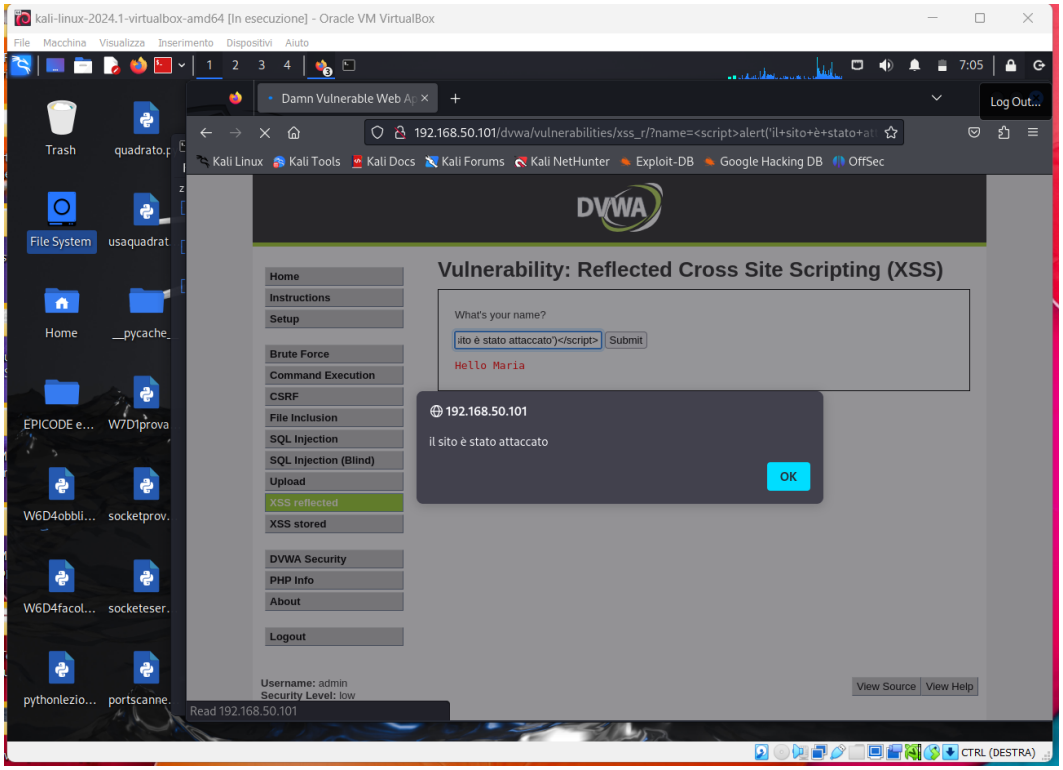
W13D4 – XSS reflected ed SQL injection.

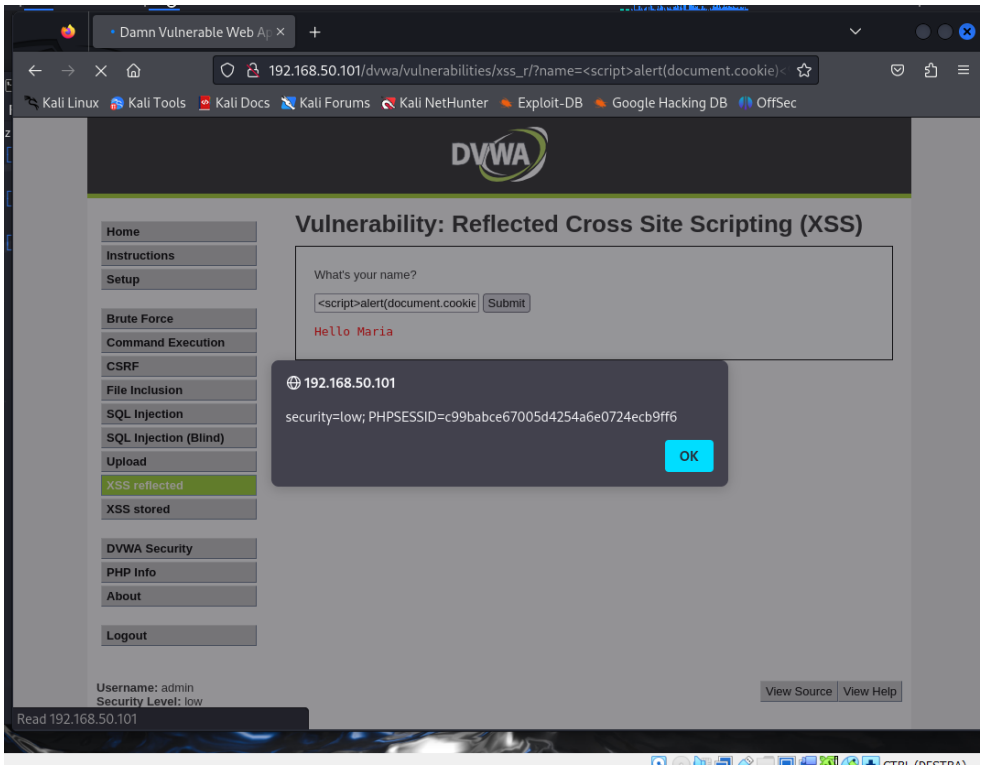
Esercizio obbligatorio

XSS reflected.

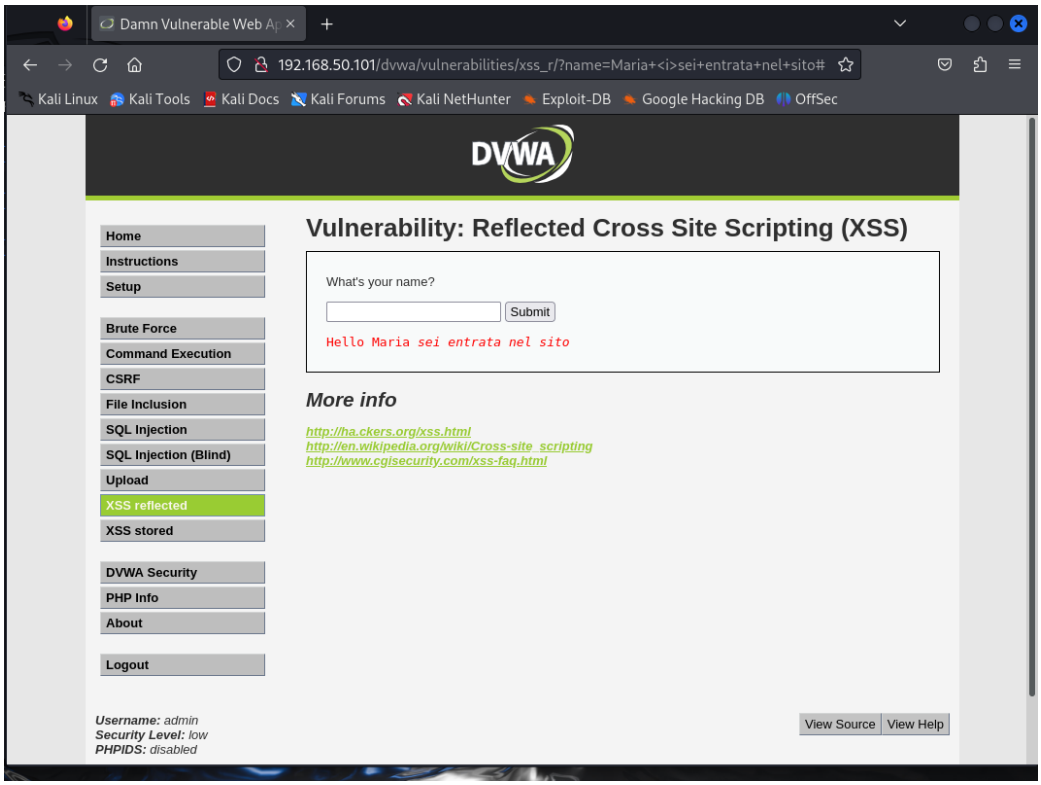
Sono entrata nella DVWA di Metasploitable 2, come si vede dall'IP di Metasploitable nell'URL della pagina ed ho provato a sfruttare la vulnerabilità XSS reflected in vari modi. Per prima cosa, ho inserito un messaggio di alert con la sintassi <script>alert(‘il sito è stato attaccato’)</script>. Ho ottenuto un messaggio di alert come previsto.



Successivamente ho cercato di ottenere informazioni riguardo ai cookie di sessione con <script>alert(document.cookie)</script> ed ho ricevuto un messaggio con PHPSESSID.

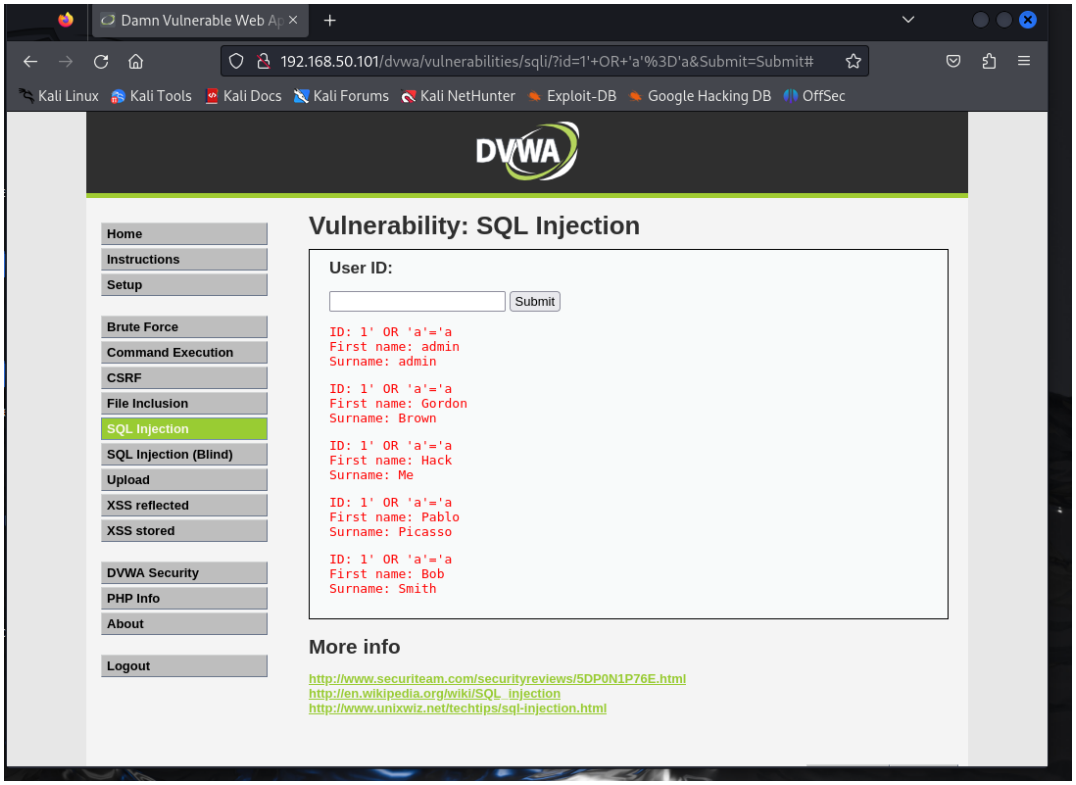


Infine ho provato a vedere l'output in corsivo con <i>stringa ed ho verificato che il comando funziona correttamente.

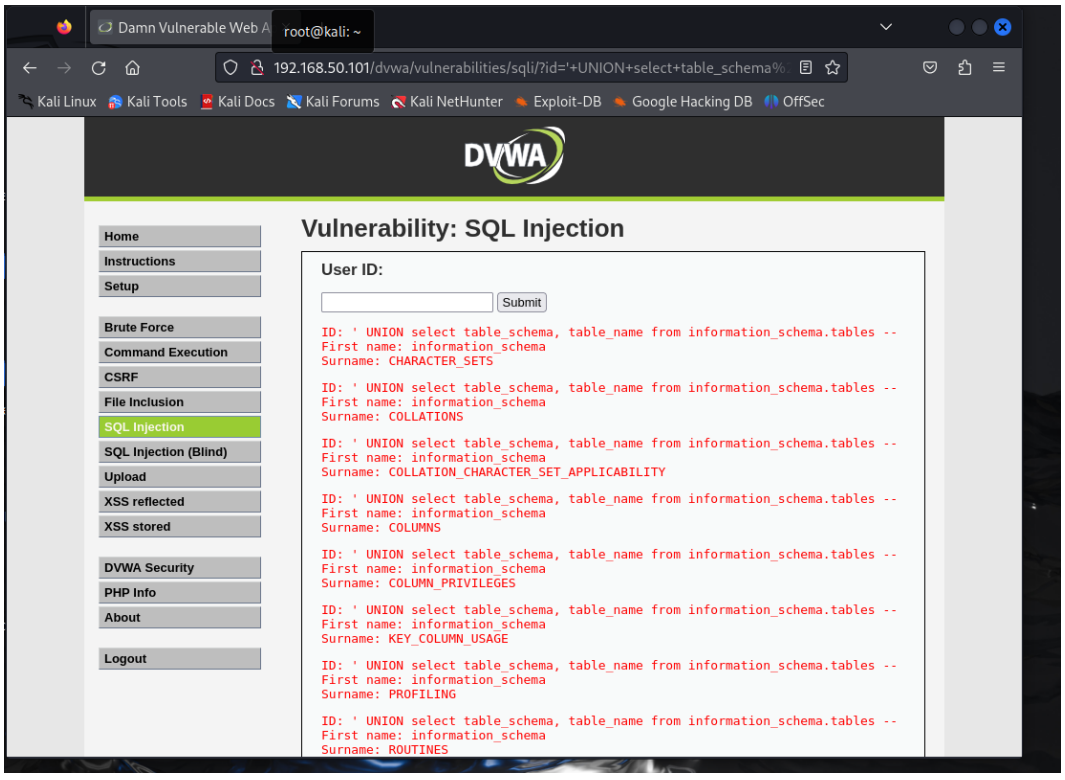


SQL injection

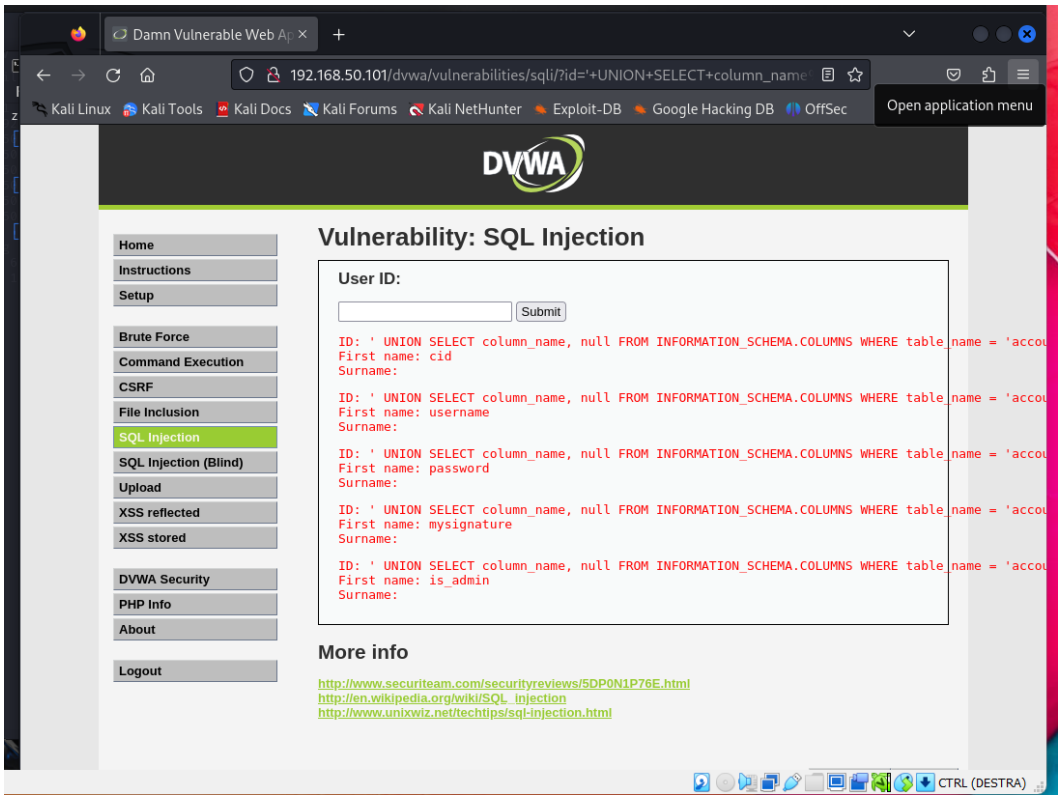
Per prima cosa, ho fatto un controllo di injection eseguendo la query 1' OR 'a'='a, verificando l'injection point e la risposta del database.



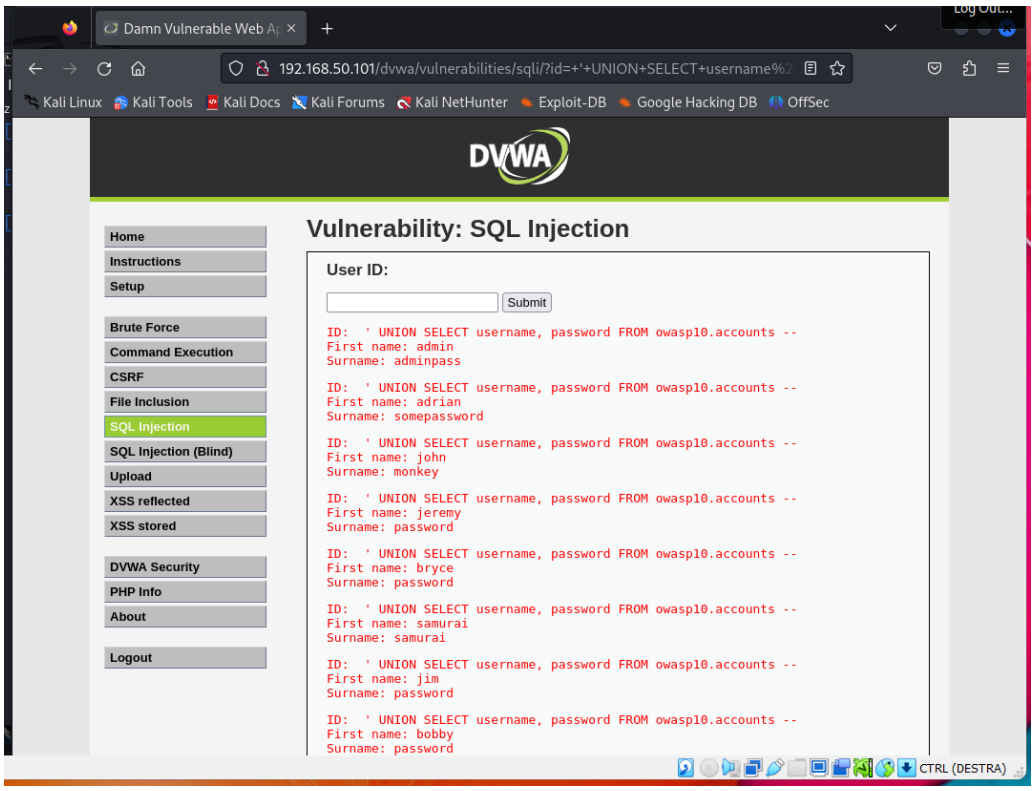
A questo punto ho cercato tutte le possibili tabelle e database alla ricerca di dati interessanti ed ho usato la seguente query ' UNION select table_schema, table_name from information_schema.tables --.



Ho individuato una tabella interessante, "accounts" ed ho eseguito la query ' UNION SELECT column_name, null FROM INFORMATION_SCHEMA.COLUMNS WHERE table_name = 'accounts' – per vedere tutte le colonne di questa tabella.



Infine, per vedere tutte le informazioni della tabella ho eseguito la query ' UNION SELECT username, password FROM owasp10.accounts – per vedere username e password.



Esercizio facoltativo.

XSS reflected

Questo è l'output di <i>molto bene! scritto in corsivo, con il livello di difficoltà settato su "medium".