Pentest-Tools.com

Website Vulnerability Scanner Report

✓ http://fiistudent.ddns.us/?fbclid=IwAR3t6gTcjz5CeBqBdyW7vVVHteTBAApfrzCbBReUT5QltZiFSQUIEFLHxjI

Summary

Overall risk level:

Medium

Risk ratings:

High:	0
Medium:	1
Low:	1
Info:	8

Scan information:

Start time:	2019-05-04 14:05:55
Finish time:	2019-05-04 14:05:57
Scan duration:	2 sec
Tests performed:	10/10
Scan status:	Finished

Findings

Communication is not secure

http://fiistudent.ddns.us/%5C?fbclid=IwAR3t6gTcjz5CeBqBdyW7vVVHteTBAApfrzCbBReUT5QltZiFSQUIEFLHxjI

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.

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

Server software and technology not found

No vulnerabilities found for server-side software (missing version information)

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/?fbclid=IwAR3t6gTcjz5CeBqBdyW7vVVHteTBAApfrzCbBReUT5QltZiFSQUIEFLHxjI
Scan type:	Light
Authentication:	False