**Lab Report**

**Lab Completed:** Netlab - SQL Injection

**Objective:** Complete the lab presented. Using your textbook, the written lab, and the hands-on activity, use the lab report to demonstrate understanding of the concept presented.

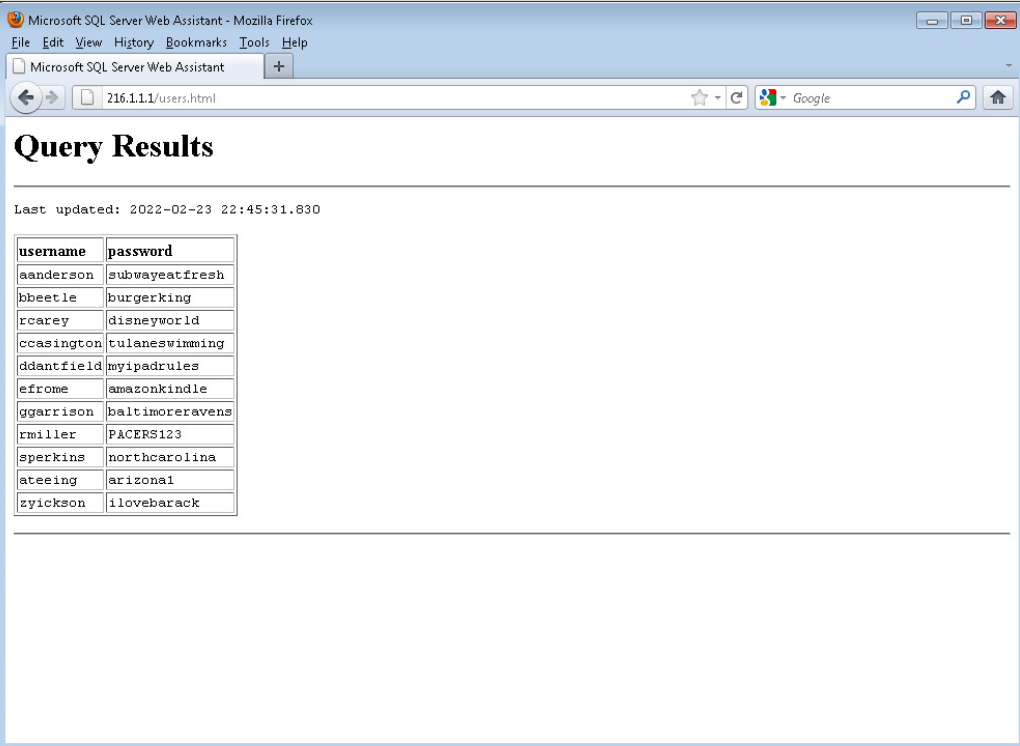
**Part 1: Lab Activity**

Directions: Complete the lab assigned in Netlab. Take 2 screenshots (or more) that demonstrate completion of the lab. Answer the following:

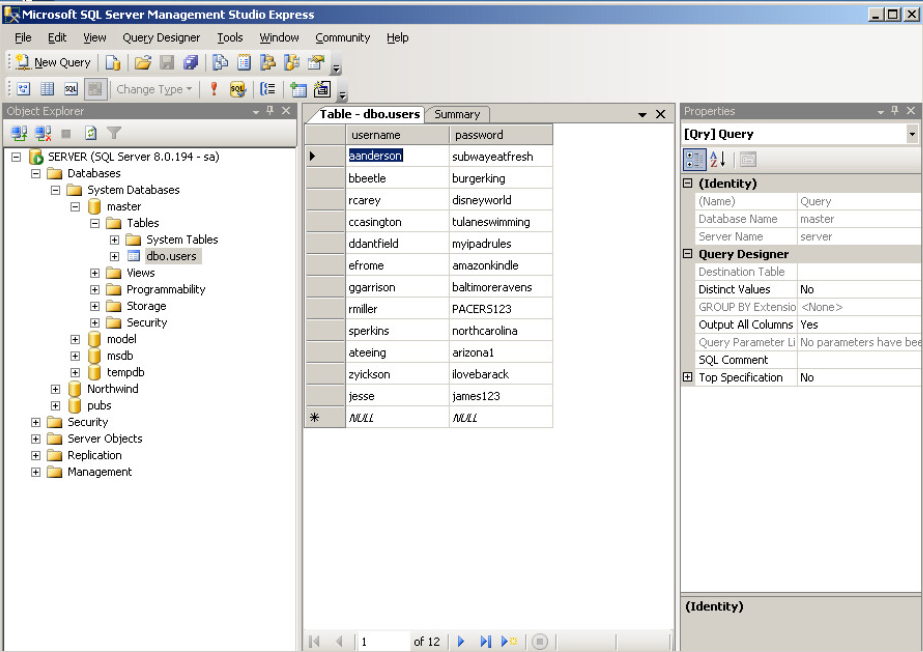
**Q1:** Provide a synthesis of the activity you completed in your own words.

In this lab we tested our SQL Injection privileges on a webserver with an SQL backend. Once learning that we could successfully inject SQL statements, we obtained a full list of usernames and passwords, created ourselves a new account in the SQL database, and then used the stored procedure xp\_cmd shell to download a malicious Poison Ivy payload with the ftp command and executed it to get the victim to connect to our Poison Ivy Client.

**Q2:** Provide 2 screenshots that demonstrate lab completion. For each screenshot, include 1-2 sentences explaining what the screenshot is demonstrating.



This was the first successful SQL injection that allowed us to grab the SQL table containing username and password combinations.



This is a screenshot of the sql database table for users that shows our newly created user (by injection) and the corresponding password for this user.

**Part 2: Critical Thinking**

**Directions**: Complete the following questions. Provide an explanation of your reasoning for each answer.

The answers should address the lab you just completed.

Suggested length for Part 2: 1-2 pages

**Q1**: What vulnerability(s) are demonstrated or found in this lab? Vulnerabilities may occur during the lab as part of the lab activity.

The input for this server is not validate server-side, which allowed us to simply disable the client-side javascript that does this job.

**Q2:** How might this (these) attack(s) be utilized during a penetration test?

They could be utilized to grab a wealth of information form the database or insert information (such as login information) into the database. The xp\_cmd shell attack could be used to execute any number of commands on the machine hosting the database.

**Q3:** Explain your reasoning as to what phase of the attacker methodology this lab falls under.

I think these could fall into infiltration/escalation, exfiltration, and access extension. With our initial sql injections we are infiltrating the web server by sending SQL statements that create an account for ourselves. In our initial sql injections we also exfiltrate information such as the users database table. We extend our access in two ways; with the malicious poison ivy payload and with the newly created user account that we can now use to log into the server.

**Q4:** Research how the attack(s) in this lab can be mitigated or prevented. Cite any sources used. (APA)

The primary way to mitigate this type of attack would be server-side input validation. One could create a class represented in server-side code that declares what kind of input can be accepted, processed, and stored in the SQL database. This would also help mitigate use of the xp\_cmd shell.

**Q5:** What ethical or potentially problematic issues should a penetration tester consider if they plan on implementing this (these) attack(s) by exploiting a vulnerability?

In this case, I feel like alot could go wrong. You are injecting SQL statements, and if you mistype even one character or mix us key words you could erase a column, drop a table, or possibly drop an entire database. I have dropped an entire production database in the past, and while I was able to restore it within 15 minutes, we lost order data for 3 days (days since the last backup) and I had to fix this manually over the span of a week which did end up costing us some money.