Website Vulnerability Scanner Report

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

Summary

Overall risk level:
Low

Risk ratings:

Critical:	0
High:	0
Medium:	0
Low:	2
Info:	0

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:	Finished

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 relative (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.

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

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:

Figure 1. robots.txt

Scan coverage information

List of tests performed (77/77)

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

Scan parameters

Target:	https://grok-pen-test.snipe-it.io/login
Scan type:	Deep_scan_default
Authentication:	True
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
depth:	10
requests_per_second:	100
xss:	True
sqli:	True
lfi:	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
xxe:	True
viewstate_rce:	True
prototype_pollution:	True
backup_files:	True
request_url_override:	True
http_request_smuggling:	True
csrf:	True
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