Website Vulnerability Scanner Report (Light)

Unlock the full capabilities of this scanner

See what the DEEP scanner can do

Perform in-depth website scanning and discover high risk vulnerabilities.

Testing areas	Light scan	Deep scan
Website fingerprinting	✓	✓
Version-based vulnerability detection	✓	✓
Common configuration issues	✓	✓
SQL injection	–	✓
Cross-Site Scripting	–	✓
Local/Remote File Inclusion	–	✓
Remote command execution	–	✓
Discovery of sensitive files	–	✓

✓ **https://www.starlink.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:	4
Info:	15

Scan information:

Start time:	Jul 19, 2024 / 04:48:57
Finish time:	Jul 19, 2024 / 04:52:23
Scan duration:	3 min, 26 sec
Tests performed:	19/19
Scan status:	Finished

Findings

Unsafe security header: Content-Security-Policy

CONFIRMED

URL	Evidence

https://www.starlink.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'.`
	`script-src:  'self' can be problematic if you host JSONP, Angular or user uploaded files.`
	`script-src:  'unsafe-eval' allows the execution of code injected into DOM APIs such as eval().`
	`default-src:  The default-src directive should be set as a fall-back when other restrictions have not been specified.`
	`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

Missing security header: Referrer-Policy

CONFIRMED

URL	Evidence
https://www.starlink.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

Robots.txt file found

CONFIRMED

URL
https://www.starlink.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
Express	Web frameworks, Web servers
Google Analytics	Analytics
Node.js	Programming languages
Google Tag Manager	Tag managers
OneTrust	Cookie compliance
Linkedin Ads	Advertising
Swiper	JavaScript libraries
hCaptcha	Security
HSTS	Security

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

HTTP OPTIONS enabled

CONFIRMED

URL	Method	Summary
https://www.starlink.com/	OPTIONS	We did a HTTP OPTIONS request. The server responded with a 200 status code and the header: `Allow: GET,HEAD` Request / Response

Details

Risk description:
The only risk this might present nowadays is revealing debug HTTP methods that can be used on the server. This can present a danger if any of those methods can lead to sensitive information, like authentication information, secret keys.

Recommendation:

We recommend that you check for unused HTTP methods or even better, disable the OPTIONS method. This can be done using your webserver configuration.

References:

https://techcommunity.microsoft.com/t5/iis-support-blog/http-options-and-default-page-vulnerabilities/ba-p/1504845
https://docs.nginx.com/nginx-management-suite/acm/how-to/policies/allowed-http-methods/

Classification:

CWE : CWE-16
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 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 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.

Scan coverage information

List of tests performed (19/19)

- ✓ Starting the scan...
- ✓ Checking for unsafe HTTP header Content Security Policy...
- ✓ 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 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 HttpOnly flag of cookie...
- ✓ Checking for Secure flag of cookie...

Scan parameters

Target:	https://www.starlink.com/
Scan type:	Light
Authentication:	False

Scan stats

Unique Injection Points Detected:	36
URLs spidered:	5
Total number of HTTP requests:	14
Average time until a response was received:	102ms