Acunetix
by Invicti

Comprehensive Report

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

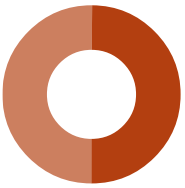
Scan Detail

Target	http://192.168.1.8:8593/
Scan Type	Critical / High / Medium Risk
Start Time	Nov 1, 2025, 6:25:18 AM GMT
Scan Duration	13 minutes
Requests	42890
Average Response Time	1ms
Maximum Response Time	34537ms
Application Build	v24.6.240626115
Authentication Profile	-

0	2	2	1	0
Critical	High	Medium	Low	Informational

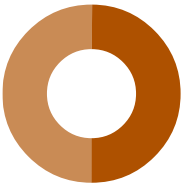
Severity	Vulnerabilities	Instances
Critical	0	0
High	2	2
Medium	2	2
Low	1	1
Informational	0	0
Total	5	5

High Severity



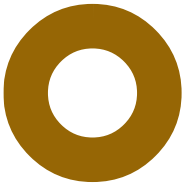
	Instances
Directory traversal	1
Local File Inclusion	1

Medium Severity



	Instances
Insecure HTTP Usage	1
SSL/TLS Not Implemented	1

Low Severity



	Instances
Version Disclosure (PHP)	1

Impacts

SEVERITY	IMPACT	
High	1	Directory traversal
High	1	Local File Inclusion
Medium	1	Insecure HTTP Usage
Medium	1	SSL/TLS Not Implemented
Low	1	Version Disclosure (PHP)

Directory traversal

This script is vulnerable to directory traversal attacks.

Directory Traversal is a vulnerability which allows attackers to access restricted directories and read files outside of the web server's root directory.

Impact

By exploiting directory traversal vulnerabilities, attackers step out of the root directory and access files in other directories. As a result, attackers might view restricted files or execute commands, leading to a full compromise of the Web server.

http://192.168.1.8:8593/index.php

URL encoded GET input **book** was set to **../../../../../../../../../../../../../etc/passwd**

File contents found:

```
root:x:0:0:root:/root:/bin/bash
```

Request

```
GET /index.php?book=../../../../../../../../../../../../../../etc/passwd HTTP/1.1
Referer: http://192.168.1.8:8593/
Cookie: PHPSESSID=mfqbmiltq1jvoatr7he5aqi00f
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36
Host: 192.168.1.8:8593
Connection: Keep-alive
```

Recommendation

Your script should filter metacharacters from user input.

References

Acunetix Directory Traversal Attacks
https://www.acunetix.com/websitesecurity/directory-traversal/

Local File Inclusion

This script is vulnerable to file inclusion attacks.

The script was found to reference and potentially retrieve files from user-specified locations. User input is not sufficiently validated or sanitized prior to being passed to the vulnerable script's include function.

Impact

It is possible for a remote attacker to include a file from local or remote resources and/or execute arbitrary script code with the privileges of the web-server.

http://192.168.1.8:8593/index.php

URL encoded GET input **book** was set to **../../../../../../../../../../../../etc/shells**

Pattern found:

```
# /etc/shells:
```

Request

```
GET /index.php?book=../../../../../../../../../../../../../etc/shells HTTP/1.1
Referer: http://192.168.1.8:8593/
Cookie: PHPSESSID=mfqbmiltq1jvoatr7he5aqi00f
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36
Host: 192.168.1.8:8593
Connection: Keep-alive
```

Recommendation

Edit the source code to ensure that input is properly validated. Where is possible, it is recommended to make a list of accepted filenames and restrict the input to that list.

For PHP, the option **allow_url_fopen** would normally allow a programmer to open, include or otherwise use a remote file using a URL rather than a local file path. It is recommended to disable this option from php.ini.

References

PHP - Using remote files

https://www.php.net/manual/en/features.remote-files.php
OWASP PHP Top 5
https://www.owasp.org/index.php/PHP_Top_5

Remote file inclusion
https://en.wikipedia.org/wiki/Remote_file_inclusion

Insecure HTTP Usage

It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.

Impact

In some circumstances, it could be used for a man-in-the-middle (MitM) attack

http://192.168.1.8:8593/

Request

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36
Host: 192.168.1.8:8593
Connection: Keep-alive
```

Recommendation

It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information

References

HTTP Redirections
https://infosec.mozilla.org/guidelines/web_security#http-redirections

SSL/TLS Not Implemented

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

Impact

Possible information disclosure.

http://192.168.1.8:8593/ Verified

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.8:8593/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36
Host: 192.168.1.8:8593
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

Version Disclosure (PHP)

The web server is sending the X-Powered-By: response headers, revealing the PHP version.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

http://192.168.1.8:8593/

Version detected: **PHP/7.3.14-1~deb10u1**.

Recommendation

Configure your web server to prevent information leakage from its HTTP response.

References

PHP Documentation: header_remove()
https://www.php.net/manual/en/function.header-remove.php

PHP Documentation: php.ini directive expose_php
https://www.php.net/manual/en/ini.core.php#ini.expose-php

Coverage

- http://192.168.1.8:8593
  - .BurpSuite
  - .cache
  - .config
  - .cpan
  - .dbus
  - .gnupg
  - .hashcat
  - .java
  - .john
  - .local
  - .mozilla
  - .msf4
  - .ngrok2
  - .ssh
  - .wine
  - .wpscan
  - admin
  - api
  - axis2
    - axis2-admin
      - welcome
  - binaries
  - cacti
  - cognos_express
    - manager
      - html
  - console
  - crottt
  - Desktop
  - dev

- Documents
- dotdotpwn
- Downloads
- Exploit-Dev
- extrahop
- host-manager
  - html
  - text
- lc
  - system
    - console
- manager
  - html
  - status
- Music
- nagios
- otrs
- Pictures
- Public
- rockmongo
- Sublist3r
- system
  - console
- Templates
- tomcat
  - host-manager
    - html
    - text
  - manager
    - html
    - status
- ui
  - authentication

Videos
webtools
zabbix
.bash_history
.dmrc
.face
.ftp_history
.ICEauthority
.mysql_history
.nc_history
.profile
.selected_editor
.vboxclient-clipboard.pid
.vboxclient-display-svga.pid
.vboxclient-display.pid
.vboxclient-draganddrop.pid
.vboxclient-seamless.pid
.viminfo
.wget-hsts
.Xauthority
.xsession-errors
.xsession-errors.old
1.py
c0up.sh
cmd.pgif
cmd.pht
crash
crash_c
crash.c
crash.cpp
debug.cpp
dokan.c
guido

- index.html
- index.php
  - Inputs
    - GET book
- link.txt
- null.py
- p
- pat
- php-reverse-shell.php
- poc.py
- seh.py
- shellcode
- style.css