# ISEC 400 Lab 4

For this assignment, you will be discovering vulnerabilities in software using an example system that was written in Java. Although the source code language may not be familiar, the concepts and vulnerabilities in the study of application security are the same. This exercise will use WebGoat, an application specifically designed to be vulnerable.

## Getting started

1. Download WebGoat from <https://code.google.com/p/webgoat/downloads/detail?name=WebGoat-5.4-OWASP_Standard_Win32.zip> (note, this is somewhat large because it embeds the Java runtime and a web server)
2. Double-click the “webgoat\_8080.bat” file to launch the web server. You may need to approve the application to communicate on a network.
3. Navigate to <http://localhost:8080/WebGoat/attack> and enter the username and password credentials of “guest” and “guest” respectively. Click the button to launch WebGoat.

## Complete the following lessons

1. Complete the lessons for Cross-Site Scripting (phishing, stored xss, reflected xss, CSRF, etc). Note that you may bypass any of the lessons that require you to fix the flaws since it is likely that Java is not a programming language you know (these are the ones that say “this lesson only works with the developer version of webgoat”).
2. Complete the lessons for Injection Flaws (LAB: SQL Injection only). Note that you may bypass any of the lessons that require you to fix the flaws since it is likely that Java is not a programming language you know (these are the ones that say “this lesson only works with the developer version of webgoat”).
3. Explain what you did for each lesson and take a screen shot of the completed lesson window and paste it into your solution document. A recommended free-for-personal-use screen capture tool is PicPick (<http://www.picpick.org/en/download_free>). This will let you capture just a region of your screen and easily paste the results.

## Submission instructions

Create a properly cited Word and formatted document for your submission. Submit the Word document to the dropbox for the course.