**Lab 4**

**Outcome**:

1.This Lab Introduces students to Web Application Security using WebGoat.

2. Students will demo a Network Vulnerability Assessment tool

**Objectives**:

1. Run WebGoat using Docker

2. Complete SQL Injection (Introduction) lesson.

3. Students will demo a Network Vulnerability Assessment tool

**Deliverables:**

One lab report that includes the following:

1. A cover page including -Course title, Lab #, Date, Name and ID…etc.
2. Filled in answer sheets for all parts of the lab.

Contents

[Task 1: Run WebGoat using Docker 2](#_Toc130284971)

[Task 2: Complete Injection Flaws > SQL Injection (Introduction) 3](#_Toc130284972)

[Task 3: Network Configuration Manager tool from SolarWinds 6](#_Toc130284973)

# Task 1: Run WebGoat using Docker

1. Open the terminal on Mac or command prompt on Windows and type:



1. Open WebGoat using the following URL: <http://127.0.0.1:8080/WebGoat>
2. Next, you'll be able to register a new user and get started.

At the left side you can see list of lessons that you can complete with the web goat. Click on introduction, then on WebGoat and read it.

WebGoat is a deliberately insecure web application maintained by OWASP designed to teach web application security lessons.

This program is a demonstration of common server-side application flaws. The exercises are intended to be used by people to learn about application security and penetration testing techniques.

WARNING 1: While running this program your machine will be extremely vulnerable to attack. You should disconnect from the Internet while using this program. WebGoat's default configuration binds to localhost to minimize the exposure.

WARNING 2: This program is for educational purposes only. If you attempt these techniques without authorization, you are very likely to get caught. If you are caught engaging in unauthorized hacking, most companies will fire you. Claiming that you were doing security research will not work as that is the first thing that all hackers claim.

# Task 2: Complete Injection Flaws > SQL Injection (Introduction)

1. After logging in to WebGoat. Browse the lessons that appears on the left side of the page.
2. Expand (A1) Injection and Click on SQL Injection (intro) under Injection Flaws.
3. **Read step 1 and step 2. What is SQL?**
4. **What are the 3 main protection goals in information security?**
5. **At the bottom of the page in step 2, use an SQL query to retrieve the department of the employee Bob Franco. What is the result of your query?**
6. **Proceed to step 3. What is DML?**
7. **In step 3, write the below SQL query to change the department of Tobi Barnett to ‘Sales’. What is the result of your query? Which of the protection goals is being compromised and why?**



1. **Proceed to step 4. How can an attacker use SQL Injection of DDL type?**
2. **In step 4, write an SQL query to modify the scheme by adding the column “phone” (varchar(20)) to the table “employees”. The SQL query will be as follows. What is the result of your query? Which of the protection goals is being compromised and why?Provide a screenshot of the result of your query.**



1. **Proceed to step 5. Write a SQL query to grant the usergroup “UnauthorizedUser” the right to alter tables. The SQL query will be as follows. What is the result of your query? Which of the protection goals is being compromised and why?Provide a screenshot of the result of your query.**



1. **Proceed to step 6. What is an SQL Injection? list three example of what a hacker could supply to the input field to perform actions on the database that go further than just reading the data of a single user.**
2. **In step 6, provide the following input and take a screenshot of the resulting query.**



1. Read through steps 7,8.
2. **Proceed to step 9, complete the SQL injection exercise by Selecting the options from the drop‐down menu to produce the below query. Why does this injection work?**



1. **Proceed to step 10, complete the Numeric SQL injection by entering values in the fields to produce the below query and provide a screenshot of the result.**

Graphical user interface, text, application

Description automatically generated

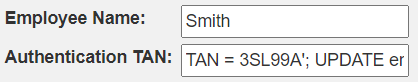


1. **Proceed to step 11 and complete the String SQL injection exercise to compromise the confidentially of data by viewing internal information that you should not have access to. Provide screenshot.**

A picture containing shape

Description automatically generated

1. **Proceed to step 12, complete the String SQL injection exercise to compromise the integrity of data by concatenating strings to it. Enter the following values in the text inputs to retrieve the requested information. Why does the below injection work and what was the result of it.**
   * + - Employee Name: *Smith*
       - Authentication TAN: *TAN = 3SL99A'; UPDATE employees SET salary = 100000 WHERE auth\_tan = '3SL99A*



1. **Proceed to step 13, complete the exercise to delete the access\_log table to compromise the availability of data. Enter the following values in the text inputs to retrieve the requested information. Why does the below injection work and what was the result of it? Provide screenshot**
   * + - Action\_contains: *John'; DROP table access\_log; --*

A picture containing text

Description automatically generated

# Task 3: Network Configuration Manager tool from SolarWinds

SolarWinds Inc. is an American company that develops software for businesses to help manage their networks, systems, and information technology infrastructure. One of the products provided by SolarWinds is “Network Configuration Manager” which is a tool used to Save time and ensure compliance with automated network configuration management and backup. It can also be used for vulnerability assessment to protect a network from malware by integrating with the National Vulnerability Database and access to the most current CVE’s to identify vulnerabilities in your devices.

1. Use your web browser to navigate to the following URL: <https://www.solarwinds.com/network-configuration-manager>
2. Click on the “Interactive demo” button
3. Fill in the required information in the fields and then click on “Proceed to online demo” button
4. Explore the dashboard
5. Click on “My Dashboards” in the top menu to display the drop-down menu. From the drop-down menu that appears, click on “Network Configuration” then on “Config Summary”.
6. When the Config Summary page appears, navigate to the “Firmware Vulnerabilities” section and click on “Show All”.
7. Examine on of the listed vulnerabilities and answer the following questions:
   1. **Provide a screenshot for the listed vulnerabilities.**
   2. **What is the vulnerability ID, provide one example?**
   3. **What is the CVSS Base score, provide the value for the chosen vulnerability?**
   4. **What is the severity level, provide the value for the chosen vulnerability?**
   5. **How many nodes are affected by this vulnerability?**
   6. **What is the vulnerability summary?**
   7. **Are there any available solutions for this vulnerability, list the solution/s?**