My Scans ⌄ | Scheduler | New Scan (/website-vulnerability-scanning/web-server-scanner)

You cannot download reports with a free account. Start by buying some credits (/credits) ✖

Website Vulnerability Scanner Result

Save as pdf

⚠ This is a passive scan which does NOT perform intrusive tests to check for: ✖

- ~~SQL Injection~~
- ~~Cross-Site Scripting (XSS)~~
- ~~Remote Command Execution~~
- ~~Sensitive Files~~

For a comprehensive assessment, you should do a Full Scan (/public/sample-reports/website-vulnscan-sample-report.pdf).

✓ https://xarcade.io

Summary

Overall risk level:

Low

Risk ratings:

High:	0
Medium:	0
Low:	2
Info:	9

Scan information:

Start time:	2017-12-30 15:21:31
Finish time:	2017-12-30 15:21:41
Scan duration:	10.0 seconds
Tests performed:	11/11
Scan status:	Finished

Findings

Server software and technology found

Software / Version	Category
Ubuntu (http://www.ubuntu.com/server)	Operating Systems
Nginx 1.10.3 (http://nginx.org/en)	Web Servers

Twitter Bootstrap (http://getbootstrap.com)	Web Frameworks
Font Awesome (http://fontawesome.io)	Font Scripts
Google Font API (http://google.com/fonts)	Font Scripts
Google Tag Manager (http://www.google.com/tagmanager)	Tag Managers
YouTube (http://www.youtube.com)	Video Players
jQuery (http://jquery.com)	JavaScript Frameworks

› Details

Missing HTTP security headers

HTTP Security Header	Header Role	Status
X-Frame-Options	Protects against Clickjacking attacks	Not set
X-XSS-Protection	Mitigates Cross-Site Scripting (XSS) attacks	Not set
X-Content-Type-Options	Prevents possible phishing or XSS attacks	Not set

› Details

No vulnerabilities found for server-side software

No exploits found for server-side software

No security issue found regarding HTTP cookies

Communication is secure

Robots.txt file not found

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 (11/11)

- ✓ Fingerprinting the server software and technology...
- ✓ Checking for vulnerabilities of server-side software...
- ✓ Checking for exploits for 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://xarcade.io
Scan type:	Quick

Follow @pentesttoolscom

You should also try

- WordPress Scan (/cms-vulnerability-scanning/wordpress-scanner-online-wpscan)
- Drupal Scan (/cms-vulnerability-scanning/drupal-scanner)
- SharePoint Scan (/cms-vulnerability-scanning/sharepoint-security-scanner)