**SQL Injection Attack- Task 2**

Completed by Eric Adamian

VirtualBox IP address:

|  |  |
| --- | --- |
| Virtual machine: | sqlVM |
| IP address: | 10.0.2.15 |

**Task 2: SQL Injection Attack on SELECT Statement**

Explanation: Understanding the SQL Injection Attack various pages and logging in to view data

**Task 2.1: SQL Injection Attack from webpage.**

**Step 1:** Login into www.SeedLabSQLInjection.com using the admin account with credentials **admin’ #** for the username (no password input)

A screenshot of a cell phone

Description automatically generatedA screenshot of a computer screen

Description automatically generated

**Observation: Successfully logged in as admin**, as data shown for all usernames is available

**Task 2.2: SQL Injection Attack from command line**

**Step 2:** In order to login to SQL Injection Attack from the command line, curl will be used to log in as admin

A screenshot of a cell phone

Description automatically generatedA screenshot of a cell phone

Description automatically generated

**Step 3:** Ensure this is correct login by checking for similar data as the website

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

**Observation: Successfully logged in as admin**, as data shown for all usernames is available through the command line

**Task 2.3: Append a new SQL statement**

**Step 4:** Go back to www.SeedLabSQLInjection.com and attempt to modify database through the username login

**Step 5:** In order to do so, the following command will be used: **‘or 1=1; update credential set Salary = ‘5000’ where Username=‘Alice’;#**

A screenshot of a computer

Description automatically generated

**Observation:**  An error resulted from this statement (attack was not successful); the PHP code for user authentication does not allow multiple queries for this case