
 jQuery 3.6.0	JavaScript libraries
 ThreatMetrix	Security, Browser fingerprinting
 Affirm 2	Payment processors, Buy now pay later
 Braintree	Payment processors
 Datadog	RUM, Analytics
 reCAPTCHA	Security
 PowerReviews	Reviews
 HSTS	Security
 Salesforce	CRM
 Salesforce Interaction Studio	Personalisation, Segmentation
 SAP Customer Data Cloud Sign-in	Authentication

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

🚩 Security.txt file is missing

CONFIRMED

URL

Missing: <https://www.irobot.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 - 2013 : [A5 - Security Misconfiguration](#)

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 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 Secure flag of cookie.

Scan coverage information

List of tests performed (19/19)

- ✓ Starting the scan...
- ✓ Checking for HttpOnly flag of cookie...
- ✓ Checking for missing HTTP header - Referrer...
- ✓ 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 - 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 Secure flag of cookie...

Scan parameters

Target: <https://www.irobot.com/>
Scan type: Light
Authentication: False

Scan stats

Unique Injection Points Detected:	95
URLs spidered:	2
Total number of HTTP requests:	11
Average time until a response was received:	422ms
