

Website Vulnerability Scanner Report

✓ <https://tocupboard.infinityfreeapp.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:

Low

Risk ratings:

High:

0

Medium:

0

Low:

5

Info:

14

Scan information:

Start time: Sep 07, 2024 / 14:32:07 UTC-05

Finish time: Sep 07, 2024 / 14:32:35 UTC-05

Scan duration: 28 sec

Tests performed: 19/19

Scan status: **Finished**

Findings

Missing security header: X-Content-Type-Options

CONFIRMED

URL	Evidence
https://tocupboard.infinityfreeapp.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](#)

Missing security header: Strict-Transport-Security

CONFIRMED

URL	Evidence
https://tocupboard.infinityfreeapp.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://tocupboard.infinityfreeapp.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: Content-Security-Policy

CONFIRMED

URL	Evidence
https://tocupboard.infinityfreeapp.com/	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](#)

Server software and technology found

UNCONFIRMED ⓘ

Software / Version	Category
 Nginx	Web servers, Reverse proxies

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](#)

🚩 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 absence of the security.txt file.

🚩 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 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)

- ✔ Starting the scan...
- ✔ Checking for missing HTTP header - X-Content-Type-Options...
- ✔ Checking for missing HTTP header - Strict-Transport-Security...
- ✔ Checking for missing HTTP header - Referrer...
- ✔ Checking for missing 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 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://tocupboard.infinityfreeapp.com/>
Scan type: Light
Authentication: False

Scan stats

Unique Injection Points Detected:	1
URLs spidered:	1
Total number of HTTP requests:	10
Average time until a response was received:	17ms
