Website Vulnerability Scanner Report

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!

✔ **http://fiistudent.ddns.us**

Summary

Overall risk level:

Medium

Risk ratings:

High:	0
Medium:	1
Low:	2
Info:	7

Scan information:

Start time:	2019-05-27 20:14:20
Finish time:	2019-05-27 20:14:33
Scan duration:	13 sec
Tests performed:	10/10
Scan status:	Finished

Findings

🚩 Communication is not secure

http://fiistudent.ddns.us/

⌄ Details

Risk description:
The communication between the web browser and the server is done using the HTTP protocol, which transmits data unencrypted over the network. Thus, an attacker who manages to intercept the communication at the network level, is able to read and modify the data transmitted (including passwords, secret tokens, credit card information and other sensitive data).

Recommendation:
We recommend you to reconfigure the web server to use HTTPS - which encrypts the communication between the web browser and the server.

🚩 Server software and technology found

Software / Version	Category
Ⓑ Twitter Bootstrap	Web Frameworks
𝓕 Google Font API	Font Scripts
jQuery 3.3.1	JavaScript Frameworks

∨ 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).

⚑ Missing HTTP security headers

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

∨ Details

Risk description:
The X-XSS-Protection HTTP header instructs the browser to stop loading web pages when they detect reflected Cross-Site Scripting (XSS) attacks. Lack of this header exposes application users to XSS attacks in case the web application contains such vulnerability.

The HTTP X-Content-Type-Options header is addressed to Internet Explorer browser and prevents it from reinterpreting the content of a web page (MIME-sniffing) and thus overriding the value of the Content-Type header). Lack of this header could lead to attacks such as Cross-Site Scripting or phishing.

Recommendation:
We recommend setting the X-XSS-Protection header to "X-XSS-Protection: 1; mode=block".
More information about this issue:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection

We recommend setting the X-Content-Type-Options header to "X-Content-Type-Options: nosniff".
More information about this issue:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

⚑ No vulnerabilities found for server-side software

⚑ No security issue found regarding HTTP cookies

⚑ 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 (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:	http://fiistudent.ddns.us
Scan type:	Light
Authentication:	False