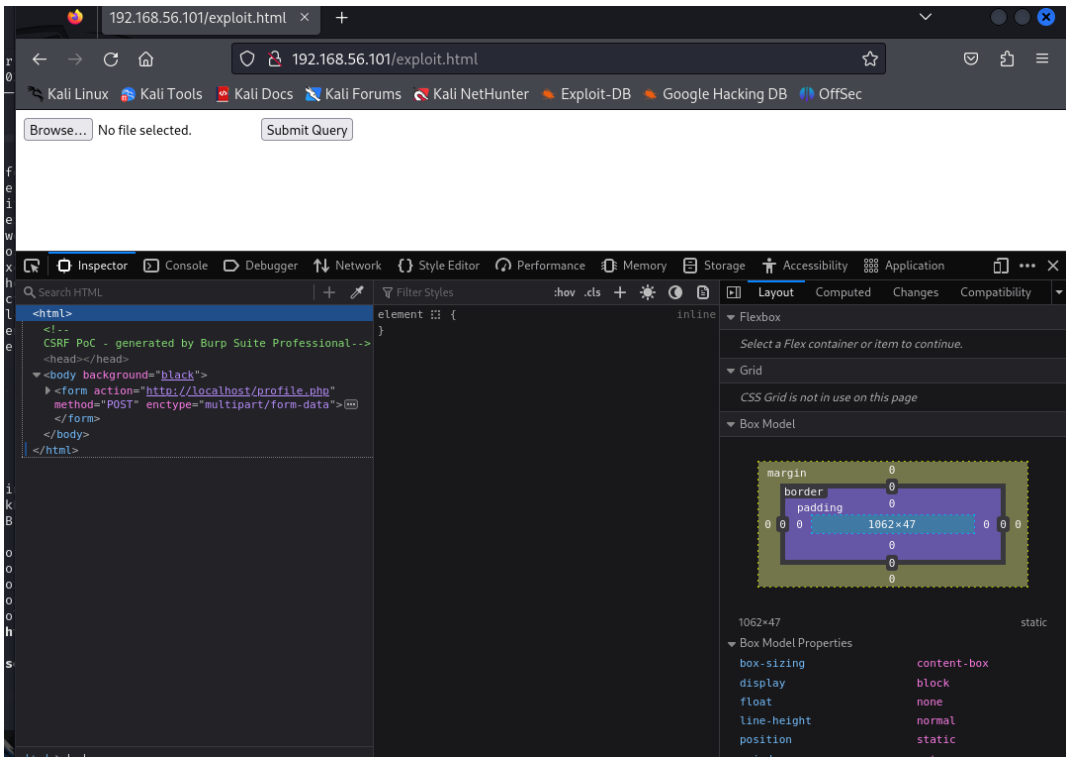
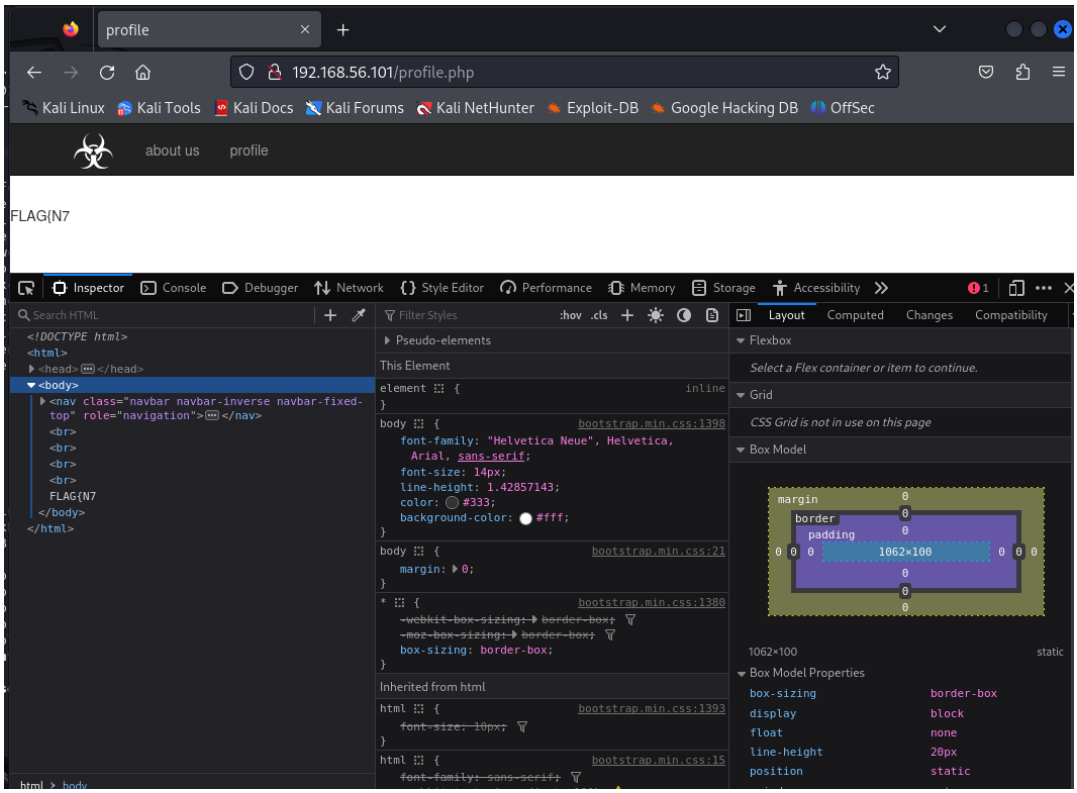
Bonus – N7

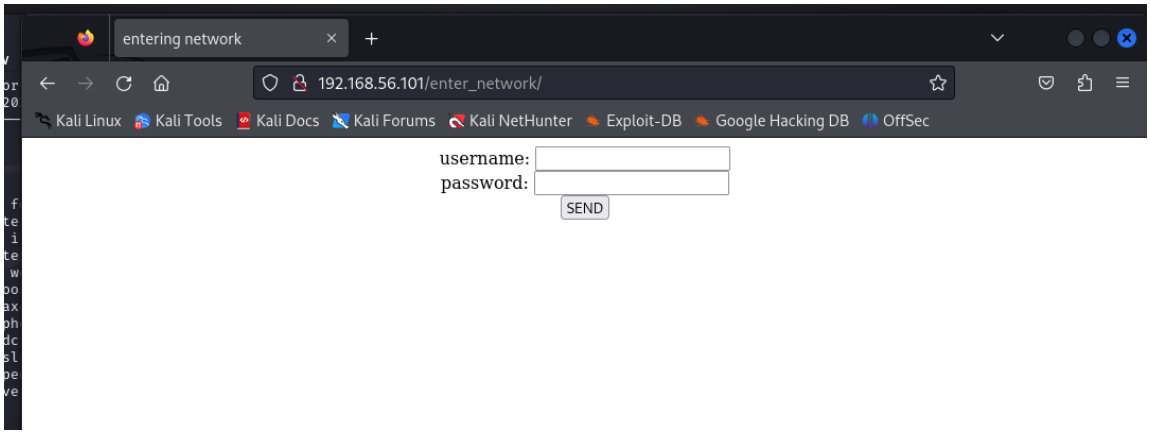
Non appena ho aperto la macchina, con una scheda di rete in modalità host-only, ho cercato l'IP della macchina con il comando sudo arp-scan 192.168.56.0/24, trovando che l'IP della macchina è 192.168.56.101. Ho eseguito anche una scansione con nmap con il comando nmap -sV 192.168.56.101 -Pn scoprendo 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.



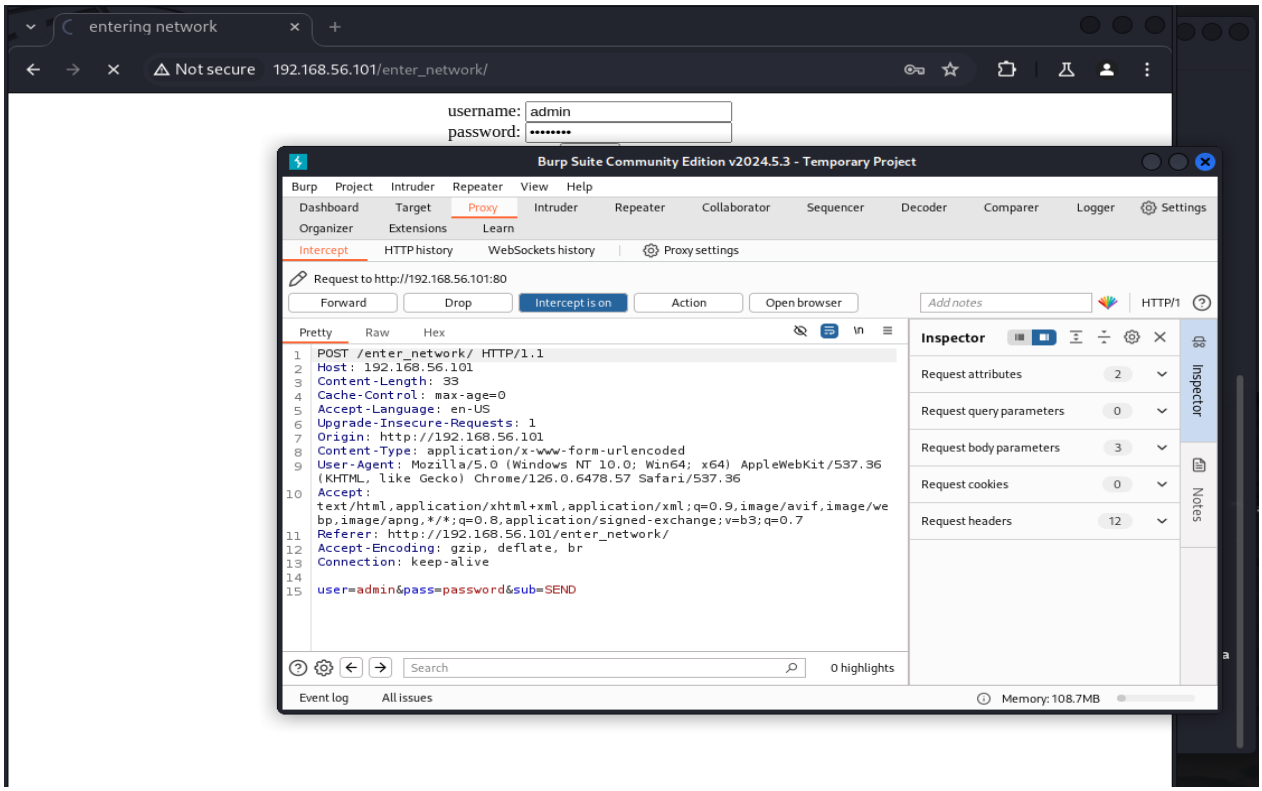
Ho provato a modificare questo URL, inserendo l'IP della macchina al posto di localhost e, rilanciando la pagina, ho trovato il primo flag.



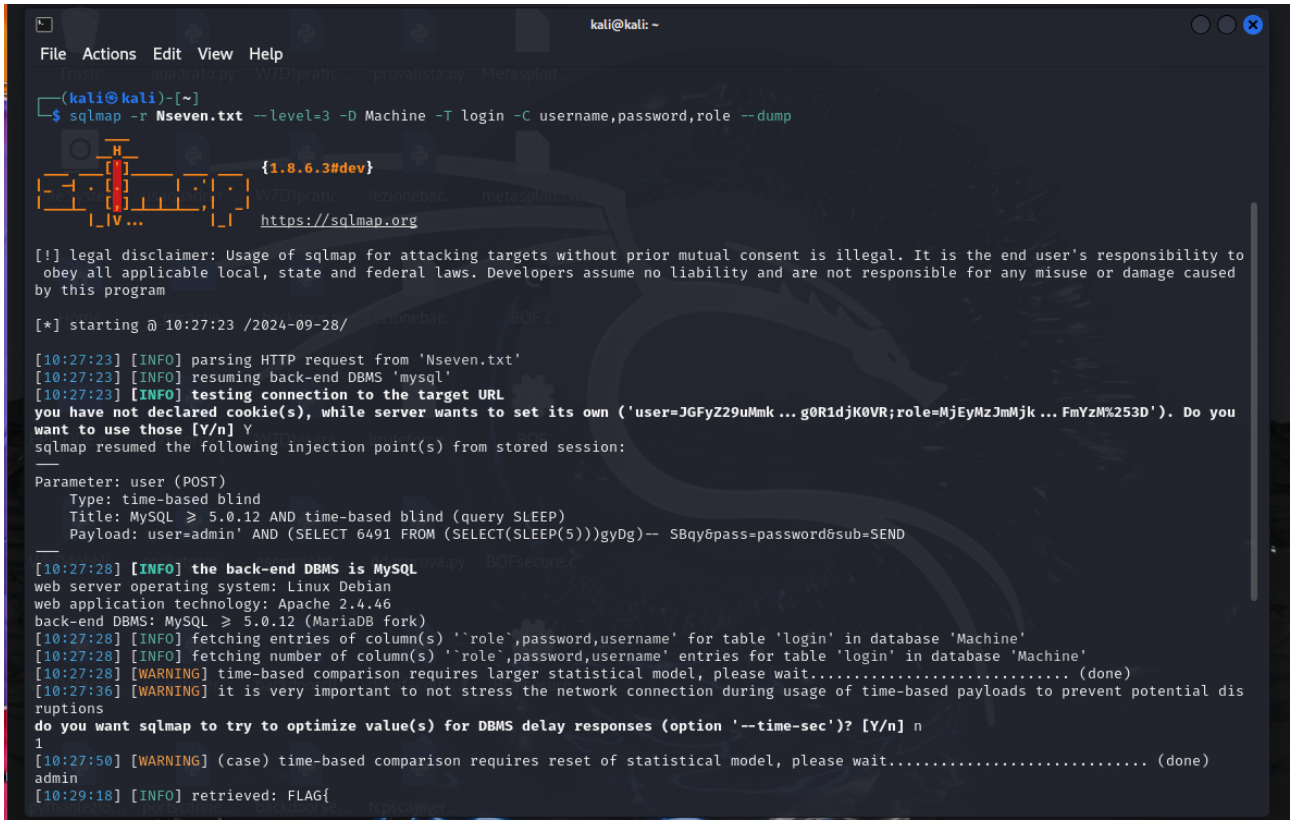
Ho proseguito l'esplorazione delle directories trovate tramite l'enumerazione ed ho trovato la pagina http://192.168.56.101/enter_network/. Vedendo uno username e una password, ho cercato dei modi per fare il login.



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 Neseven.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.



Alla fine ho trovato il secondo flag.