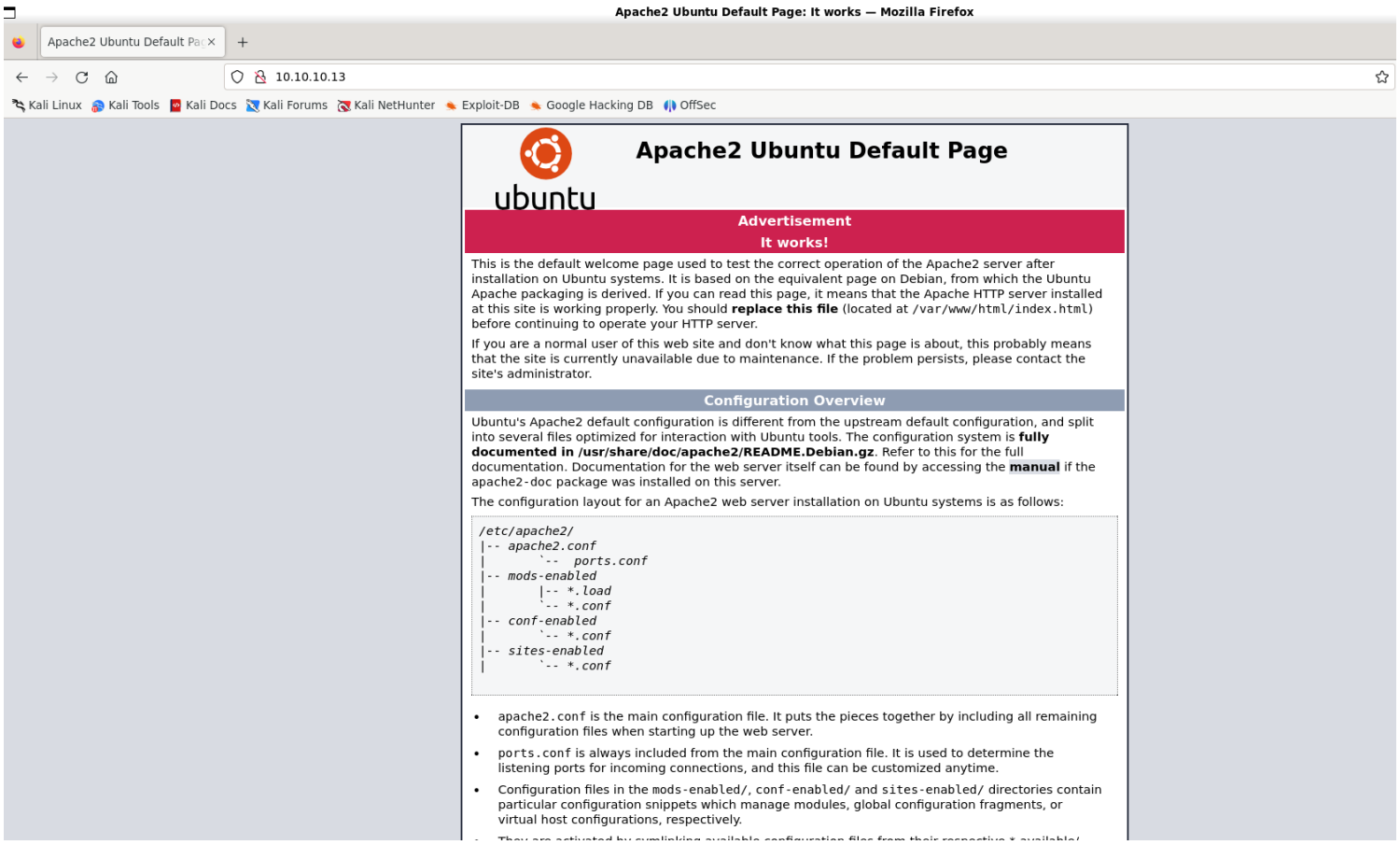
Information Gathering

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
```

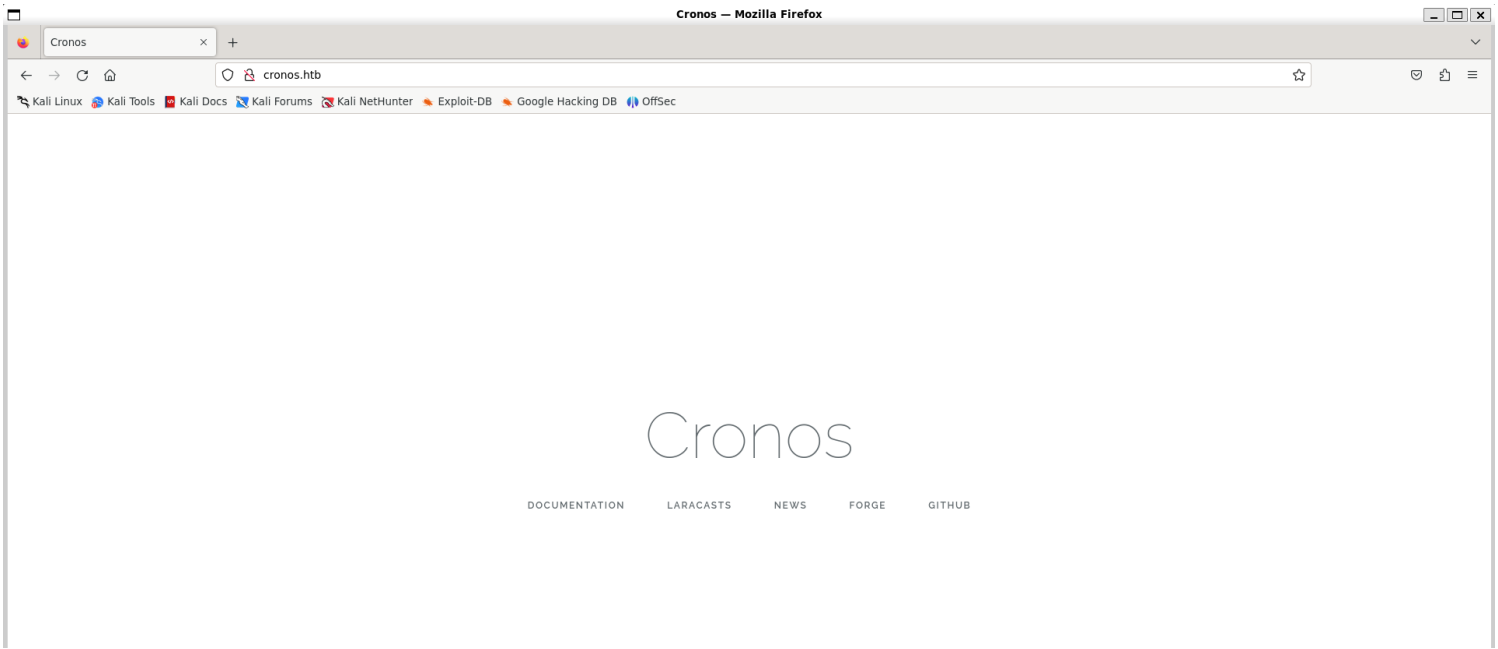
2) Checked the web



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
```

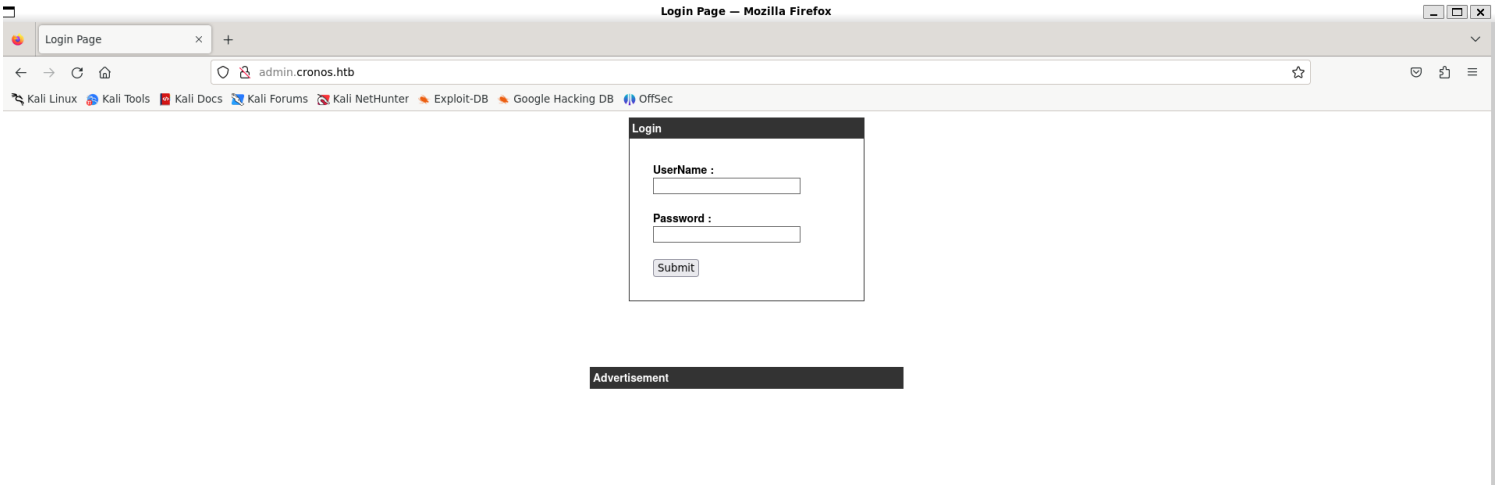
4) The server uses virtual host



5) Found subdomain

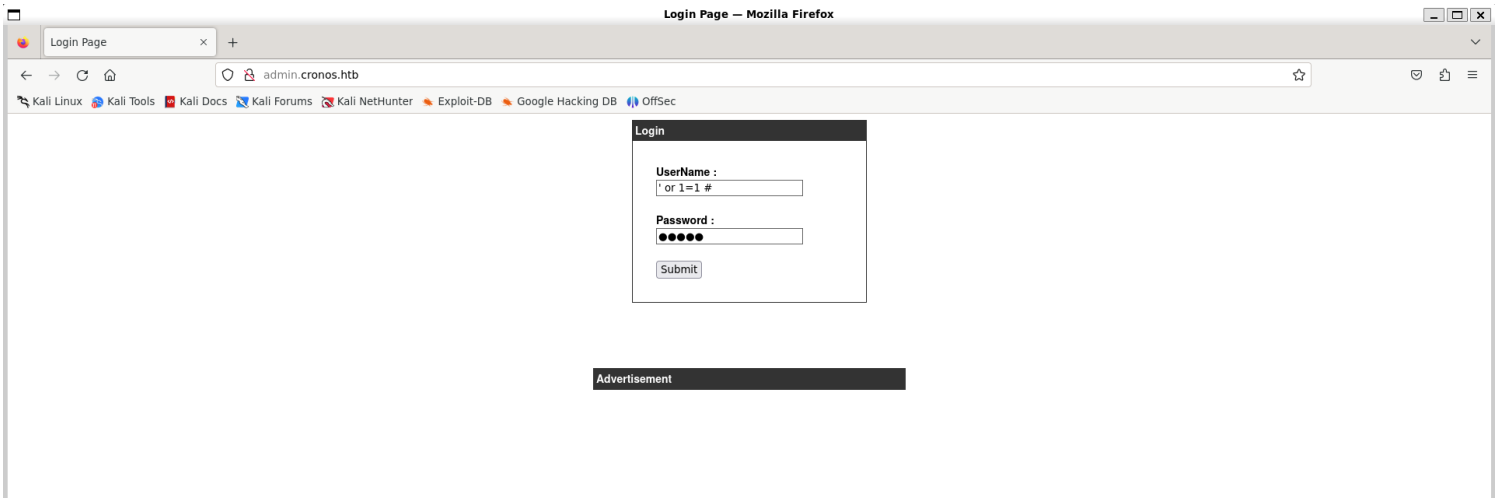
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt -u 'http://10.10.10.13/' -H "Host: FUZZ.cronos.htb" -ic -t 200 -fs 11439

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

      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]
```

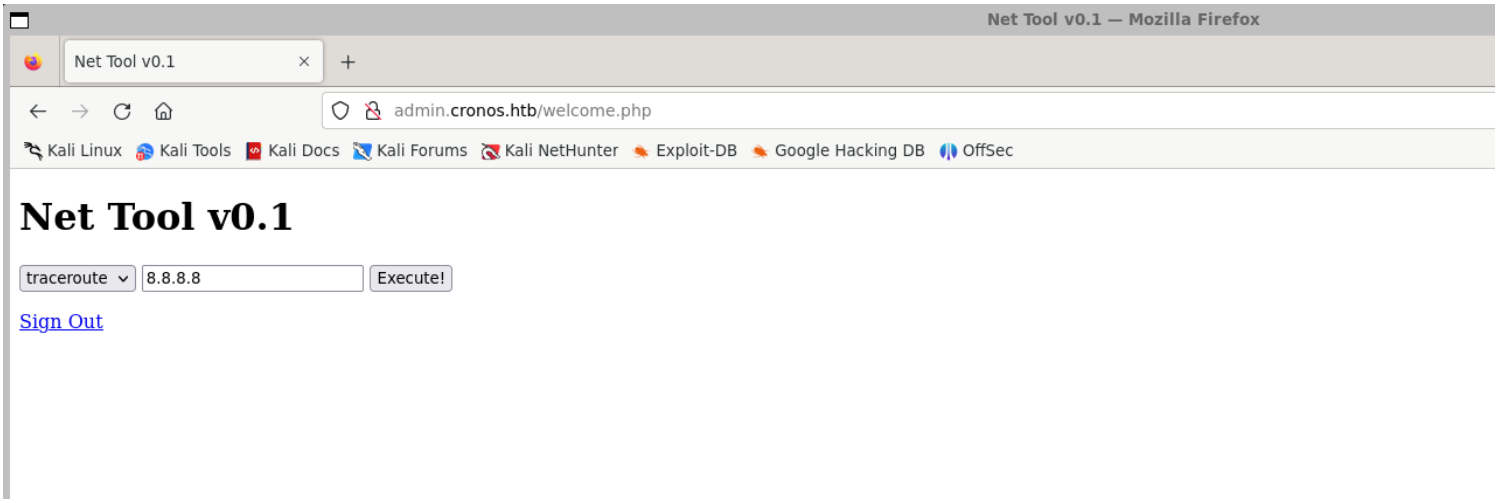
6) Checked admin domain



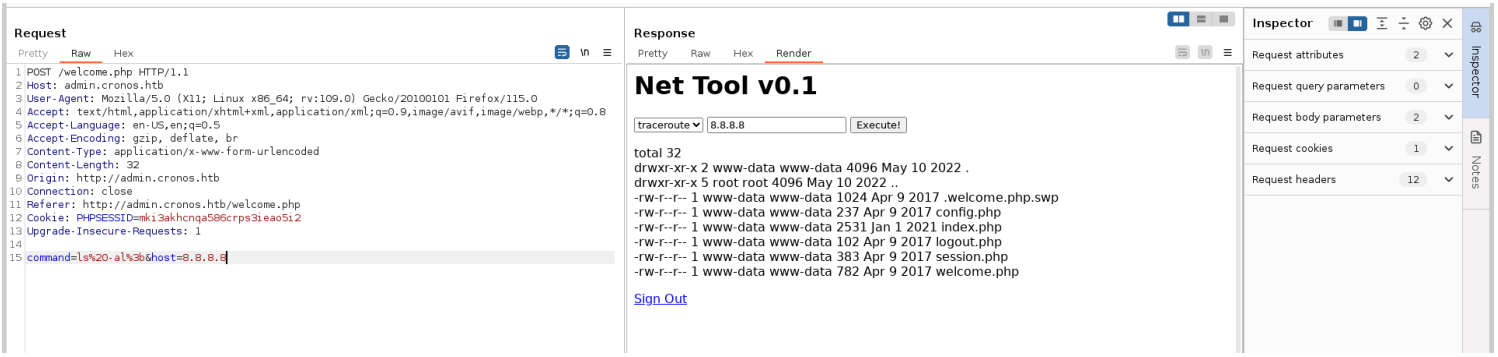
Vulnerability Assessment

1) The login page is vulnerable to sql injection



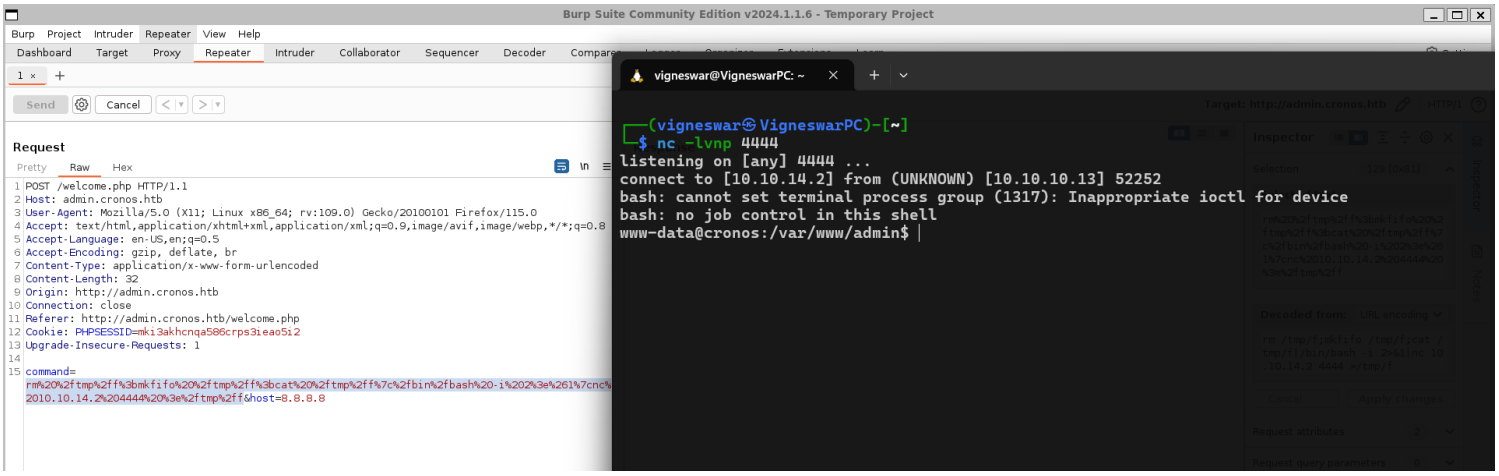


2) The tool is vulnerable to command injection



Exploitation

1) Got reverse shell using command injection



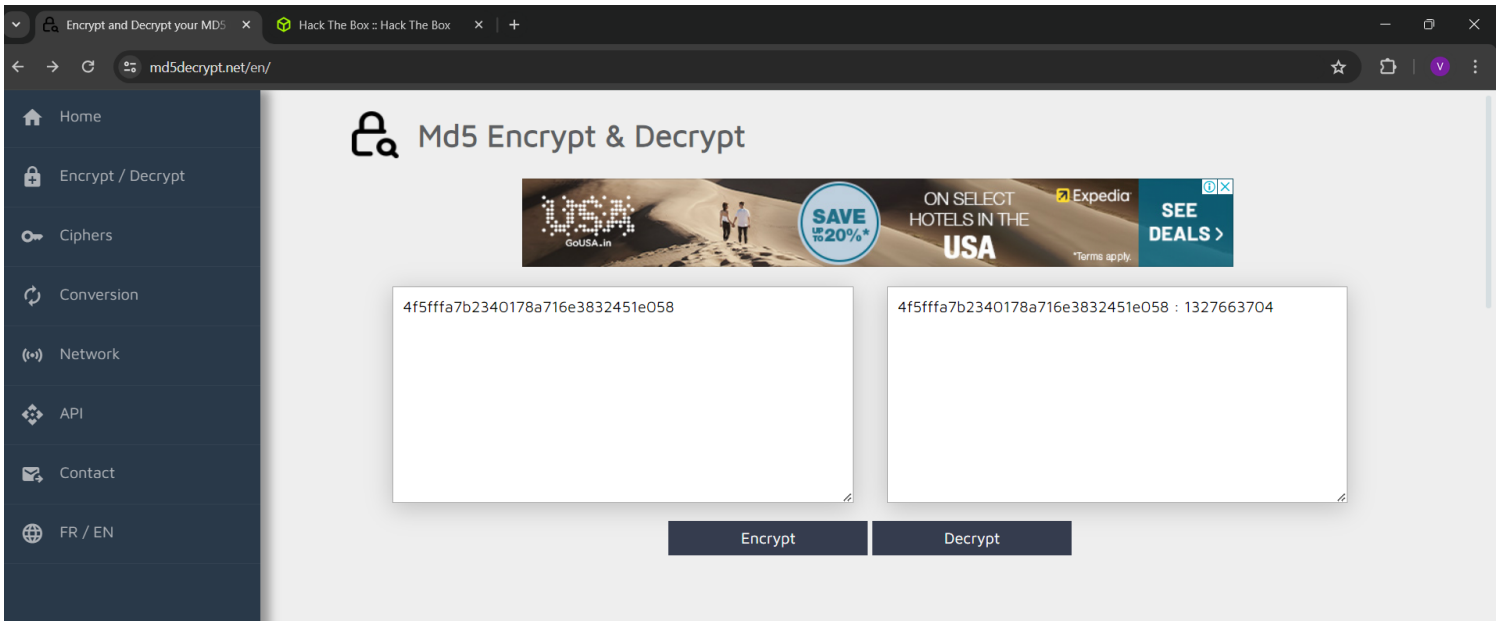
2) Found database credentials

```
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

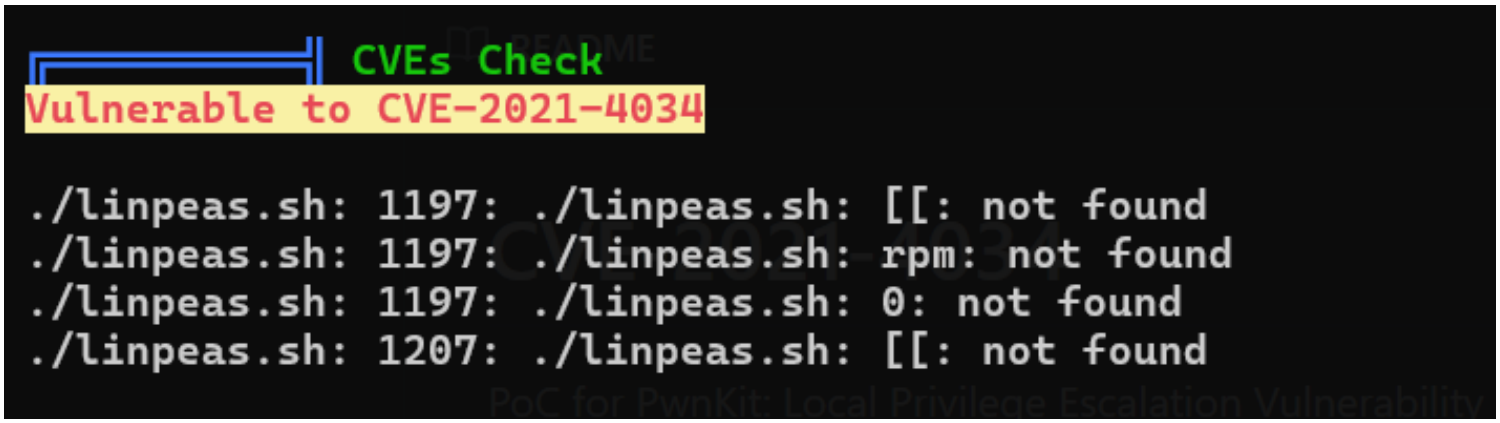
```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| admin              |
+--------------------+
2 rows in set (0.00 sec)

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

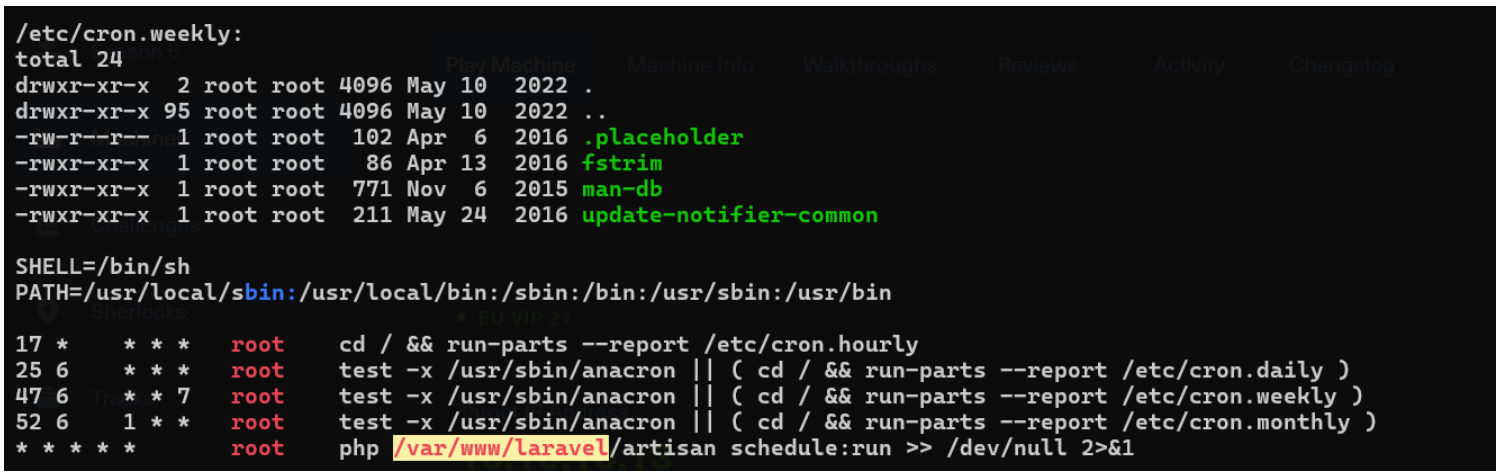


Privilege Escalation

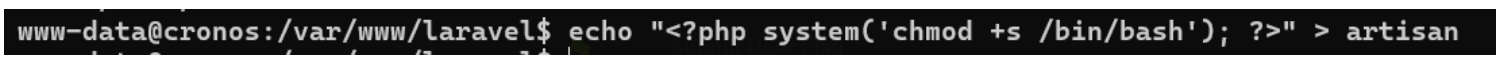
1) Found a CVE for privilege escalation



2) Found cron.weekly with writable directory



3) Made a payload



4) Got root access

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