Homework 6

1. WebGoat

The WebGoat is a deliberately insecure web application. It helps developers learn about security vulnerabilities first hand by hacking the WebGoat.

a) Download and start the WebGoat
https://github.com/WebGoat/WebGoat
WebGoat should be running on your machine on port 8080
http://localhost:8080/WebGoat/

b) Login using guest account. User:guest Password:guest

Problem 1

Navigate to Injection Flaws > Numeric SQL Injection
The goal is to send a malicious query to the server, which will get it to return all the results instead of just one.

Submit a screenshot of the SQL query and the result of that query.

Problem 2

Navigate to XSS > Stored XSS

Login as a hacker and create a stored XSS that shows a popup showing "You have been hacked by <Group Name>"
Login as a victim and to show the alert message.

Submit a screenshot of the stored XSS code as the hacker and the popup as the victim.

Problem 3

Navigate to XSS > CSRF

Login as a hacker and create an interesting title which includes your group name. In the message, put in a code showing an image whose URL points to the 'attack' servlet with 'Screen', 'menu' and 'transferFunds' as parameters. All parameters are numeric values. After submitting the post, click your message in the Message List.

Submit a screenshot of the code before submission and the result of clicking that post.