(A1) Injection - SQL Injection

# BACKGROUND

Injection is perhaps one of the most recognized and constant vulnerabilities of web applications. Injection attacks are not limited to only web applications, however.

# DESCRIPTION

This exercise will familiarize you with SQL as well as some SQL injection tactics to obtain, change and delete data using injection techniques.

# REQUIREMENTS

A computer that can run Java. Most modern Windows, Linux and MacOS machines can run Java, as can Google Cloud Shell. This exercise assumes you’re running an instance of Linux (either virtualized or other). This exercise will run in Google Cloud Shell. Previous exercises in this chapter walk through the Java and WebGoat installations. A web browser (preferably Chrome).

# PART I: SQL Injection (intro) (Steps 1, 2, 3, 6, 7 and 8)

1. Log into WebGoat
2. From the left navigation bar, select "(A1) Injection"
3. From the left navigation bar, select "SQL Injection (intro)"
4. Click on Step 1 (a gray box) and read an overview of the exercises
5. Click on Step 2 (a red box)
6. Successfully construct a query which obtains the department for Bob Franco

HINT: Your query should return exactly one result; there are several ways to do this
7. Click on Step 3 (a red box)
8. Successfully execute a query which changes the department of "Tobi Barnett" to "Sales"

HINT: You may need to do some reading on the UPDATE command for SQL

HINT: Equality in SQL is expressed with one equal sign (the = character)

HINT: Strings are quoted with SINGLE quotes, not double quotes (the ' character)
9. Click on Step 6 (a gray box) and read the overview for SQL injection attacks
10. Click on Step 7 (a gray box) and read about consequences of a SQL injection attack
11. Click on Step 8 (a gray box) and learn about SQL attack severity

# PART 2: SQL Injection (intro) (Steps 9, 10, 11, 12 and 13)

1. Log into WebGoat
2. From the left navigation bar, select "(A1) Injection"
3. From the left navigation bar, select "SQL Injection (intro)"
4. Click on Step 1 (a gray box) and read an overview of the exercises
5. Click on Step 9 (a red box)
6. Use the SQL builder to successfully execute a SQL injection attack to retrieve all the users from the users table
7. Click on Step 10 (a red box)
8. Use the form to successfully execute a SQL injection attack to retrieve all the data from the users table

HINT: Use your knowledge from Step 9
9. Click on Step 11 (a red box)
10. Use the form to successfully execute a SQL injection attack to retrieve all employee data from the employees table
11. Click on Step 12 (a red box)
12. Use the form to successfully execute a SQL injection attack in order to set your salary

HINT: Step 3 has some information about how to UPDATE data

HINT: Previous steps can be referenced for column names in the database

HINT: Numerical values are not put in quotes when used as values in SQL queries, nor do numerical values contain commas
13. Click on Step 13 (a red box)
14. Use the form to successfully execute an SQL injection attack which removes a table from the database

HINT: The percent sign (the % character) is a wildcard in SQL; try running the query with ONLY the percent sign first

HINT: You may have to research how to DROP a table in SQL

HINT: SQL will stop processing a statement once two consecutive hyphens are encountered (the -- characters)

| EVIDENCE #1 |
| --- |
| **PASTE THE IMAGE OF THE LESSON ("SQL Injection (intro)") AND STEPS 2, 3, 9, 10, 11, 12 AND 13 AS GREEN**  |