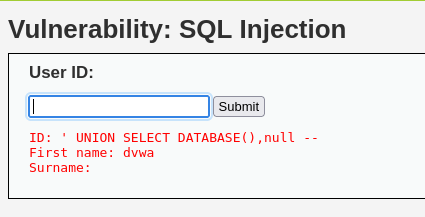
**SQL Injection**

Come prima cosa impostiamo la security a LOW

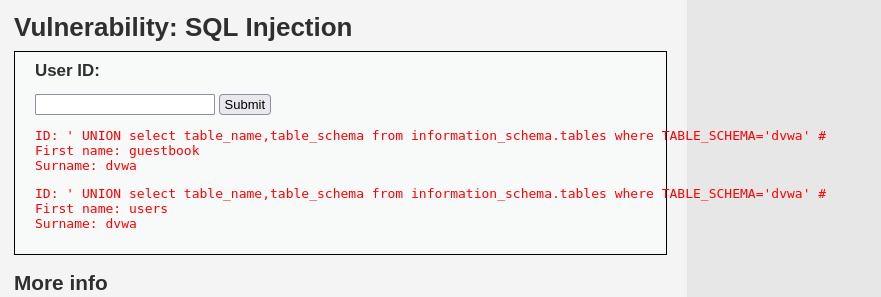
e recuperiamo il nome del database tramite la segente query :

**' UNION SELECT DATABASE(),null #**

E ritorna come risultato il nostro db : **dvwa**

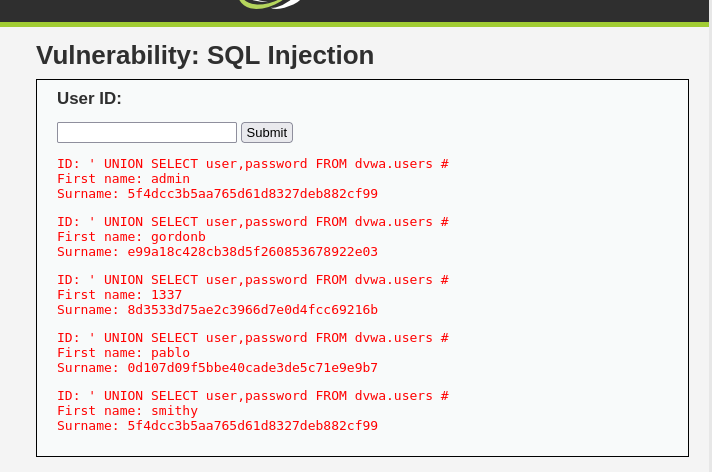


Grazie a questo possiamo navigare più in profondità nel database e quindi scoprire che tabelle ci sono all’interno del database sotto lo schema dvwa tramite il comando  
**' UNION select table\_name,table\_schema from information\_schema.tables where TABLE\_SCHEMA='dvwa' #**

E scopriamo 2 tabelle : guestbook e users.  


Possiamo entrare ancora più a fondo per scoprire quali user sono registrati all’interno del database interrogando con la seguente SQL Injection:

**' UNION SELECT user,password FROM dvwa.users #**

****

XSS Reflected

è una vulnerabilità di sicurezza che si verifica quando un'applicazione web non riesce a validare correttamente i dati inseriti dagli utenti, permettendo l'inserimento di codice malevolo (tipicamente JavaScript) che viene eseguito direttamente nel browser della vittima.

Come in questo caso tramite il tag <script> possiamo far comparire un alert non presente all’interno del javascript

**<script>alert('XSS!')</script>**

