Website Vulnerability Scanner Report

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://www.volody.com/insidertrading/login

Summary

Overall risk level:
Medium

Risk ratings:

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

Scan information:

Start time:	2019-07-24 15:54:11 UTC+03
Finish time:	2019-07-24 15:54:30 UTC+03
Scan duration:	19 sec
Tests performed:	10/10
Scan status:	Finished

Findings

Insecure HTTP cookies

Cookie Name	Flags missing
PHPSESSID	Secure, HttpOnly

Details

Risk description:
Since the Secure flag is not set on the cookie, the browser will send it over an unencrypted channel (plain HTTP) if such a request is made. Thus, the risk exists that an attacker will intercept the clear-text communication between the browser and the server and he will steal the cookie of the user. If this is a session cookie, the attacker could gain unauthorized access to the victim's web session.

Lack of the HttpOnly flag permits the browser to access the cookie from client-side scripts (ex. JavaScript, VBScript, etc). This can be exploited by an attacker in conjuction with a Cross-Site Scripting (XSS) attack in order to steal the affected cookie. If this is a session cookie, the attacker could gain unauthorized access to the victim's web session.

Recommendation:
We recommend reconfiguring the web server in order to set the flag(s) Secure , HttpOnly to all sensitive cookies.

More information about this issue:
https://blog.dareboost.com/en/2016/12/secure-cookies-secure-httponly-flags/.

Server software and technology found

Software / Version	Category
Ubuntu	Operating Systems
Apache 2.4.18	Web Servers
PHP	Programming Languages
TweenMax	JavaScript Frameworks
jQuery	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).

Password auto-complete is enabled

```
<input id="password" name="password" placeholder="Password" required="" type="password" value=""/>
```

Details

Risk description:
When password auto-complete is enabled, the browser will remember the password entered into the login form, such that it will automatically fill it next time the user tries to login.
However, if an attacker gains physical access to the victim's computer, he can retrieve the saved password from the browser's memory and use it to gain access to the victim's account in the application.
Furthermore, if the application is also vulnerable to Cross-Site Scripting, the attacker could steal the saved password remotely.

Recommendation:
We recommend you to disable the password auto-complete feature on the login forms by setting the attribute `autocomplete="off"` on all password fields.

More information about this issue:
https://www.owasp.org/index.php/Testing_for_Vulnerable_Remember_Password_(OTG-AUTHN-005).

No vulnerabilities found for server-side software

HTTP security headers are properly configured

Communication is secure

Robots.txt file not found

No security issue found regarding client access policies

Directory listing not found (quick scan)

Passwords are submitted over an encrypted channel

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://www.volody.com/insidertrading/login
Scan type:	Light
Authentication:	False