**Cosa è SQL**

SQL è un linguaggio utilizzato per gestire i database. Esso permette, ad un utente, di poter interagire con lo stesso permettendogli di eseguire diversi tipi di azioni.

Questi database, naturalmente, non sono invulnerabili. È possibile infatti utilizzare un attacco SQL Injection per andare a prendere il controllo sui determinati SQL di una determinata Web App.

Noi, per esempio, utilizzeremo la pagina DVWA per effettuare un attacco. Nella sezione relativa a SQL Injection, nella casella è possibile inserire un dato e ci verrà fornito un risultato corrispondente a quel dato in quanto SQL ha un database di informazioni.

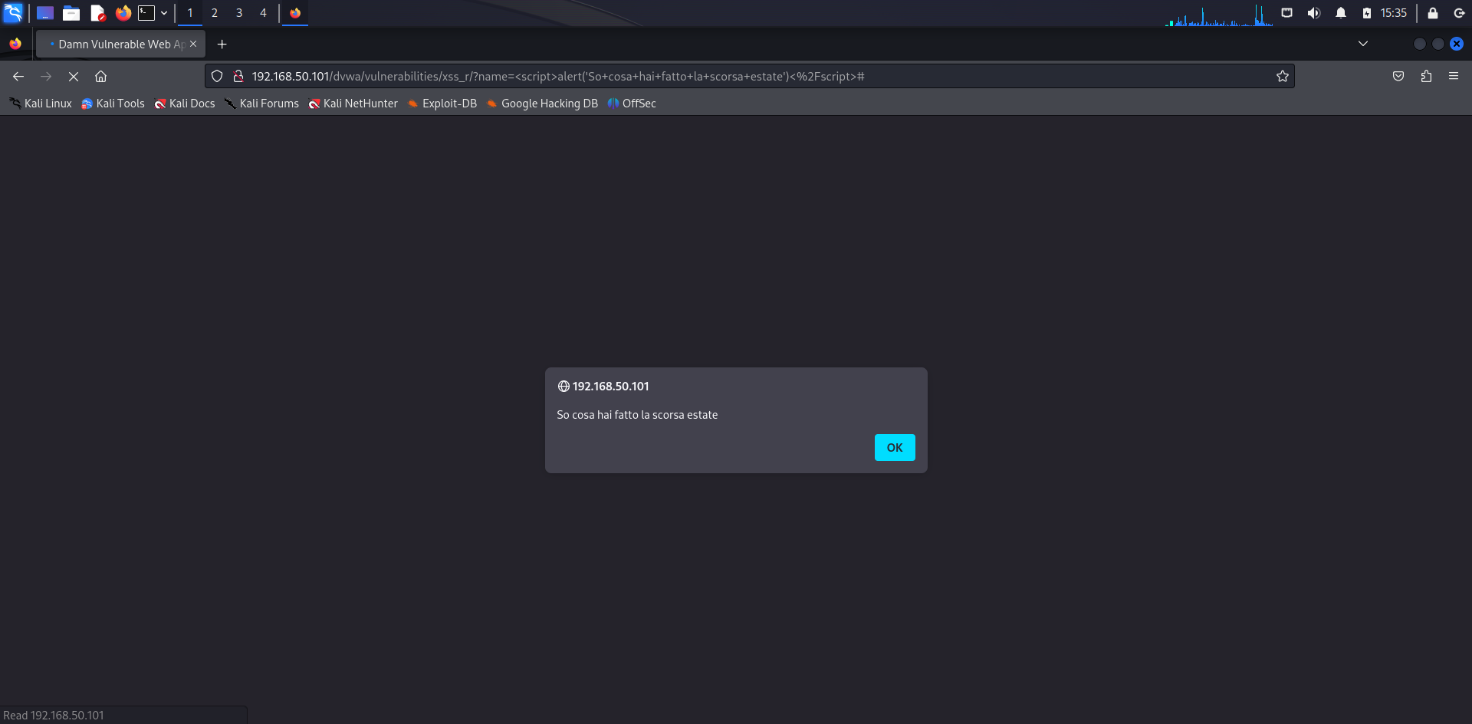
Utilizzando questa stringa %’ or ‘1’=’1 il database ci ritornerà tutte le informazioni presenti al suo interno.



Questo sarà il risultato dell’attacco.

**ATTACCHI XSS**

Un altro gruppo di vulnerabilità potenzialmente sfruttabili da un attaccante sono le XSS. Un attacco XSS serve ad un attaccante immettere all’interno di un sito web contenuti malevoli o script dannosi per l’utente. Tali contenuti dannosi possono “rubare” informazioni riguardante l’utente visitatore del sito, come credenziali di login o addirittura cookie di sessioni, oltre a poter diffondere malware. Questo è possibile poiché alcune pagine web non applicano i corretti controlli di sicurezza (dati forniti da fonti esterne che vengono approvati senza alcun controllo, per esempio). Un esempio di attacco XSS, è quello reflected. In questo caso, l’attaccante può inviare il contenuto malevolo attraverso una URL, ad esempio. Una volta che l’utente cliccherà su tale URL, il contenuto verrà eseguito immediatamente.

[](file:///C:\Users\Utente\Pictures\XSS%20Reflected.png)