

# 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: 59

### Scan information:

Start time: Feb 16, 2024 / 16:56:30  
 Finish time: Feb 16, 2024 / 17:15:33  
 Scan duration: 19 min, 3 sec  
 Tests performed: 64/64  
 Scan status: **Finished**

## Findings

### Insecure cookie setting: missing HttpOnly flag

CONFIRMED

| URL   | Cookie Name | Evidence   |
|---|-------------|--|
| <a href="https://grok-pen-test.snipe-it.io/login">https://grok-pen-test.snipe-it.io/login</a> | XSRF-TOKEN  | The server responded with Set-Cookie header(s) that does not specify the HttpOnly flag:<br>Set-Cookie: XSRF-TOKEN=eyJpdil6Ik9ta2VMbmpHeDM3WnBHOVpaeGhZTFE9PSIsInZhbHVlIjoY054SFBuT3k4L3lOaGtKdTBqRmlwczF4NnB2TXIiUTJaNHZvUUVVOTGE1ZTRTNytBRlpZc2p2anAwU25SVGp5Y3NHKzICVWpTY3dTzVM2S3hhRjAvMTRFRk3Q3WGNLTnRHNzdmWWFxcEtoTXRXVnhFOXhFMXdPVXk3dmphWE5DUGkiLCJtYWMiOiI4YTI mYmFiYjcyNDI3YzA5NzFhZTE3NTBIMmJmZWU2Yjc0ZDM1NTNiM2RmNWE0ZmE2YzU2ZmJkODIxZjdhNTNhliwidGFnljoiln0%3D<br><a href="#">Request / Response</a> |

#### Details

#### Risk description:

A cookie has been set without the **HttpOnly** flag, which means that it can be accessed by the JavaScript code running inside the web page. If an attacker manages to inject malicious JavaScript code on the page (e.g. by using an XSS attack) then the cookie will be accessible and it can be transmitted to another site. In case of a session cookie, this could lead to session hijacking.

#### Recommendation:

Ensure that the HttpOnly flag is set for all cookies.

#### References:

<https://owasp.org/www-community/HttpOnly>

#### Classification:

CWE : [CWE-1004](#)  
 OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)  
 OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

### Vulnerabilities found for server-side software

UNCONFIRMED ⓘ

| Risk Level | CVSS | CVE                            | Summary  | Affected software               |
|------------|------|--------------------------------|--|---------------------------------|
| ●          | 4.3  | <a href="#">CVE-2016-10735</a> | 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. | <a href="#">bootstrap 3.3.4</a> |

|   |     |                                |  |                                 |
|---|-----|--------------------------------|--|---------------------------------|
| ● | 4.3 | <a href="#">CVE-2018-14040</a> | In Bootstrap before 4.1.2, XSS is possible in the collapse data-parent attribute.  | <a href="#">bootstrap 3.3.4</a> |
| ● | 4.3 | <a href="#">CVE-2018-14042</a> | In Bootstrap before 4.1.2, XSS is possible in the data-container property of tooltip.  | <a href="#">bootstrap 3.3.4</a> |
| ● | 4.3 | <a href="#">CVE-2018-20676</a> | In Bootstrap before 3.4.0, XSS is possible in the tooltip data-viewport attribute.   | <a href="#">bootstrap 3.3.4</a> |
| ● | 4.3 | <a href="#">CVE-2018-20677</a> | In Bootstrap before 3.4.0, XSS is possible in the affix configuration target property.   | <a href="#">bootstrap 3.3.4</a> |
| ● | 4.3 | <a href="#">CVE-2018-14041</a> | XSS in data-target property of scrollspy. More details at:<br><a href="https://github.com/advisories/GHSA-pj7m-g53m-7638">https://github.com/advisories/GHSA-pj7m-g53m-7638</a><br><a href="https://github.com/twbs/bootstrap/issues/20184">https://github.com/twbs/bootstrap/issues/20184</a> | <a href="#">Bootstrap 3.3.4</a> |
| ● | N/A | N/A                            | Bootstrap before 4.0.0 is end-of-life and no longer maintained. More details at:<br><a href="https://github.com/twbs/bootstrap/issues/20631">https://github.com/twbs/bootstrap/issues/20631</a>  | <a href="#">Bootstrap 3.3.4</a> |

▼ Details

**Risk description:**

These vulnerabilities expose the affected applications to the risk of unauthorized access to confidential data and possibly to denial of service attacks. 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:**

We recommend you to upgrade the affected software to the latest version in order to eliminate the risk of these vulnerabilities.

**Classification:**

CWE : [CWE-1026](#)

OWASP Top 10 - 2013 : [A9 - Using Components with Known Vulnerabilities](#)

OWASP Top 10 - 2017 : [A9 - Using Components with Known Vulnerabilities](#)

🚩 Missing security header: Content-Security-Policy

CONFIRMED

| URL   | Evidence   |
|---|--|
| <a href="https://grok-pen-test.snipe-it.io/login">https://grok-pen-test.snipe-it.io/login</a> | Response headers do not include the HTTP Content-Security-Policy security header<br><a href="#">Request / Response</a> |

▼ Details

**Risk description:**

The Content-Security-Policy (CSP) header activates a protection mechanism implemented in web browsers which prevents exploitation of Cross-Site Scripting vulnerabilities (XSS). If the target application is vulnerable to XSS, lack of this header makes it easily exploitable by attackers.

**Recommendation:**

Configure the Content-Security-Header to be sent with each HTTP response in order to apply the specific policies needed by the application.

**References:**

[https://cheatsheetseries.owasp.org/cheatsheets/Content\\_Security\\_Policy\\_Cheat\\_Sheet.html](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 - 2013 : [A5 - Security Misconfiguration](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

🚩 Robots.txt file found

CONFIRMED

| URL   |
|---|
| <a href="https://grok-pen-test.snipe-it.io/robots.txt">https://grok-pen-test.snipe-it.io/robots.txt</a> |

▼ Details

**Risk description:**

There is no particular security risk in having a robots.txt file. However, this file is often misused by website administrators to try to hide some web pages from the users. This should not be considered a security measure because these URLs can be easily read directly from the robots.txt file.

**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 - 2013 : [A5 - Security Misconfiguration](#)  
OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

🚩 Server software and technology found

UNCONFIRMED ⓘ

| Software / Version   | Category                      |
|--|-------------------------------|
|  Bootstrap Table    | JavaScript libraries          |
|  jQuery UI 1.13.2   | 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                 |
|  Alpine.js 3.13.5 | JavaScript frameworks         |
|  core-js 3.34.0   | JavaScript libraries          |
|  jQuery 3.5.1     | JavaScript libraries          |
|  Livewire         | Web frameworks, Miscellaneous |
|  Laravel          | Web frameworks                |
|  Select2          | JavaScript libraries          |
|  Vue.js 2.4.4     | JavaScript frameworks         |
|  Webpack          | Miscellaneous                 |
|  Chart.js         | JavaScript graphics           |
|  HSTS             | Security                      |

▼ Details

**Risk description:**

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](https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html)

**Classification:**

**Screenshot:**

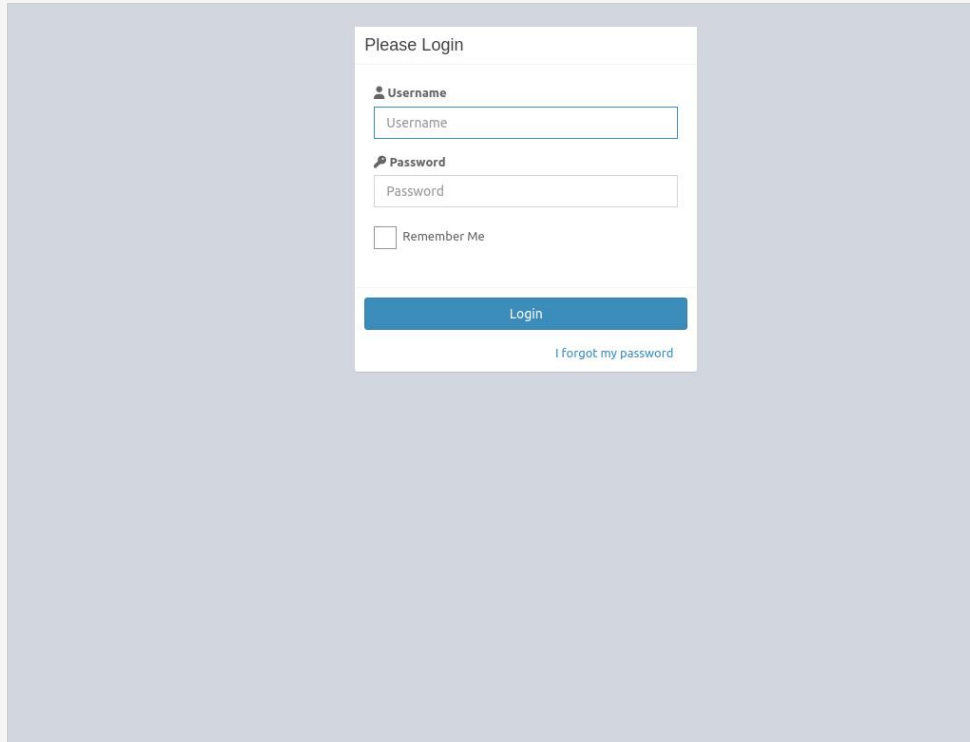


Figure 1. Website Screenshot

**🚩 Login Interface Found**

**CONFIRMED**

| URL   | Evidence   |
|---|--|
| <a href="https://grok-pen-test.snipe-it.io/login">https://grok-pen-test.snipe-it.io/login</a> | <pre>&lt;input autocomplete="off" autofocus="" class="form-control" id="username" name="username" placeholder="Username" type="text"/&gt; &lt;input aria-hidden="true" id="password_fake" name="password_fake" style="display:none;" type="password" value="" /&gt; &lt;button class="btn btn-primary btn-block"&gt;Login&lt;/button&gt;</pre> <p><a href="#">Request / Response</a></p> |

▼ Details

**Risk description:**

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:**

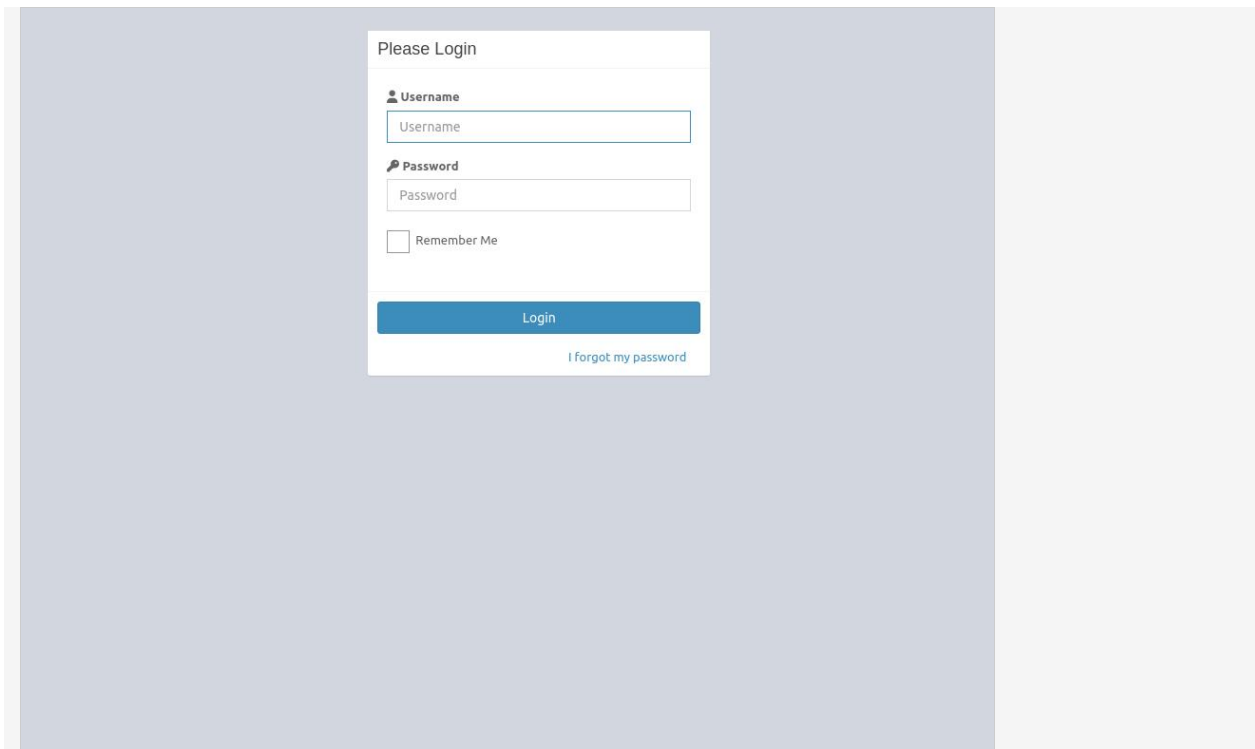


Figure 2. Login Interface

## Security.txt file is missing

CONFIRMED

### URL

Missing: <https://grok-pen-test.snipe-it.io/well-known/security.txt>

### Details

#### Risk description:

We have detected that the server is missing the security.txt file. There is no particular risk in not creating a valid Security.txt file for your server. However, this file is important because it offers a designated channel for reporting vulnerabilities and security issues.

#### Recommendation:

We recommend you to implement the security.txt file according to the standard, in order to allow researchers or users report any security issues they find, improving the defensive mechanisms of your server.

#### References:

<https://securitytxt.org/>

#### Classification:

OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

## Authentication complete: Recorded method.

### URL

<https://grok-pen-test.snipe-it.io/>

### Details

#### Screenshot:

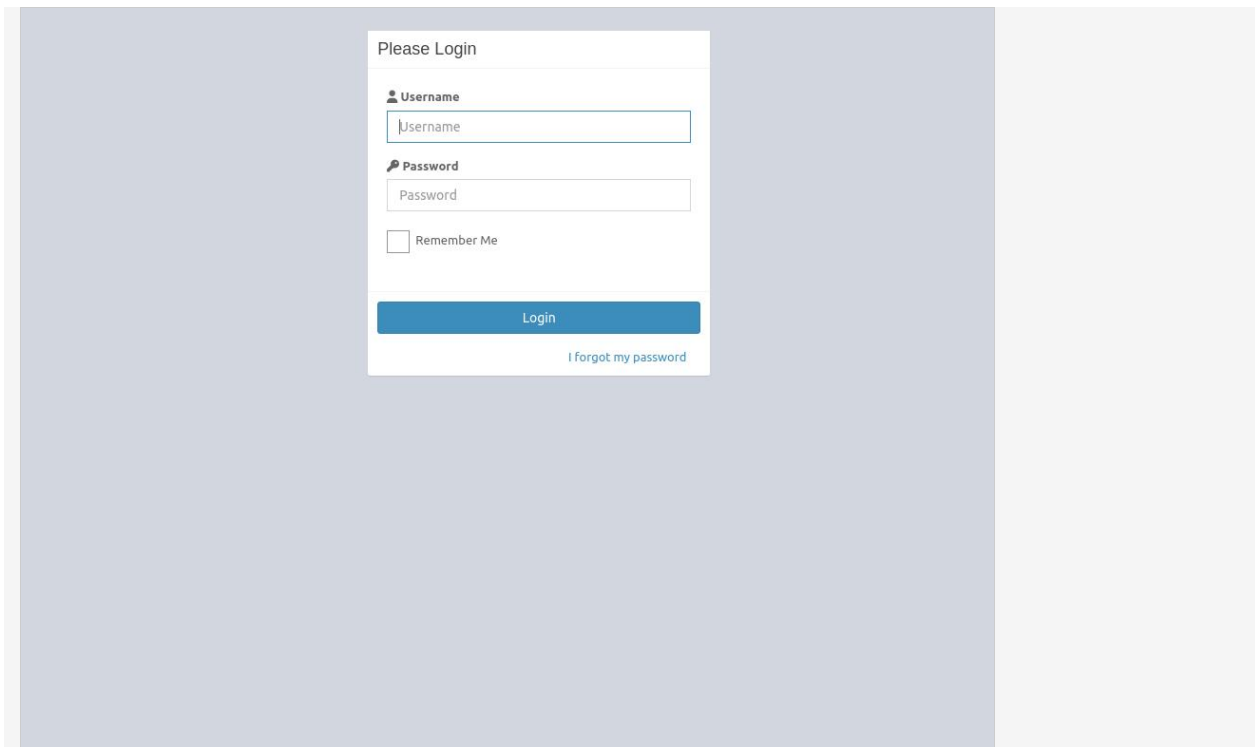


Figure 3. Authentication sequence result

## Spider results

| URL   | Method |
|---|--------|
| <a href="https://grok-pen-test.snipe-it.io/">https://grok-pen-test.snipe-it.io/</a>           | GET    |
| <a href="https://grok-pen-test.snipe-it.io/login">https://grok-pen-test.snipe-it.io/login</a> | GET    |

### 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 |
|---|----------------|
| <a href="https://grok-pen-test.snipe-it.io/users">https://grok-pen-test.snipe-it.io/users</a> | AWS            |

Website is accessible.

Nothing was found for client access policies.

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 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 - X-Frame-Options.

---

🚩 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 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 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 unsafe HTTP header Content Security Policy.

---

🚩 Nothing was found for Session Fixation.

---

## Scan coverage information

---

### List of tests performed (64/64)

- ✓ Checking for website accessibility...
- ✓ Trying to authenticate...
- ✓ Checking for missing HTTP header - Content Security Policy...
- ✓ Checking for HttpOnly flag of cookie...
- ✓ Checking for login interfaces...
- ✓ Spidering target...
- ✓ Scanning for cloud URLs on target...
- ✓ 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 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 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 - X-Frame-Options...
- ✓ 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 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 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 unsafe HTTP header Content Security Policy...
- ✓ Checking for Session Fixation...

### Scan parameters

Target: <https://grok-pen-test.snipe-it.io/login>  
Scan type: Deep\_scan\_default  
Authentication: True

### Scan stats

Unique Injection Points Detected: 2  
URLs spidered: 2  
Total number of HTTP requests: 16133  
Average time until a response was received: 71ms

---