

# Website Vulnerability Scanner Report

✓ https://grok-pen-test.snipe-it.io/login

## **Summary**





### **Scan information:**

Start time: Aug 01, 2025 / 10:25:07 UTC+01 Finish time: Aug 01, 2025 / 11:13:12 UTC+01

Scan duration: 48 min, 5 sec Tests performed: 77/77 Scan status:

## **Findings**



# Unsafe security header: Content-Security-Policy

port 443/tcp

CONFIRMED

URL	Evidence
https://grok-pen- test.snipe- it.io/login	Response headers include the HTTP Content-Security-Policy security header with the following security issues:  script-src: 'self' can be problematic if you host JSONP, Angular or user uploaded files. base-uri: Missing base-uri allows the injection of base tags. They can be used to set the base URL for all r elative (script) URLs to an attacker controlled domain. We recommend setting it to 'none' or 'self'. script-src: 'unsafe-eval' allows the execution of code injected into DOM APIs such as eval(). img-src: Allow only resources downloaded over HTTPS. script-src: ''unsafe-inline'' allows the execution of unsafe in-page scripts and event handlers.
	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.

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.

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

port 443/tcp

CONFIRMED

URL

https://grok-pen-test.snipe-it.io/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).

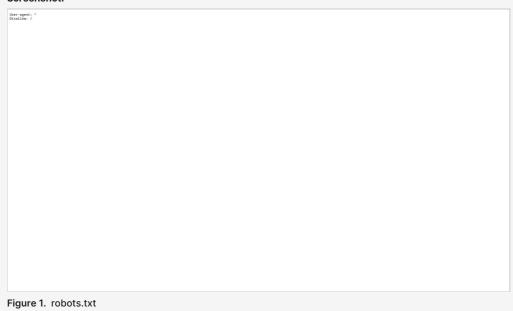
#### References:

https://www.theregister.co.uk/2015/05/19/robotstxt/

#### Classification:

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

### Screenshot:



## Scan coverage information

## List of tests performed (77/77)

- Scanned for unsafe HTTP header Content Security Policy
- Scanned for robots.txt file

## Scan parameters

Authentication:

Target: https://grok-pen-test.snipe-it.io/login

True

Scan type: Deep\_scan\_default

fingerprint: True software\_vulnerabilities: True check\_robots: True outdated\_js: True untrusted\_certificates: True client\_access\_policies: True http\_debug\_methods: True security\_txt: True cors\_misconfiguration: True resource\_discovery: True sensitive\_files: True admin\_consoles: True interesting\_files: True server\_info\_disc: True server\_software: True approach: Auto 10 depth: 100 requests\_per\_second: True xss: sqli: True Ifi: True

oscmdi: True ssrf: True open\_redirect: True broken\_authentication: True php\_code\_injection: True js\_code\_injection: True ruby\_code\_injection: True python\_code\_injection: True perl\_code\_injection: True log4j\_rce: True ssti: True True xxe: viewstate\_rce: True prototype\_pollution: True backup\_files: True request\_url\_override: True http\_request\_smuggling: True True csrf: insecure\_deserialization: True nosqli: True session\_fixation: True security\_headers: True cookie\_security: True directory\_listing: True secure\_communication: True weak\_password\_submission: True error\_debug\_messages: True password\_cleartext: True cross\_domain\_source: True mixed\_content: True sensitive\_data: True login\_interfaces: True

## Scan stats

Unique Injection Points Detected: 2
URLs spidered: 2
Total number of HTTP requests: 13194
Average time until a response was received: 92ms
Total number of HTTP request errors: 287