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:	1
Info:	0

Scan information:

Start time:	Sep 01, 2026 / 10:25:09 UTC+01
Finish time:	Sep 01, 2026 / 12:29:51 UTC+01
Scan duration:	2 hrs, 4 min, 42 sec
Tests performed:	81
Scan status:	Finished

Findings

Unsafe security header: Content-Security-Policy

CONFIRMED

port 443/tcp

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: 'unsafe-eval' allows the execution of code injected into DOM APIs such as eval().`
	`script-src: 'self' can be problematic if you host JSONP, Angular or user uploaded files.`
	`script-src: ''unsafe-inline'' allows the execution of unsafe in-page scripts and event handlers.`
	`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'.`
	`img-src: Allow only resources downloaded over HTTPS.`
	
	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-1021
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration
OWASP Top 10 - 2025 : A02 - Security Misconfiguration

Scan coverage information

List of tests performed (81)

Port 443

✔ Scanned for version-based vulnerabilities of server-side software

- ✔ Scanned for CSRF
- ✔ Scanned for sensitive data
- ✔ Scanned for Broken Authentication
- ✔ Scanned for website technologies
- ✔ Scanned for unsafe HTTP header Content Security Policy
- ✔ Scanned for API endpoints
- ✔ Obtained an authenticated session
- ✔ Scanned for emails
- ✔ Scanned for file upload
- ✔ Scanned for enabled HTTP OPTIONS method
- ✔ Scanned for Input Reflected in response body
- ✔ Scanned for login interfaces
- ✔ Scanned for misconfigurations
- ✔ Scanned for Path Disclosure
- ✔ Performed web-crawling on target
- ✔ Scanned for client access policies
- ✔ Scanned for robots.txt file
- ✔ Scanned for absence of the security.txt file
- ✔ Scanned for CORS misconfiguration
- ✔ Scanned for use of untrusted certificates
- ✔ Scanned for enabled HTTP debug methods
- ✔ Scanned for administration consoles
- ✔ Scanned for information disclosure
- ✔ Scanned for software identification
- ✔ Scanned for sensitive files
- ✔ Performed Flowmapping
- ✔ Scanned for interesting files
- ✔ Performed URL search in Wayback Machine
- ✔ Scanned for GraphQL endpoints
- ✔ Performed fuzzing for OpenAPI files
- ✔ Scanned for secure communication
- ✔ Scanned for directory listing
- ✔ Scanned for passwords submitted unencrypted
- ✔ Scanned for Cross-Site Scripting
- ✔ Scanned for SQL Injection
- ✔ Scanned for Local File Inclusion
- ✔ Scanned for OS Command Injection
- ✔ Scanned for error messages
- ✔ Scanned for debug messages
- ✔ Scanned for code comments
- ✔ Scanned for missing HTTP header - Strict-Transport-Security
- ✔ Scanned for missing HTTP header - Content Security Policy
- ✔ Scanned for missing HTTP header - X-Content-Type-Options
- ✔ Scanned for missing HTTP header - Referrer
- ✔ Scanned for XML External Entity Injection
- ✔ Scanned for Insecure Direct Object Reference
- ✔ Scanned for passwords submitted in URLs
- ✔ Scanned for JWT weaknesses
- ✔ Scanned for domain too loose set for cookies
- ✔ Scanned for mixed content between HTTP and HTTPS
- ✔ Scanned for cross domain file inclusion
- ✔ Scanned for internal error code
- ✔ Scanned for HttpOnly flag of cookie
- ✔ Scanned for Secure flag of cookie
- ✔ Scanned for secure password submission
- ✔ Scanned for Server Side Request Forgery
- ✔ Scanned for Open Redirect
- ✔ Scanned for PHP Code Injection
- ✔ Scanned for JavaScript Code Injection
- ✔ Scanned for Ruby Code Injection
- ✔ Scanned for Python Code Injection
- ✔ Scanned for Perl Code Injection

- ✔ Scanned for Remote Code Execution through Log4j
- ✔ Scanned for Server Side Template Injection
- ✔ Scanned for Remote Code Execution through VIEWSTATE
- ✔ Scanned for Prototype Pollution
- ✔ Scanned for Exposed Backup Files
- ✔ Scanned for Request URL Override
- ✔ Scanned for HTTP/1.1 Request Smuggling
- ✔ Scanned for NoSQL Injection
- ✔ Scanned for Insecure Deserialization
- ✔ Scanned for Session Fixation
- ✔ Scanned for OpenAPI files
- ✔ Scanned for SQL statement in request parameter
- ✔ Scanned for password returned in later response
- ✔ Scanned for Session Token in URL
- ✔ Scanned for Response Header Injection
- ✔ Scanned for missing HTTP header - Rate Limit
- ✔ Scanned for PEM-encoded private key material
- ✔ Scanned for partial PEM-encoded private key material

Scan parameters

Target:	https://grok-pen-test.snipe-it.io/login
Scan type:	Deep
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:	621
URLs spidered:	102
Total number of HTTP requests:	33422
Average time until a response was received:	943ms
Total number of HTTP request errors:	837