# Website Vulnerability Scanner Report (Light)

## See what the FULL scanner can do

Perform in-depth website scanning and discover high risk vulnerabilities.

| Testing areas | Light scan | Full scan |
|---|---|---|
| Website fingerprinting | ✔ | ✔ |
| Version-based vulnerability detection | ✔ | ✔ |
| Common configuration issues | ✔ | ✔ |
| SQL injection | ✖ | ✔ |
| Cross-Site Scripting | ✖ | ✔ |
| Local/Remote File Inclusion | ✖ | ✔ |
| Remote command execution | ✖ | ✔ |
| Discovery of sensitive files | ✖ | ✔ |

Get a PRO Account to unlock the full capabilities of this scanner!

✔ https://aninix.net/pay

## Summary

**Overall risk level:**

Low

**Risk ratings:**

| | |
|---|---|
| High: | 0 |
| Medium: | 0 |
| Low: | 2 |
| Info: | 8 |

**Scan information:**

| | |
|---|---|
| Start time: | 2019-08-14 22:01:24 UTC+03 |
| Finish time: | 2019-08-14 22:01:29 UTC+03 |
| Scan duration: | 5 sec |
| Tests performed: | 10/10 |
| Scan status: | Finished |

## Findings

### Server software and technology found

| Software / Version | Category |
|---|---|
| lighttpd | Web Servers |
| Google Analytics | Analytics |

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 permit the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

More information about this issue:
https://www.owasp.org/index.php/Fingerprint_Web_Server_(OTG-INFO-002).

## Robots.txt file found

https://aninix.net/robots.txt

Details

**Risk description:**
There is no particular security risk in having a robots.txt file. However, this file is often misused to try to hide some web pages from the users. This should not be done as a security measure because these URLs can easily be read from the robots.txt file.

**Recommendation:**
We recommend you to remove the entries from robots.txt which lead to sensitive locations in the website (ex. administration panels, configuration files, etc).

More information about this issue:
https://www.theregister.co.uk/2015/05/19/robotstxt/

## No vulnerabilities found for server-side software

## No security issue found regarding HTTP cookies

## HTTP security headers are properly configured

## Communication is secure

## No security issue found regarding client access policies

## Directory listing not found (quick scan)

## No password input found (auto-complete test)

## No password input found (clear-text submission test)

## Scan coverage information

### List of tests performed (10/10)

- Fingerprinting the server software and technology...
- Checking for vulnerabilities of server-side software...
- Analyzing the security of HTTP cookies...
- Analyzing HTTP security headers...
- Checking for secure communication...
- Checking robots.txt file...
- Checking client access policies...
- Checking for directory listing (quick scan)...
- Checking for password auto-complete (quick scan)...
- Checking for clear-text submission of passwords (quick scan)...

### Scan parameters

| | |
|---|---|
| Website URL: | https://aninix.net/pay |
| Scan type: | Light |
| Authentication: | False |