Pentest-Tools.com

Website Vulnerability Scanner Report (Light)

Get a PRO Account to unlock the FULL capabilities of this scanner

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	✗	✓

✓ http://cpnsuser.esemkaprima.com

Summary

Overall risk level:

High

Risk ratings:

High:	2
Medium:	3
Low:	2
Info:	3

Scan information:

Start time:	2020-04-16 17:27:31 UTC+03
Finish time:	2020-04-16 17:27:53 UTC+03
Scan duration:	22 sec
Tests performed:	10/10
Scan status:	Finished

Findings

Vulnerabilities found for server-side software

Risk Level	CVSS	CVE	Summary	Exploit	Affected software
🔴	7.5	CVE-2019-9641	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF.	N/A	PHP 5.6.40
🟠	6.8	CVE-2015-9253	An issue was discovered in PHP 7.3.x before 7.3.0alpha3, 7.2.x before 7.2.8, and before 7.1.20. The php-fpm master process restarts a child process in an endless loop when using program execution functions (e.g., passthru, exec, shell_exec, or system) with a non-blocking STDIN stream, causing this master process to consume 100% of the CPU, and consume disk space with a large volume of error logs, as demonstrated by an attack by a customer of a shared-hosting facility.	N/A	PHP 5.6.40
🟠	5	CVE-2019-9637	An issue was discovered in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. Due to the way rename() across filesystems is implemented, it is possible that file being renamed is briefly available with wrong permissions while the rename is ongoing, thus enabling unauthorized users to access the data.	N/A	PHP 5.6.40

●	5	CVE-2019-9638	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the maker_note->offset relationship to value_len.	N/A	PHP 5.6.40
●	5	CVE-2019-9639	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the data_len variable.	N/A	PHP 5.6.40

Details

Risk description:
These vulnerabilities expose the affected applications to the risk of unauthorized access to confidential data and possibly to denial of service attacks. An attacker could search for an appropriate exploit (or create one himself) for any of these vulnerabilities and use it to attack the system.

Recommendation:
We recommend you to upgrade the affected software to the latest version in order to eliminate the risk of these vulnerabilities.

Passwords are submitted unencrypted over the network

Login form: http://cpnsuser.esemkaprima.com/

Details

Risk description:
An attacker could intercept the communication between the web browser and the server and he could retrieve the clear-text authentication credentials.

Recommendation:
We recommend you to reconfigure the web server to use HTTPS - which encrypts the communication between the web browser and the server. This way, the attacker will not be able to obtain the clear-text passwords, even though he manages to intercept the network communication.

Insecure HTTP cookies

Cookie Name	Flags missing
ci_session	Secure

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.

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

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

Communication is not secure

http://cpnsuser.esemkaprima.com/

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.

Directory listing is enabled

http://cpnsuser.esemkaprima.com/assets/img/
http://cpnsuser.esemkaprima.com/assets/global/plugins/select2/css/
http://cpnsuser.esemkaprima.com/assets/pages/css/
http://cpnsuser.esemkaprima.com/assets/global/plugins/bootstrap-switch/css/
http://cpnsuser.esemkaprima.com/assets/global/css/
http://cpnsuser.esemkaprima.com/assets/global/plugins/simple-line-icons/
http://cpnsuser.esemkaprima.com/assets/global/plugins/bootstrap/css/
http://cpnsuser.esemkaprima.com/assets/global/plugins/font-awesome/css/
http://cpnsuser.esemkaprima.com/assets/global/plugins/jquery-validation/js/
http://cpnsuser.esemkaprima.com/assets/global/plugins/
http://cpnsuser.esemkaprima.com/assets/global/plugins/bootstrap/js/
http://cpnsuser.esemkaprima.com/assets/pages/scripts/
http://cpnsuser.esemkaprima.com/assets/global/plugins/bootstrap-switch/js/
http://cpnsuser.esemkaprima.com/assets/global/plugins/jquery-slimscroll/
http://cpnsuser.esemkaprima.com/assets/global/scripts/

Details

Risk description:
An attacker can see the entire structure of files and subdirectories from the affected URL. It is often the case that sensitive files are 'hidden' among public files in that location and attackers can use this vulnerability to access them.

Recommendation:
We recommend reconfiguring the web server in order to deny directory listing. Furthermore, you should verify that there are no sensitive files at the mentioned URLs.

More information about this issue:
http://projects.webappsec.org/w/page/13246922/Directory%20Indexing.

Server software and technology found

Software / Version	Category
LiteSpeed	Web Servers
PHP 5.6.40	Programming Languages
CodeIgniter	Web Frameworks
Twitter Bootstrap	Web Frameworks
Font Awesome	Font Scripts
Google Font API	Font Scripts
Select2	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).

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

Robots.txt file not found

No security issue found regarding client access policies

Password auto-complete is disabled

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://cpnsuser.esemkaprima.com
Scan type:	Light
Authentication:	False