Website Vulnerability Scanner Report

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

Summary

Overall risk level:

Medium

Risk ratings:

High:	0
Medium:	2
Low:	3
Info:	69

Scan information:

Start time:	Sep 01, 2024 / 10:25:25 UTC+01
Finish time:	Sep 01, 2024 / 11:27:44 UTC+01
Scan duration:	1 hrs, 2 min, 19 sec
Tests performed:	74/74
Scan status:	Finished

Findings

Session Fixation

UNCONFIRMED

URL	Method	Parameters	Evidence

https://grok-pen-test.snipe-it.io/login	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		XSRF-TOKEN=eyJpdiI6IlJWMFlUdUhMdG5HK1I4elJeW5uL3c9PSIsInZhbHVlIjoiS2dxdXI3eE9NTXZoZ0RlMTBmRStKSndVT3ExaHl2WUxqSmxjQXJjZUZ4TEFFbzBSc3FhWi9QdWV...
			We used the original cookies after login to generate a new set of session cookies with the same structure. We injected those in the browser and logged in again. The server returned new session cookies after this new login, but our forged cookies could still be used to potentially continue accessing the account.
			The forged cookies used were:
			`XSRF-TOKEN=fzKqejJ7Jn03S30lTEmbbISlSFm5SaOWS1uSAXd0QTJtJoAicIWmJkpjSaAtZWmPPYK5A2AOWFuCbn25Z1qsAEeJbASScF2jV4JxcWCRNoKRckATSAioA4ASXIiMVXAbPAN1dl63UmSSA3SrcX0TT2CudIi6cYAON2SPVUh5eFWvfoWieV2mRmKIWVNsPYp2L3ZwcHNzVAKnemqSbVepLaZ6ZlWiU2S1T3JjMDKuZXNjPjJzOEl4AUB4OkWjAHSkZXV3OnWlAUKlAnVzAUFzNnN5Akd1NkV5OnFaZXOmOXV2NkZxNEV3PHNyOkl2NEJ5PEF6JjxjeHAoJkpjJo1%4E;grok-pen-test_snipeitv6_session=uc4YL8lRQsDFb43A4nN5ZvmJLWV9slDIW4tI0SXf`
			Request / Response

Details

Risk description:

The risk is that an attacker might be able to fixate or set a user's session ID to one known to them, perhaps through social engineering or by leaving a fixated cookie on a shared or public computer. When a victim logs in using the fixated session ID, they attach the attacker-set session to their authenticated account.

Recommendation:

Ensure a new and cryptographically secure random session ID is generated post-authentication. After a successful authentication, invalidate the user's previous session tokens.

References:

https://owasp.org/www-community/attacks/Session_fixation

Classification:

CWE : CWE-384
OWASP Top 10 - 2017 : A2 - Broken Authentication
OWASP Top 10 - 2021 : A7 - Identification and Authentication Failures

Vulnerabilities found for server-side software

UNCONFIRMED

Risk Level	CVSS	CVE	Summary	Affected software

●	6.4	CVE-2024-6484	Bootstrap Cross-Site Scripting (XSS) vulnerability. More details at: https://github.com/advisories/GHSA-9mvj-f7w8-pvh2 https://nvd.nist.gov/vuln/detail/CVE-2024-6484 https://github.com/rubysec/ruby-advisory-db/blob/master/gems/bootstrap-sass/CVE-2024-6484.yml https://github.com/rubysec/ruby-advisory-db/blob/master/gems/bootstrap/CVE-2024-6484.yml https://github.com/twbs/bootstrap https://www.herodevs.com/vulnerability-directory/cve-2024-6484	Bootstrap 3.3.4
●	4.3	CVE-2018-14040	In Bootstrap before 4.1.2, XSS is possible in the collapse data-parent attribute.	bootstrap 3.3.4
●	4.3	CVE-2018-14042	In Bootstrap before 4.1.2, XSS is possible in the data-container property of tooltip.	bootstrap 3.3.4
●	4.3	CVE-2016-10735	In Bootstrap 3.x before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS is possible in the data-target attribute, a different vulnerability than CVE-2018-14041.	bootstrap 3.3.4
●	4.3	CVE-2018-20676	In Bootstrap before 3.4.0, XSS is possible in the tooltip data-viewport attribute.	bootstrap 3.3.4
●	4.3	CVE-2018-20677	In Bootstrap before 3.4.0, XSS is possible in the affix configuration target property.	bootstrap 3.3.4
●	4.3	CVE-2018-14041	XSS in data-target property of scrollspy. More details at: https://github.com/advisories/GHSA-pj7m-g53m-7638 https://github.com/twbs/bootstrap/issues/20184	Bootstrap 3.3.4
●	N/A	N/A	Bootstrap before 4.0.0 is end-of-life and no longer maintained. More details at: https://github.com/twbs/bootstrap/issues/20631	Bootstrap 3.3.4

⌄ Details

Risk description:
The risk is that an attacker could search for an appropriate exploit (or create one himself) for any of these vulnerabilities and use it to attack the system.

Recommendation:
In order to eliminate the risk of these vulnerabilities, we recommend you check the installed software version and upgrade to the latest version.

Classification:
CWE : CWE-1026
OWASP Top 10 - 2017 : A9 - Using Components with Known Vulnerabilities
OWASP Top 10 - 2021 : A6 - Vulnerable and Outdated Components

Unsafe security header: Content-Security-Policy

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.`
	`script-src:  'unsafe-eval' allows the execution of code injected into DOM APIs such as eval().`
	`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.`
	`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

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

Server software and technology found

UNCONFIRMED

Software / Version	Category
Bootstrap Table	JavaScript libraries
jQuery UI 1.13.3	JavaScript libraries
List.js	JavaScript libraries
Nginx	Web servers, Reverse proxies
PHP	Programming languages
Lodash 4.17.21	JavaScript libraries
Bootstrap 3.3.4	UI frameworks
jQuery 3.5.1	JavaScript libraries
Laravel	Web frameworks
Select2	JavaScript libraries
Webpack	Miscellaneous
Chart.js	JavaScript graphics
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

Screenshot:

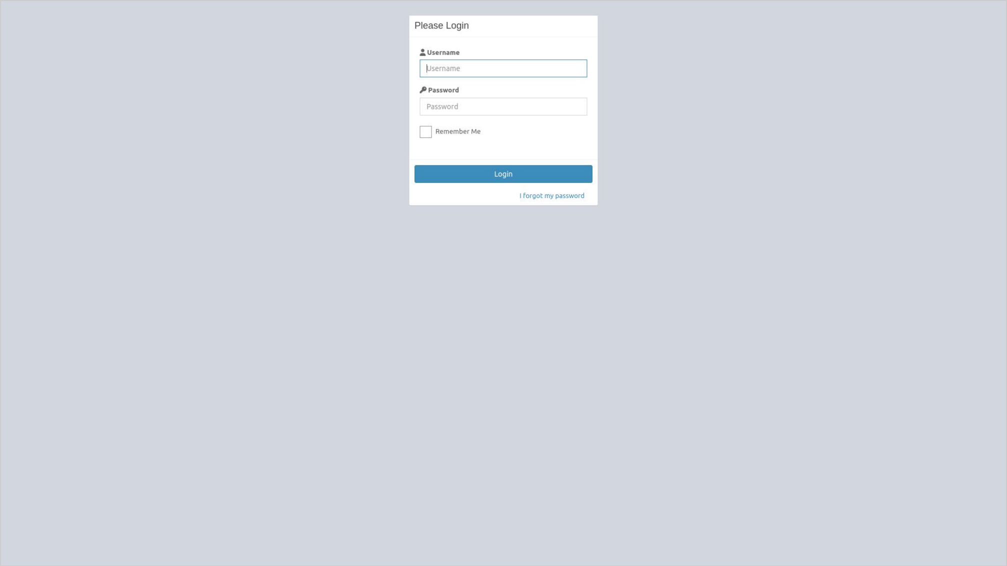

Figure 1. Website Screenshot

Login Interface Found

CONFIRMED

URL	Evidence

https://grok-pen-test.snipe-it.io/login	`<input autocomplete="off" autofocus="" class="form-control" id="username" name="username" placeholder="Username" type="text"/>`
	`<input aria-hidden="true" id="password_fake" name="password_fake" style="display:none;" type="password" value=""/>`
	`<button class="btn btn-primary btn-block">Login</button>`
	Request / Response

Details

Risk description:
The risk is that an attacker could use this interface to mount brute force attacks against known passwords and usernames combinations leaked throughout the web.

Recommendation:
Ensure each interface is not bypassable using common knowledge of the application or leaked credentials using occasional password audits.

References:
https://pentest-tools.com/network-vulnerability-scanning/password-auditor
http://capec.mitre.org/data/definitions/16.html

Screenshot:

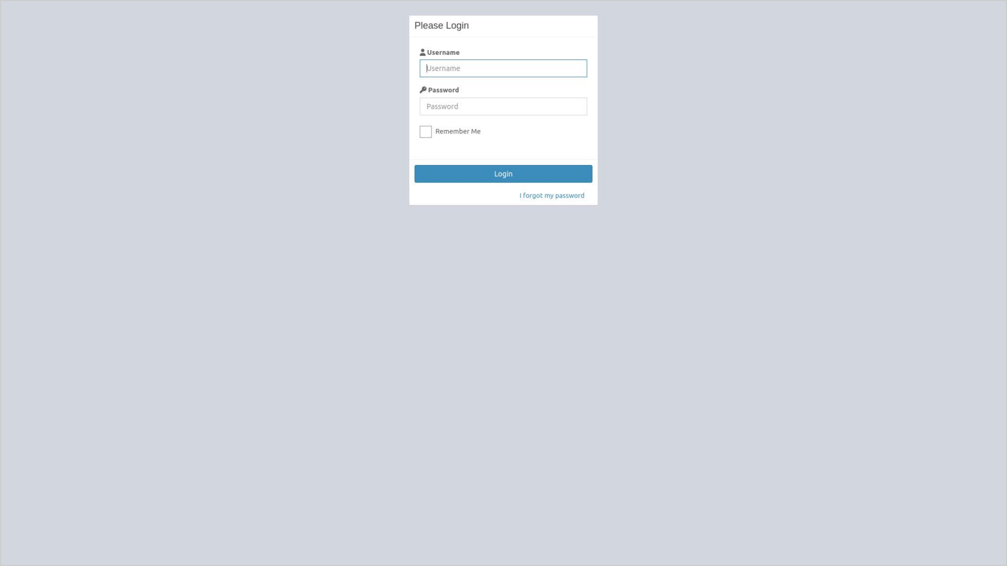

Figure 2. Login Interface

HTTP OPTIONS enabled

CONFIRMED

URL	Method	Summary
https://grok-pen-test.snipe-it.io/login	OPTIONS	We did a HTTP OPTIONS request. The server responded with a 200 status code and the header: `Allow: GET,HEAD,POST` 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

Authentication complete: Recorded method.

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

Details

Screenshot:

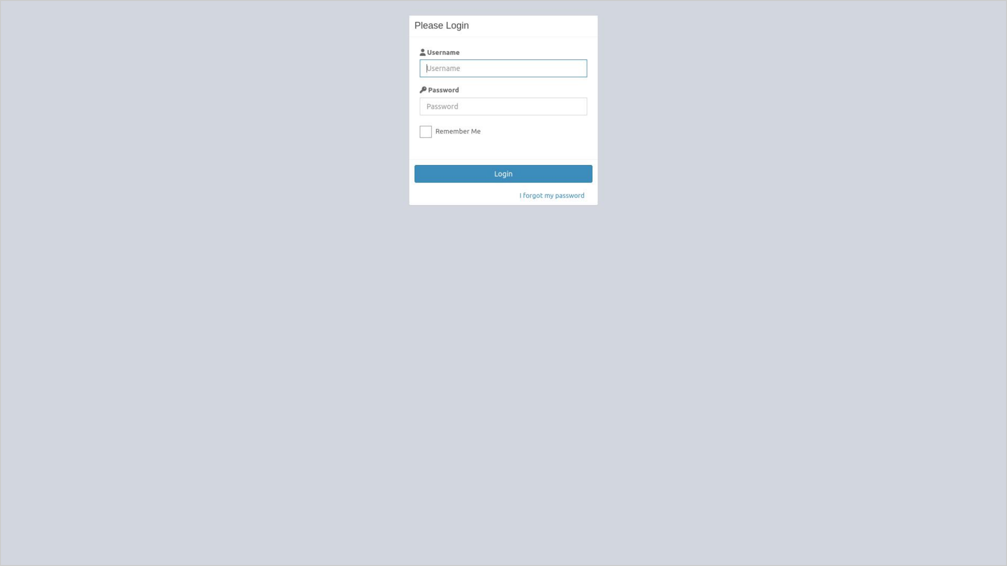

Figure 3. Authentication sequence result

Spider results

URL	Method	Page Title	Page Size	Status Code
https://grok-pen-test.snipe-it.io/login	GET	Dashboard :: Grokability,	113.45 KB	200
https://grok-pen-test.snipe-it.io/	GET	Dashboard :: Grokability,	113.45 KB	200

Details

Risk description:
The table contains all the unique pages the scanner found. The duplicated URLs are not available here as scanning those is considered unnecessary

Recommendation:
We recommend to advanced users to make sure the scan properly detected most of the URLs in the application.

References:
All the URLs the scanner found, including duplicates (available for 90 days after the scan date)

Cloud Hosted URLs

URL	Cloud Provider	Found at URL
https://grok-pen-test.snipe-it.io/account/requestable-assets	AWS	https://grok-pen-test.snipe-it.io/login

Details

Risk description:
The risk is that publicly accessible web addresses hosted in the cloud can expose sensitive information. If access to these resources is not carefully configured, it makes it easier for attackers to gain unauthorized access and cause data breaches.

Recommendation:
We recommend you to implement strong access controls and conduct regular security checks to protect these URLs. Ensure compliance with best practices to protect sensitive data.

website is accessible.

Nothing was found for client access policies.

Nothing was found for absence of the security.txt file.

Outdated JavaScript libraries were merged into server-side software vulnerabilities.

Nothing was found for CORS misconfiguration.

Nothing was found for use of untrusted certificates.

Nothing was found for enabled HTTP debug methods.

Nothing was found for sensitive files.

Nothing was found for administration consoles.

Nothing was found for interesting files.

Nothing was found for information disclosure.

Nothing was found for software identification.

Searching for URLs in Wayback Machine.

Nothing was found for GraphQL endpoints.

Nothing was found for secure communication.

Nothing was found for directory listing.

Nothing was found for passwords submitted unencrypted.

Nothing was found for Cross-Site Scripting.

Nothing was found for SQL Injection.

Nothing was found for Local File Inclusion.

Nothing was found for OS Command Injection.

- Nothing was found for error messages.
- Nothing was found for debug messages.
- Nothing was found for code comments.
- 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 missing HTTP header - Referrer.
- Nothing was found for missing HTTP header - Feature.
- Nothing was found for XML External Entity Injection.
- Nothing was found for Insecure Direct Object Reference.
- Nothing was found for passwords submitted in URLs.
- Nothing was found for JWT weaknesses.
- Nothing was found for domain too loose set for cookies.
- Nothing was found for mixed content between HTTP and HTTPS.
- Nothing was found for cross domain file inclusion.
- Nothing was found for internal error code.
- Nothing was found for HttpOnly flag of cookie.
- Nothing was found for Secure flag of cookie.
- Nothing was found for secure password submission.

Nothing was found for sensitive data.

Nothing was found for Server Side Request Forgery.

Nothing was found for Open Redirect.

Nothing was found for PHP Code Injection.

Nothing was found for JavaScript Code Injection.

Nothing was found for Broken Authentication.

Nothing was found for Ruby Code Injection.

Nothing was found for Python Code Injection.

Nothing was found for Perl Code Injection.

Nothing was found for Remote Code Execution through Log4j.

Nothing was found for Server Side Template Injection.

Nothing was found for Remote Code Execution through VIEWSTATE.

Nothing was found for Exposed Backup Files.

Nothing was found for Request URL Override.

Nothing was found for HTTP/1.1 Request Smuggling.

Nothing was found for CSRF

Nothing was found for NoSQL Injection.

Nothing was found for Insecure Deserialization.

Nothing was found for OpenAPI files.

Nothing was found for file upload.

Nothing was found for SQL statement in request parameter.

Nothing was found for password returned in later response.

Nothing was found for Path Disclosure.

Nothing was found for Session Token in URL.

Scan coverage information

List of tests performed (74/74)

- ✓ Starting the scan...
- ✓ Trying to authenticate...
- ✓ Checking for unsafe HTTP header Content Security Policy...
- ✓ Checking for login interfaces...
- ✓ Spidering target...
- ✓ Scanning for cloud URLs on target...
- ✓ Checking for website technologies...
- ✓ Checking for Session Fixation...
- ✓ 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 outdated JavaScript libraries...
- ✓ Checking for CORS misconfiguration...
- ✓ Checking for use of untrusted certificates...
- ✓ Checking for enabled HTTP debug methods...
- ✓ Checking for sensitive files...
- ✓ Checking for administration consoles...
- ✓ Checking for interesting files... (this might take a few hours)
- ✓ Checking for information disclosure... (this might take a few hours)
- ✓ Checking for software identification...
- ✓ Searching for URLs in Wayback Machine...
- ✓ Checking for enabled HTTP OPTIONS method...
- ✓ Checking for GraphQL endpoints...
- ✓ Checking for secure communication...
- ✓ Checking for directory listing...
- ✓ Checking for passwords submitted unencrypted...
- ✓ Checking for Cross-Site Scripting...
- ✓ Checking for SQL Injection...
- ✓ Checking for Local File Inclusion...
- ✓ Checking for OS Command Injection...
- ✓ Checking for error messages...
- ✓ Checking for debug messages...
- ✓ Checking for code comments...
- ✓ 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 missing HTTP header - Referrer...
- ✓ Checking for missing HTTP header - Feature...
- ✓ Checking for XML External Entity Injection...
- ✓ Checking for Insecure Direct Object Reference...
- ✓ Checking for passwords submitted in URLs...
- ✓ Checking for JWT weaknesses...
- ✓ Checking for domain too loose set for cookies...
- ✓ Checking for mixed content between HTTP and HTTPS...
- ✓ Checking for cross domain file inclusion...
- ✓ Checking for internal error code...
- ✓ Checking for HttpOnly flag of cookie...
- ✓ Checking for Secure flag of cookie...
- ✓ Checking for secure password submission...

- ✓ Checking for sensitive data...
- ✓ Checking for Server Side Request Forgery...
- ✓ Checking for Open Redirect...
- ✓ Checking for PHP Code Injection...
- ✓ Checking for JavaScript Code Injection...
- ✓ Checking for Broken Authentication...
- ✓ Checking for Ruby Code Injection...
- ✓ Checking for Python Code Injection...
- ✓ Checking for Perl Code Injection...
- ✓ Checking for Remote Code Execution through Log4j...
- ✓ Checking for Server Side Template Injection...
- ✓ Checking for Remote Code Execution through VIEWSTATE...
- ✓ Checking for Exposed Backup Files...
- ✓ Checking for Request URL Override...
- ✓ Checking for HTTP/1.1 Request Smuggling...
- ✓ Checking for CSRF
- ✓ Checking for NoSQL Injection...
- ✓ Checking for Insecure Deserialization...
- ✓ Checking for OpenAPI files...
- ✓ Checking for file upload...
- ✓ Checking for SQL statement in request parameter...
- ✓ Checking for password returned in later response...
- ✓ Checking for Path Disclosure...
- ✓ Checking for Session Token in URL...

Scan parameters

Target:	https://grok-pen-test.snipe-it.io/login
Scan type:	Deep_scan_default
Authentication:	True

Scan stats

Unique Injection Points Detected:	1
URLs spidered:	2
Total number of HTTP requests:	15969
Average time until a response was received:	130ms