Pentest-Tools.com

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://13.67.136.91/PROGETTO_TSW/**

Summary

Overall risk level:

Medium

Risk ratings:

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

Scan information:

Start time:	2019-06-10 16:30:40
Finish time:	2019-06-10 16:30:42
Scan duration:	2 sec
Tests performed:	10/10
Scan status:	Finished

Findings

⚑ Communication is not secure

http://13.67.136.91/PROGETTO_TSW/

⌄ 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-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

Risk description:
Because the X-Frame-Options header is not sent by the server, an attacker could embed this website into an iframe of a third party website. By manipulating the display attributes of the iframe, the attacker could trick the user into performing mouse clicks in the application, thus performing activities without user's consent (ex: delete user, subscribe to newsletter, etc). This is called a Clickjacking attack and it is described in detail here:
https://www.owasp.org/index.php/Clickjacking

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 you to add the X-Frame-Options HTTP response header to every page that you want to be protected against Clickjacking attacks.
More information about this issue:
https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

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://13.67.136.91/PROGETTO_TSW/
Scan type:	Light
Authentication:	False