LAB 5: Web Server Script Attacks

WebGoat is a set of intentionally insecure web applications with progressively more difficult CSQL injection vulnerabilities. This lab has a total of 100 points and 10 points of extra credit. You do not have to complete any parts that require the developer installation or fixing the code.

Read more about SQL Injection: https://www.owasp.org/index.php/SQL_Injection

Hint and Solutions for the lab (try your best before looking at the solutions): http://webappsecmovies.sourceforge.net/webgoat/

You can do this lab on the Windows XP VM or on your own computer. If you choose your own computer, you will need to download (and unzip) the appropriate version of Webgoat. Make sure to follow the corresponding Readme file (use the correct version of Java, start/stop WebGoat using the correct commands, and access the webpage at the correct case-sensitive URL). The extra credit is only available on Webgoat 5.3 and later. Webgoat 5.3 is already installed on the Windows XP VM.

On Windows, start WebGoat by double-clicking **webgoat.bat** in the folder **WebGoat-5.3_RC1**. On anything except Windows, start WebGoat by navigating to the unzipped directory and entering the start command (specified in the Readme).

Then wait for the server to start. On Windows, a Tomcat window will open. Everywhere else, the messages will appear in the terminal. The message should end with "INFO: Server startup in [number] ms" when it is ready.

Once it has started, you can then open a web browser and visit the WebGoat page. On Windows, it is http://localhost/webgoat/attack. Note that these URLs are case-sensitive.

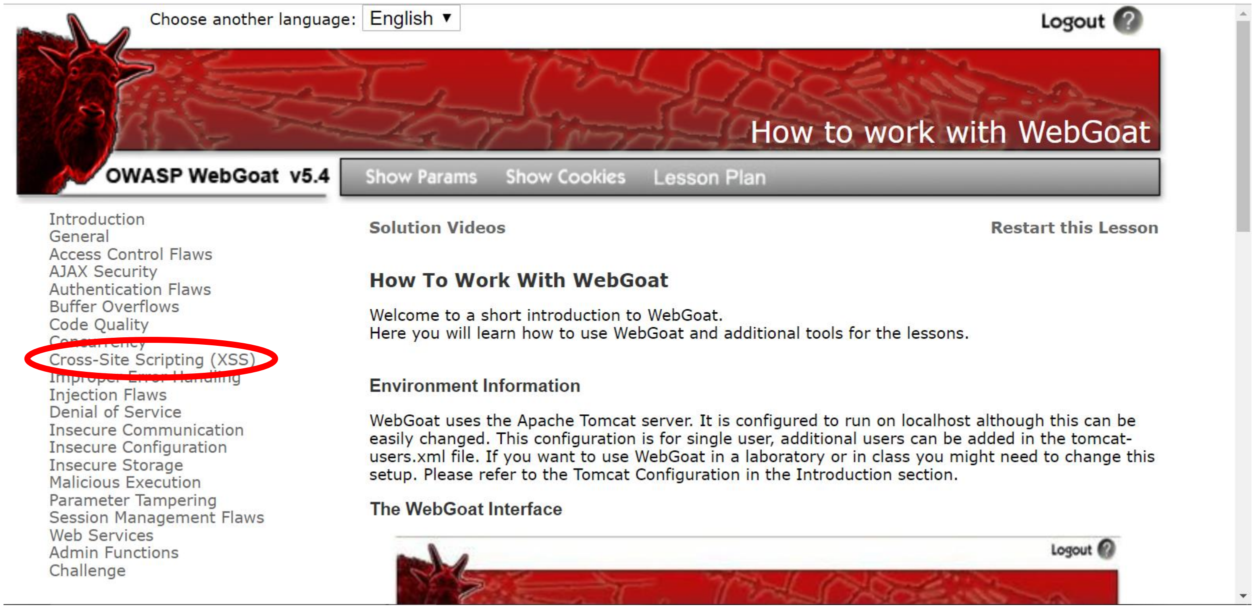
Username: webgoat   Password: webgoat

Click "Start Webgoat" about halfway down the webpage.

Note: When you are done, make sure to stop Webgoat.

1) Cross-Site Scripting (XSS)

To start this part of the lab, click on the Cross-Site Scripting (XSS) tab:



How To Work With WebGoat

Welcome to a short introduction to WebGoat.
Here you will learn how to use WebGoat and additional tools for the lessons.

Environment Information

WebGoat uses the Apache Tomcat server. It is configured to run on localhost although this can be easily changed. This configuration is for single user, additional users can be added in the tomcat-users.xml file. If you want to use WebGoat in a laboratory or in class you might need to change this setup. Please refer to the Tomcat Configuration in the Introduction section.

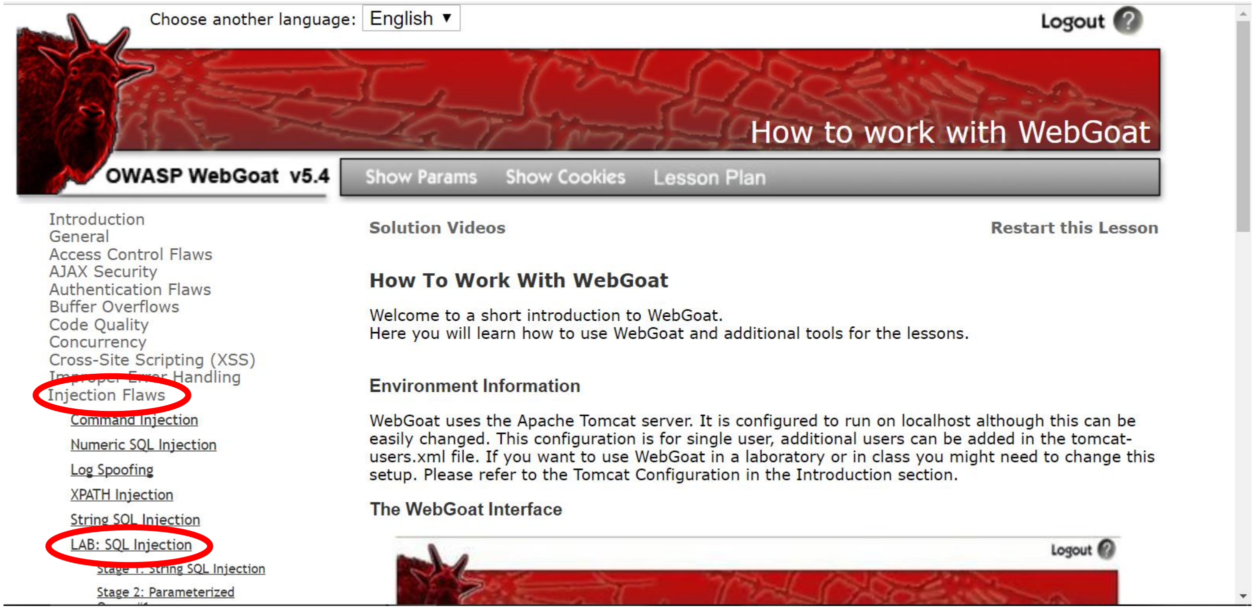
The WebGoat Interface

Complete the following two parts of the XSS Lab. For each part, include the correct values used to successfully exploit the application for each stage.

a. Phishing with XSS (20 points)
b. Cross Site Request Forgery (CSRF) (30 points)

2) SQL Injection Flaws

You start this part by clicking on the “Injection Flaws” tab and looking under the LAB: SQL Injection section:



How To Work With WebGoat

Welcome to a short introduction to WebGoat.
Here you will learn how to use WebGoat and additional tools for the lessons.

Environment Information

WebGoat uses the Apache Tomcat server. It is configured to run on localhost although this can be easily changed. This configuration is for single user, additional users can be added in the tomcat-users.xml file. If you want to use WebGoat in a laboratory or in class you might need to change this setup. Please refer to the Tomcat Configuration in the Introduction section.

The WebGoat Interface

Complete the following two parts of the SQL Injection Lab. For each part, include the correct values used to successfully exploit the application for each stage.

Stage 1: String SQL Injection 20 points

Stage 3 Numeric SQL Injection 30 points

3) Extra Credit:

Complete the following two parts of the Injection Flaws lab. For each part, include the correct values used to successfully exploit the application for each stage.

Blind Numeric SQL Injection (5 points)

Blind String SQL Injection (5 points)