Progetto settimanale

Web application hacking

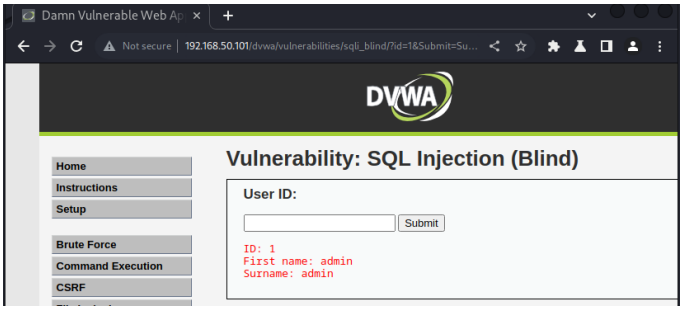
L'esercizio ci chiede di exploitare le vulnerabilità di DVWA di metaspoitable, dove va preconfigurato il livello di sicurezza low:

SQL injection (blind) , XSS stored

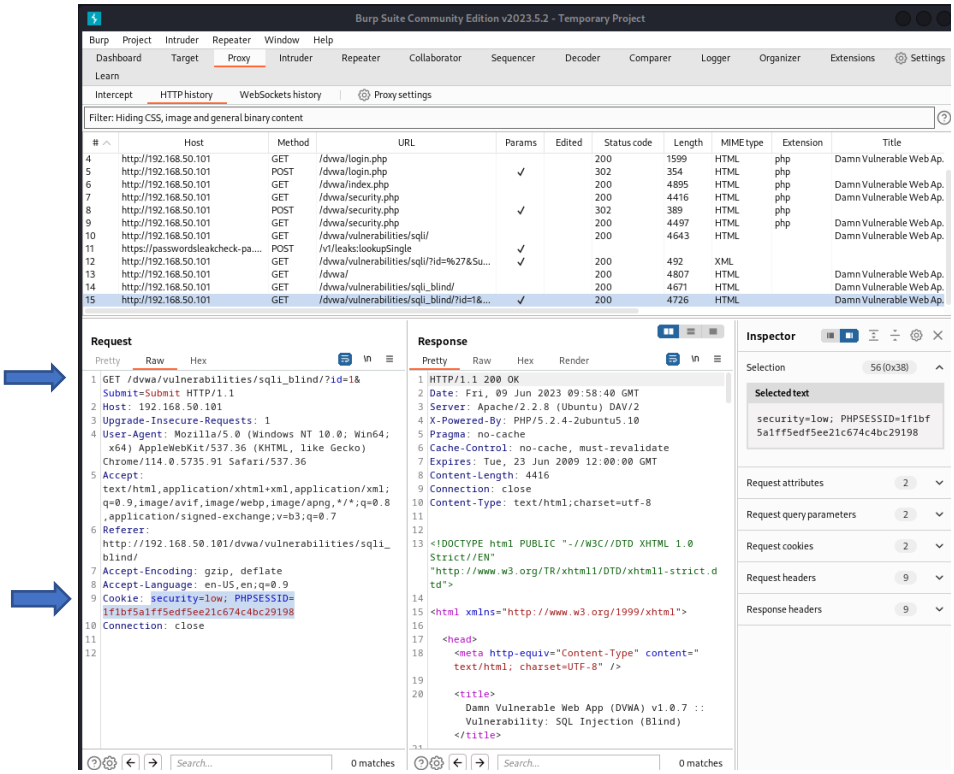
SQL injection (blind)

Lo scopo è quello di recuperare le password degli utenti presenti sul Database, sfruttando la SQLi. Come primo passo, apro Burpsuite per intercettare tutte le richieste così da prendere tutte le informazioni che mi servono. Per svolgere l'esercizio, ho approfondito le conoscenze sul tool di kali **sqlmap**, che permette di automatizzare il rivelamento e lo sfruttamento di difetti nelle SQL injection e prendere così il controllo del server DBMS.

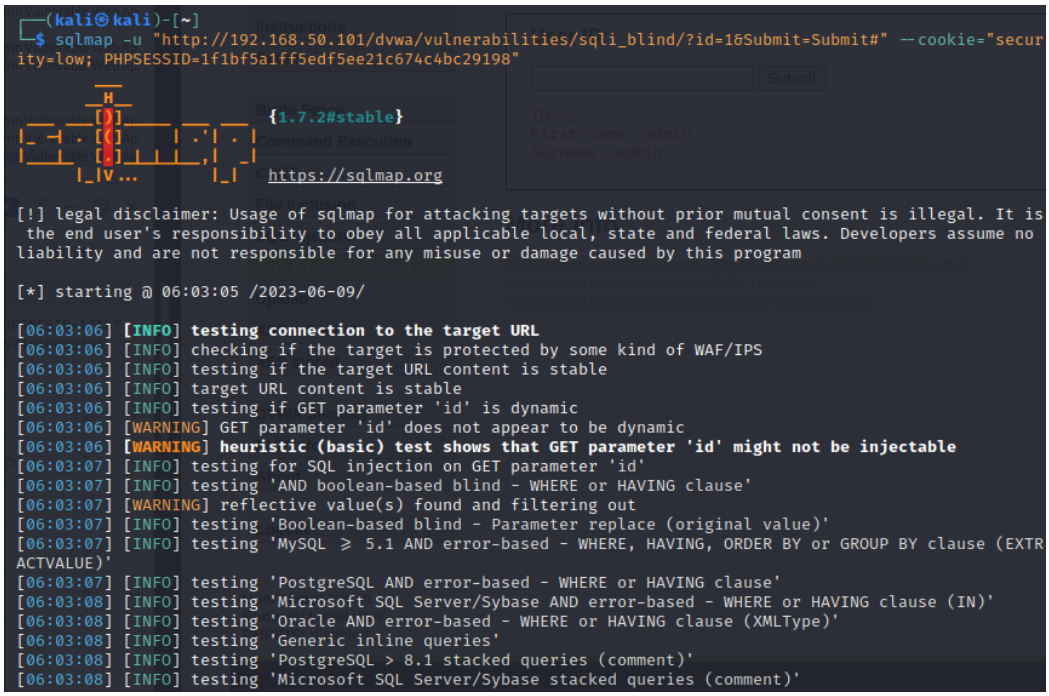
Trovandomi sulla schermata di DVWA, inserisco un numero id casuale, in questo caso 1, così da poter intercettare la richiesta con Burp.

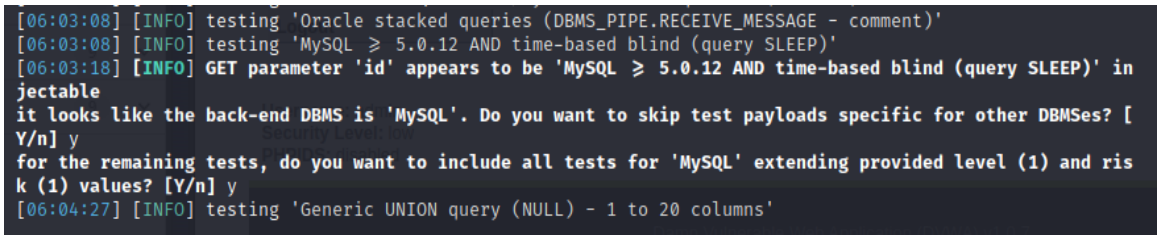


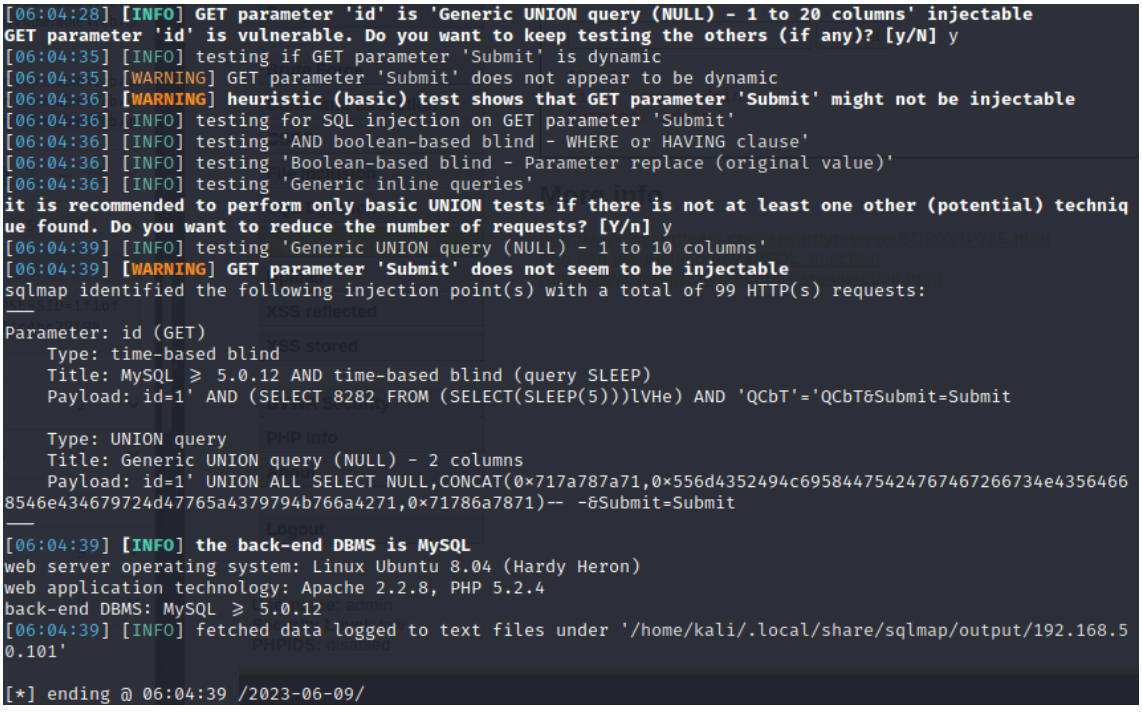
Ora andando su Burp e prendendo l'ultima richiesta fatta, possiamo vedere le informazioni per procedere con il tool sqlmap. In questo caso andiamo a prendere l'URL e il cookie.



Vado sulla shell di kali e digito il comando **sqlmap** seguito da **-u** (che sta ad indicare url) dopo l'url inserisco la stringa di cookie catturata da Burp, preceduta da **–cookie.**



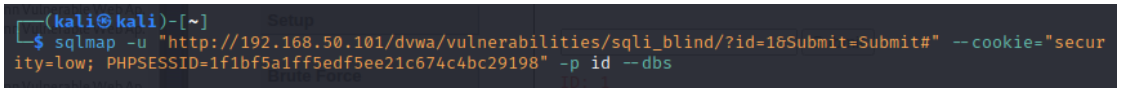


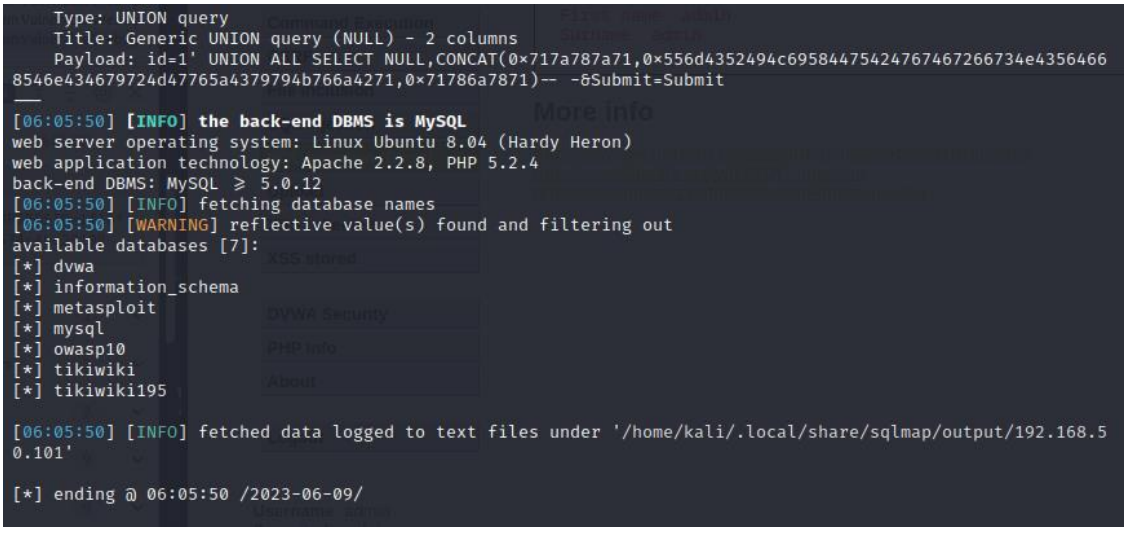


Questa schermata ci mostra tutte le vulnerabilità, come si può leggere , la vulnerabilità sta nel parametro **GET 'id'.**

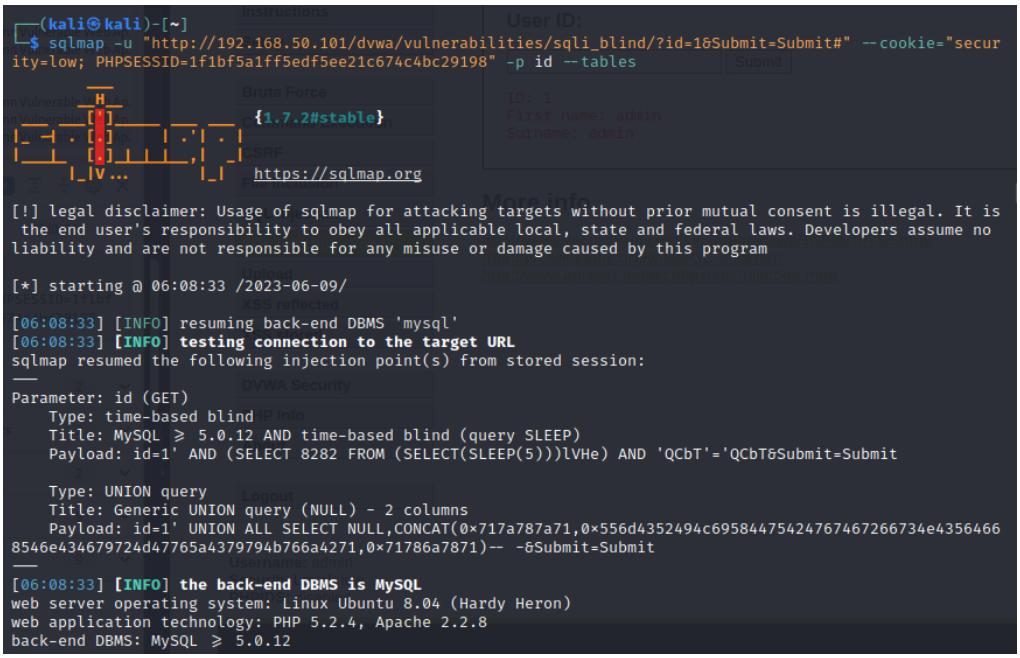
Successivamente vado ad aggiungere uno switch, all'url e al cookie. **-p id** che sarebbe il parametro vulnerabile. Questo parametro mi dice che c'è un database, e mi dice tutte le info correlate. Inoltre mi riporta tutti i payload che sono stati efficaci nella ricerca dell'injection.

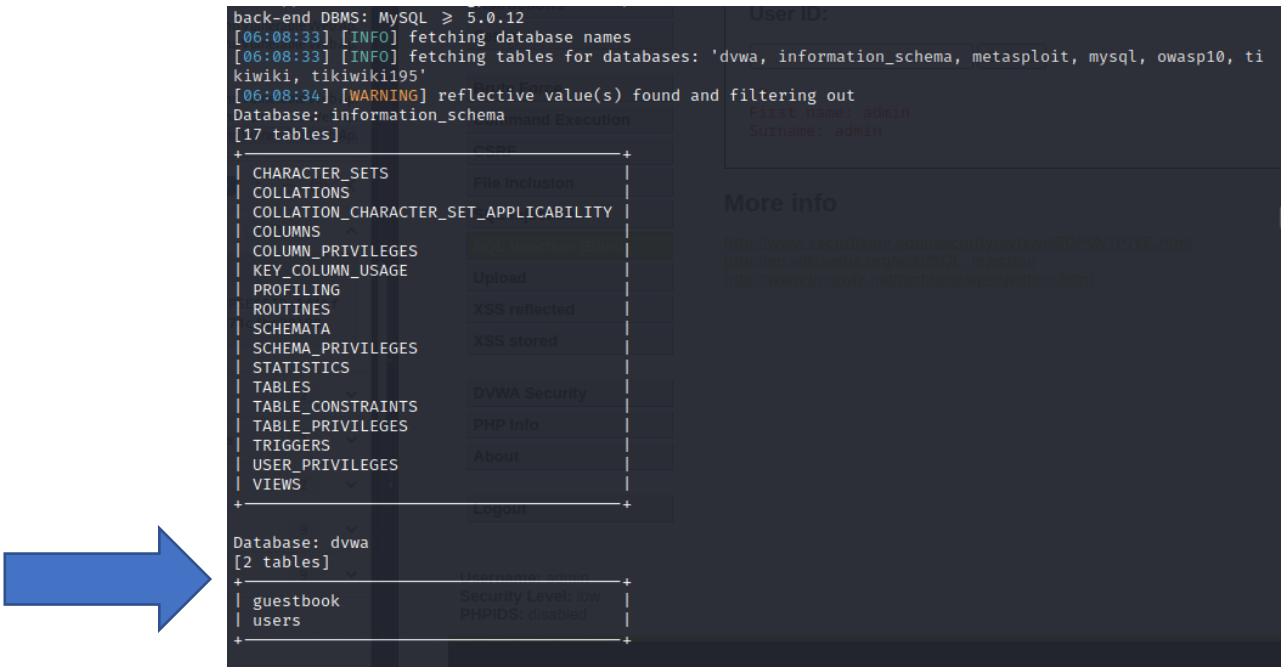
Vado poi a richiamare il database, con lo switch **–dbs** e mi mostra tutti i database disponibili, in questo caso 7, tra cui DVWA.



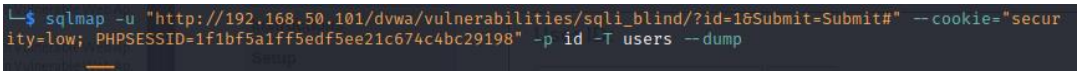


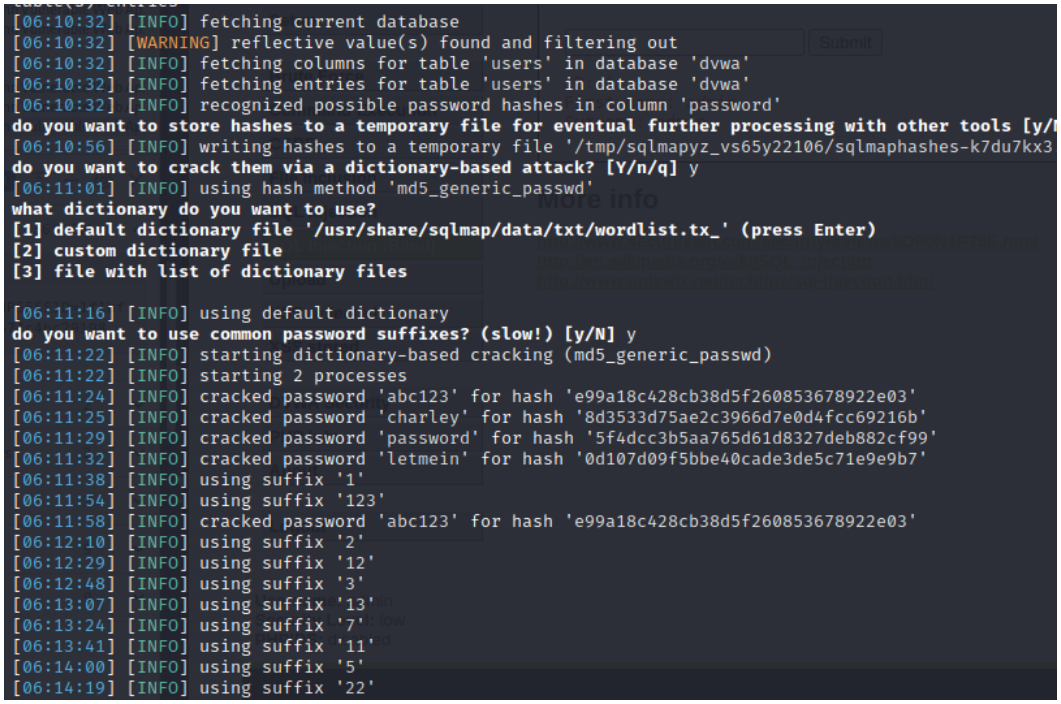
Successivamente aggiungendo lo switch **–tables ,** il tool mi manda a schermo tutte le tabelle disponibili, tra i quali il database DVWA con due tabelle, guestbook e users.

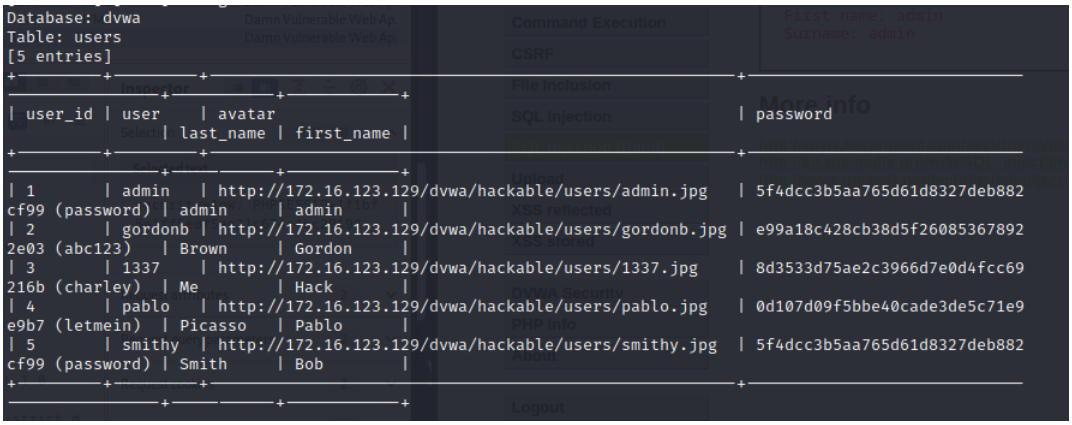




Il passo successivo è quello di estrapolare solo la tabella users, per fare ciò uso lo switch **-T users –dump.** Lo switch dump serve proprio per estrapolare tutti i dati dalla tabella. Durante l'esecuzione del programma, il tool chiede se vogliamo salvare le hash trovate e successivamente ci chiede se vogliamo fare un attacco a dizionario decriptandole. Io ho scelto di far fare tutto al tool automatizzato. Infatti nelle foto che seguono, si possono vedere le fasi di cracking delle password e la tabella finale del database.



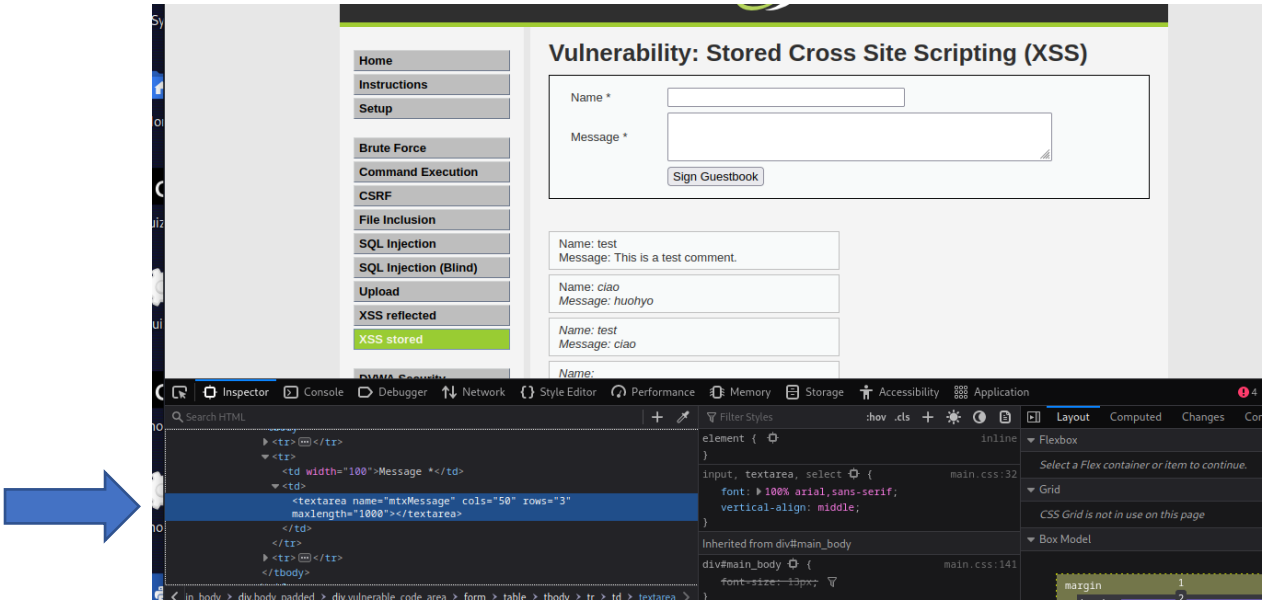




Tramite l'utilizzo di sqlmap, son riuscito a prendere tutte le password della tabella users e con lo stesso utilizzo, le password sono state craccate in breve tempo.

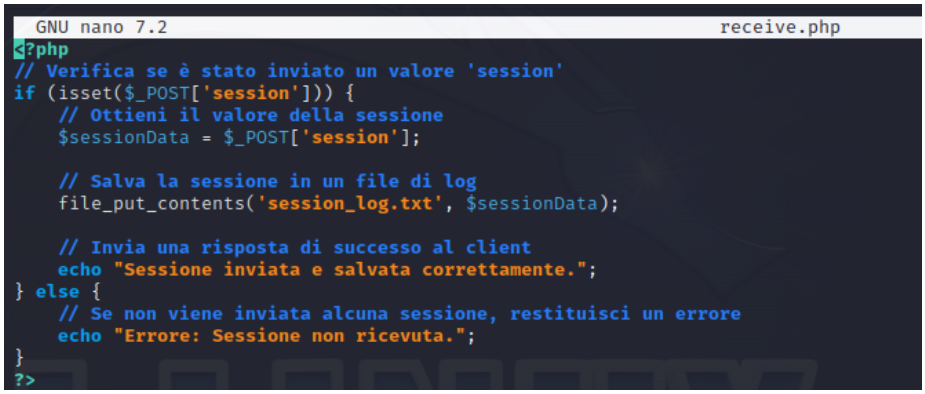
XSS stored

L'esercizio ci chiede di recuperare i cookie di sessione delle vittime del XSS stored ed inviarli ad un server. Come prima cosa va risolto il problema dei caratteri massimi sull'input "message", portandolo da 50 a 1000.

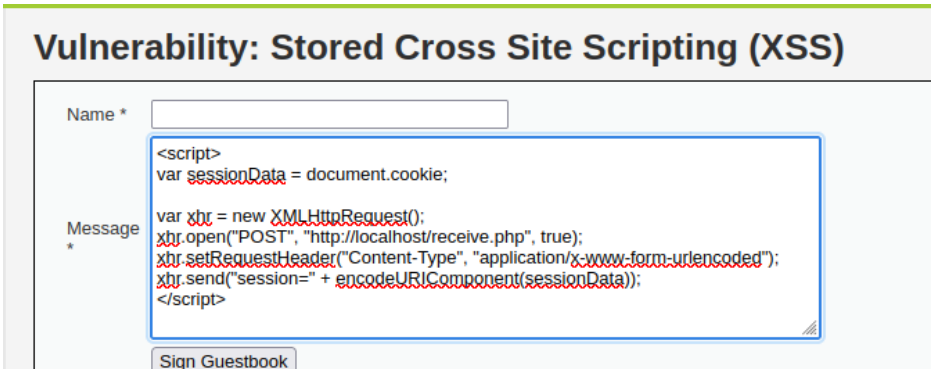


Successivamente avvio il server **apache 2 e mysql** da shell.

Con Cd mi sposto in **/var/www/html/** e creo due file "receive.php" e un "session_log.txt" dove in quest'ultimo dovrebbe esser scritta la sessione importata dall'input di dvwa. Cambio i privilegi del file per permettere la scrittura nel file con **chmod** e mi sposto nel file php dove inserisco un codice reperito su internet per permettere la scrittura della sessione nella cartella "session_log.txt".



Mi sposto sull'input di dvwa e inserisco uno script che prende il cookie e lo manda in localhost/receive.php, il quale successivamente dovrebbe scriverlo in session_log.txt.



Cambiando i privilegi di scrittura, mi scrive la sessione, nel file apposito.