

Lab 8.8.11 Red Teaming: SQL Injection Attack

From TestOut CompTIA Security+ Course

In this lab I will conduct a SQL Injection attack as a hypothetical pentester on a Corporate Bank's Banking Web App.

The scenario for this lab is as follows:

"Your name is Blake Jackson. You are the penetration tester for a small corporate network. After performing several SQL injection attract tests on the corporate network, you have decided to see how secure your own online bank's web page is.

In this lab, your task is to perform a simple SQL injection attack using the following information:

- Your bank's URL: MySecureOnlineBank.com
- Make an account query using your account number: 90342
- Answer Question 1.
 - What is Blake Johnson's account balance ?
- Perform a simple SQL attack using: 0 OR 1=1
- Use the entire statement of "0 OR 1=1" but without quotes.
- Answer Question 2.
 - What is the balance of Nisha Dickson?"

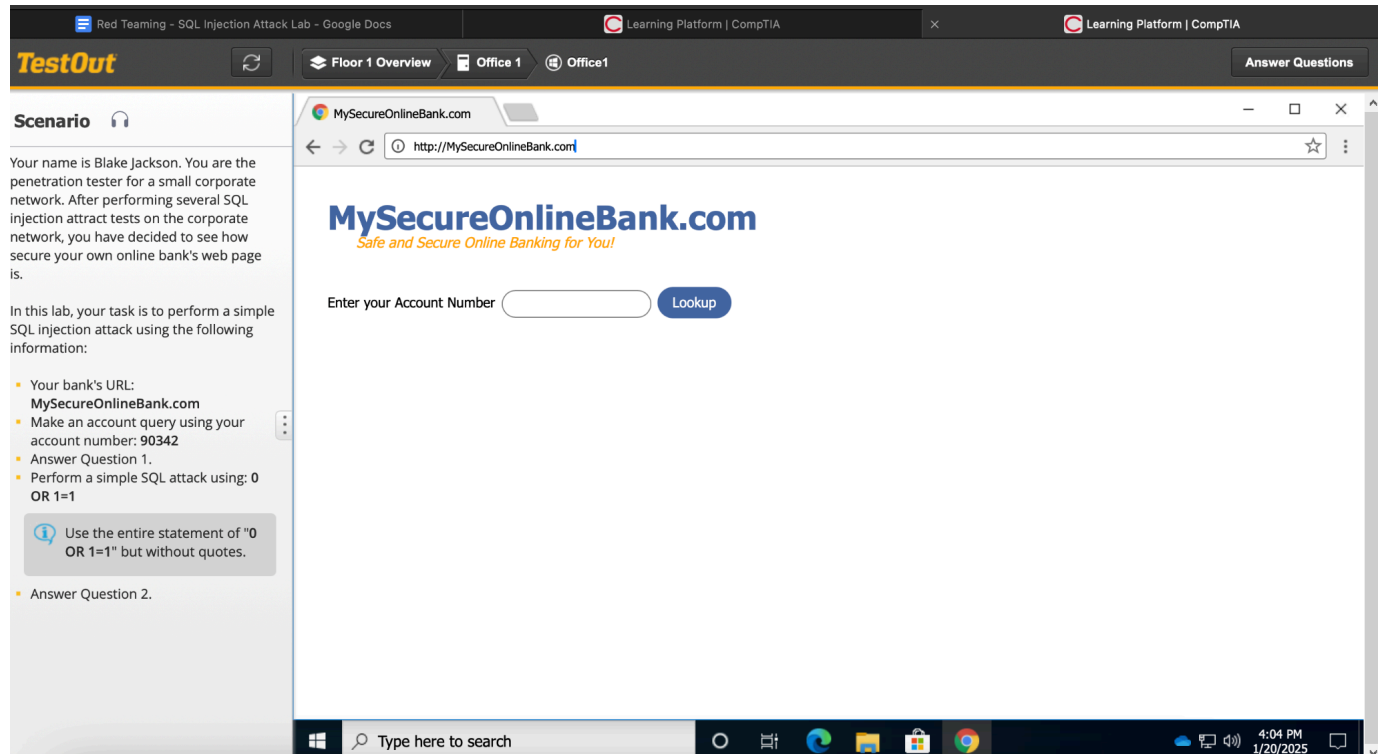
For this Lab, an isolated virtual environment is available to me. No Laws were broken or crime committed against an actual Financial Institution.

With that disclosed , I will open my Web Browser and head to the website www.MySecureOnlineBank.com to take a look around and see if there's any forms present that I might be able to inject SQL into.

Robert Carpenter

github.com/robertmcarpenter

Mon January 20th 2025



I can see that there is a field for users to input their account number in order to lookup their details. I'm assuming on the backend, the Web App will take the User's input and query the database to fetch the details. Since the Lab says I am a theoretical employee of this Bank , I also have a bank account setup for myself (Blake Johnson). Following the lab's instruction:

- **Make an account query using your account number: 90342**
- **Answer Question 1.**
 - **What is Blake Johnson's account balance ?**

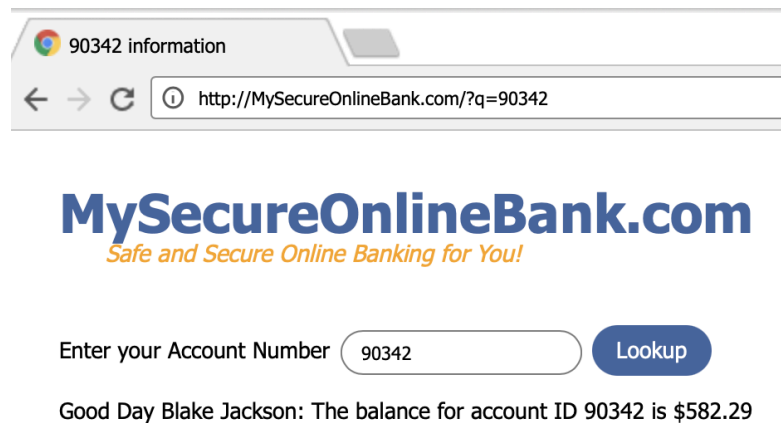
I will enter the number 90342 into the **Lookup** field.

Robert Carpenter
github.com/robertmcarpenter
Mon January 20th 2025



A screenshot of a web browser showing the MySecureOnlineBank.com login page. The browser's address bar displays 'http://MySecureOnlineBank.com'. The page features the bank's logo and tagline 'Safe and Secure Online Banking for You!'. Below this, there is a form with the label 'Enter your Account Number' and a text input field containing '90342'. To the right of the input field is a blue button labeled 'Lookup'.

After hitting **Lookup** I can see the following balance is shown:



A screenshot of the same web browser showing the result of the account lookup. The browser's address bar now displays 'http://MySecureOnlineBank.com/?q=90342'. The page content is identical to the previous screenshot, but the 'Lookup' button is now disabled. Below the form, a message reads: 'Good Day Blake Jackson: The balance for account ID 90342 is \$582.29'.

Since I know this form is working , I can conduct a very simple SQL Injection attack to see what I can find. I'll input **0 OR 1=1** and see what happens.



A screenshot of the web browser showing the account lookup page with a SQL injection payload. The browser's address bar displays 'http://MySecureOnlineBank.com/?q=90342'. The form label 'Enter your Account Number' is present, and the text input field now contains '0 OR 1=1'. The blue 'Lookup' button remains. Below the form, the same message is displayed: 'Good Day Blake Jackson: The balance for account ID 90342 is \$582.29'.

And now, I get every hacker's favorite thing; getting that dopamine rush when your attack was successful! The **0 OR 1=1** statement was injected as SQL code to the backend database and returned **ALL** of the user's balances in this bank's database:

The screenshot shows a web browser window with the URL `http://MySecureOnlineBank.com/?q=0%20OR%201%3D1`. The page title is "MySecureOnlineBank.com" with the tagline "Safe and Secure Online Banking for You!". The main content area displays a list of account balances for all users, including Blake Johnson with a balance of \$582.29 and Nisha Dickson with a balance of \$289.00. The left sidebar shows the lab instructions and the injected SQL statement "0 OR 1=1".

Scenario

Your name is Blake Jackson. You are the penetration tester for a small corporate network. After performing several SQL injection attract tests on the corporate network, you have decided to see how secure your own online bank's web page is.

In this lab, your task is to perform a simple SQL injection attack using the following information:

- Your bank's URL: **MySecureOnlineBank.com**
- Make an account query using your account number: **90342**
- Answer Question 1.
- Perform a simple SQL attack using: **0 OR 1=1**

Use the entire statement of "0 OR 1=1" but without quotes.

Answer Question 2.

0 OR 1=1 Information

Enter your Account Number

Good Day Ben Baird: The balance for account ID 90001 is \$16,519.00
Good Day Drew Manning: The balance for account ID 90002 is \$11,186.00
Good Day Nisha Dickson: The balance for account ID 90003 is \$289.00
Good Day Corrie Long: The balance for account ID 90004 is \$11,875.00
Good Day Zoya Franco: The balance for account ID 90005 is \$18,876.00
Good Day Ocean Padilla: The balance for account ID 90006 is \$3,326.00
Good Day Brittany Decker: The balance for account ID 90007 is \$17,589.00
Good Day Shea McDonald: The balance for account ID 90008 is \$3,999.00
Good Day Harmony Gamble: The balance for account ID 90009 is \$12,152.00
Good Day Janelle Monaghan: The balance for account ID 90010 is \$15,340.00
Good Day Josef Mathis: The balance for account ID 90011 is \$17,172.00
Good Day Kalra Ford: The balance for account ID 90012 is \$10,471.00
Good Day Rhiann Barton: The balance for account ID 90013 is \$145.00
Good Day Nelly Britt: The balance for account ID 90014 is \$7,154.00
Good Day Hamish Riggs: The balance for account ID 90015 is \$7,783.00
Good Day Samiha Mendoza: The balance for account ID 90016 is \$8,260.00
Good Day Dotty O'Brien: The balance for account ID 90017 is \$17,606.00
Good Day Elinor Cooper: The balance for account ID 90018 is \$7,628.00
Good Day Bjorn Pratt: The balance for account ID 90019 is \$10,587.00
Good Day Aila Harris: The balance for account ID 90020 is \$821.00
Good Day Agnes Mercado: The balance for account ID 90021 is \$9,404.00
Good Day Connie Rivers: The balance for account ID 90022 is \$13,475.00
Good Day Shakeel Holder: The balance for account ID 90023 is \$795.00
Good Day Nel Peacock: The balance for account ID 90024 is \$8,173.00

Now that I've conducted the SQL Injection Attack I will answer the 2 questions asked by the lab:

- What is Blake Johnson's account balance ?
- What is the balance of Nisha Dickson?

As I've discovered before, Blake Johnson's balance is **\$582.29**. Scrolling down on the page I can also see Nisha Dickson's balance listed as **\$289.00**.

Now that I've completed all tasks and all questions, this now concludes this Lab.

Robert Carpenter
github.com/robertmcarpenter
Mon January 20th 2025

The screenshot displays a web browser window with a 'Lab Report' modal open. The modal is titled 'Lab Report' and shows a score of 2/2 (100%) and a time spent of 13:45. The report includes a 'TASK SUMMARY' section and 'Lab Questions'.

Lab Questions

- ✓ Q1: What is your account balance?
Your answer: 582.29
Correct answer: \$582.29
- ✓ Q2: What is the account number of Nisha Dickson?
Your answer: 90003

The background shows the 'TestOut' interface for a 'Red Teaming - SQL Injection Attack Lab'. The scenario description states: 'Your name is Blake Jackson. You are the penetration tester for a small corporate network. After performing several SQL injection attack tests on the corporate network, you have decided to see how secure your own online bank's web page is. In this lab, your task is to perform a simple SQL injection attack using the following information:'

- Your bank's URL: MySecureOnlineBank.com
- Make an account query using your account number: 90342
- Answer Question 1.
- Perform a simple SQL attack using: 0 OR 1=1

A tip box indicates: 'Use the entire statement of "0 OR 1=1" but without quotes.'

The bottom of the screen shows a Windows taskbar with the search bar and various application icons. The system clock shows 4:39 PM on 1/20/2025.