**LAB 5: Web Server Script Attacks**

**WebGoat** is a set of intentionally insecure web application with progressively more difficult CSQL injection vulnerabilities. The 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

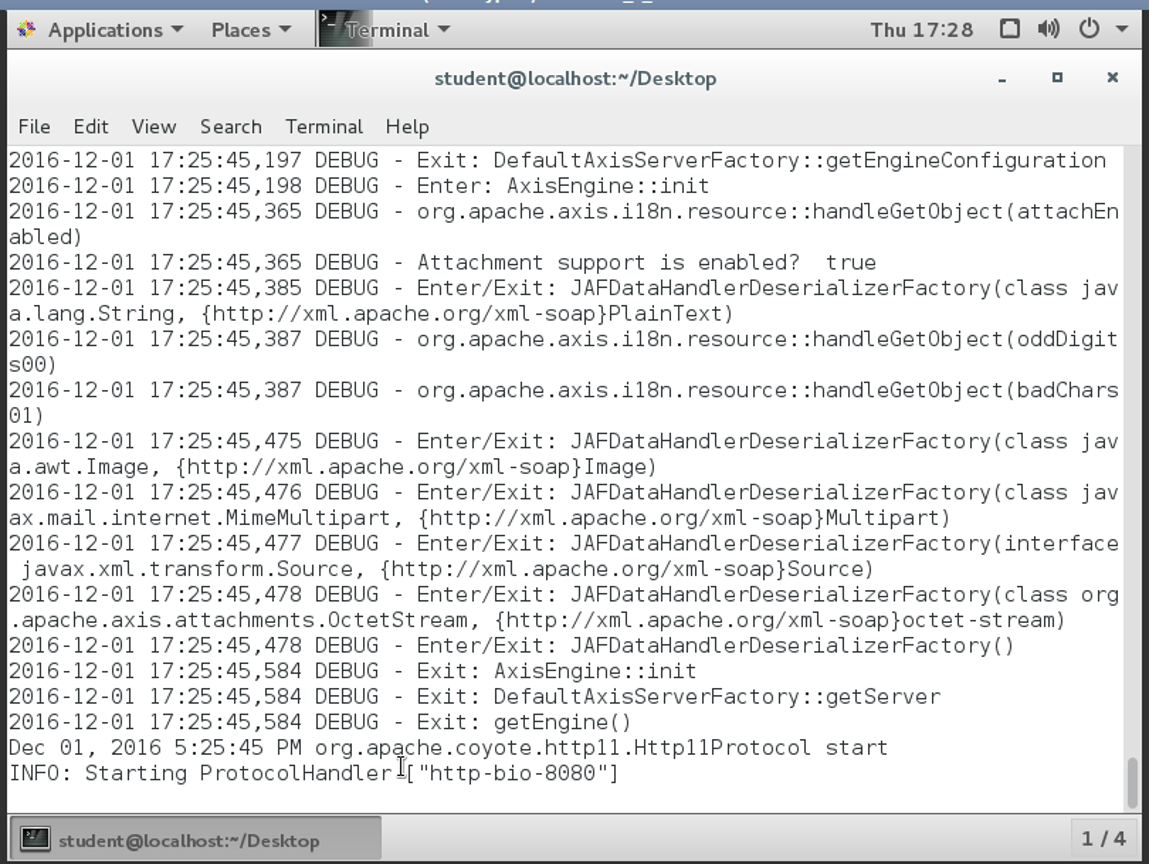
Hint and Solutions for the lab, try your best before looking at the solutions: <http://webappsecmovies.sourceforge.net/webgoat/#Injection_Flaws>

Before you starting the lab, you must first start WebGoat by opening a terminal and entering these commands:

cd Desktop

./RunWebgoat8080.sh

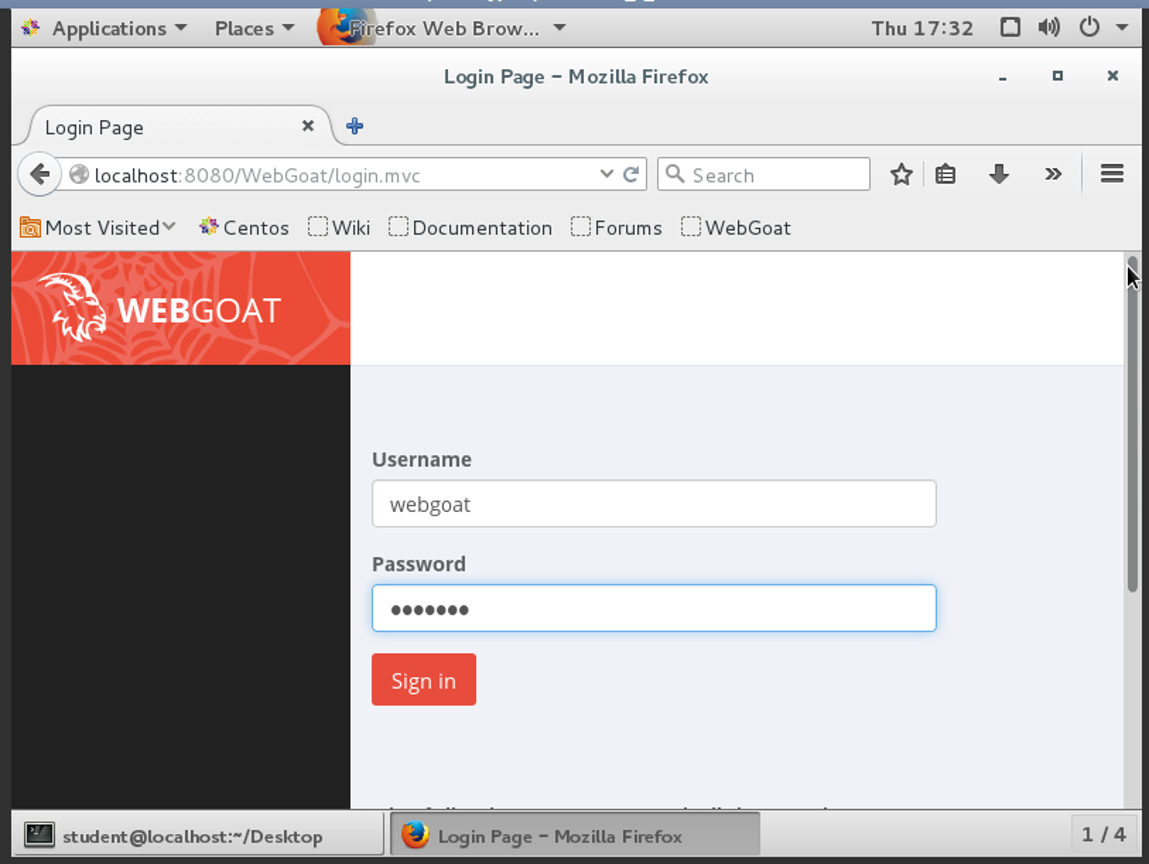
Then wait for the server to start:



It will take a few minutes to start the WebGoat framework, once it has started you can then open a web browser and visit the WebGoat page:

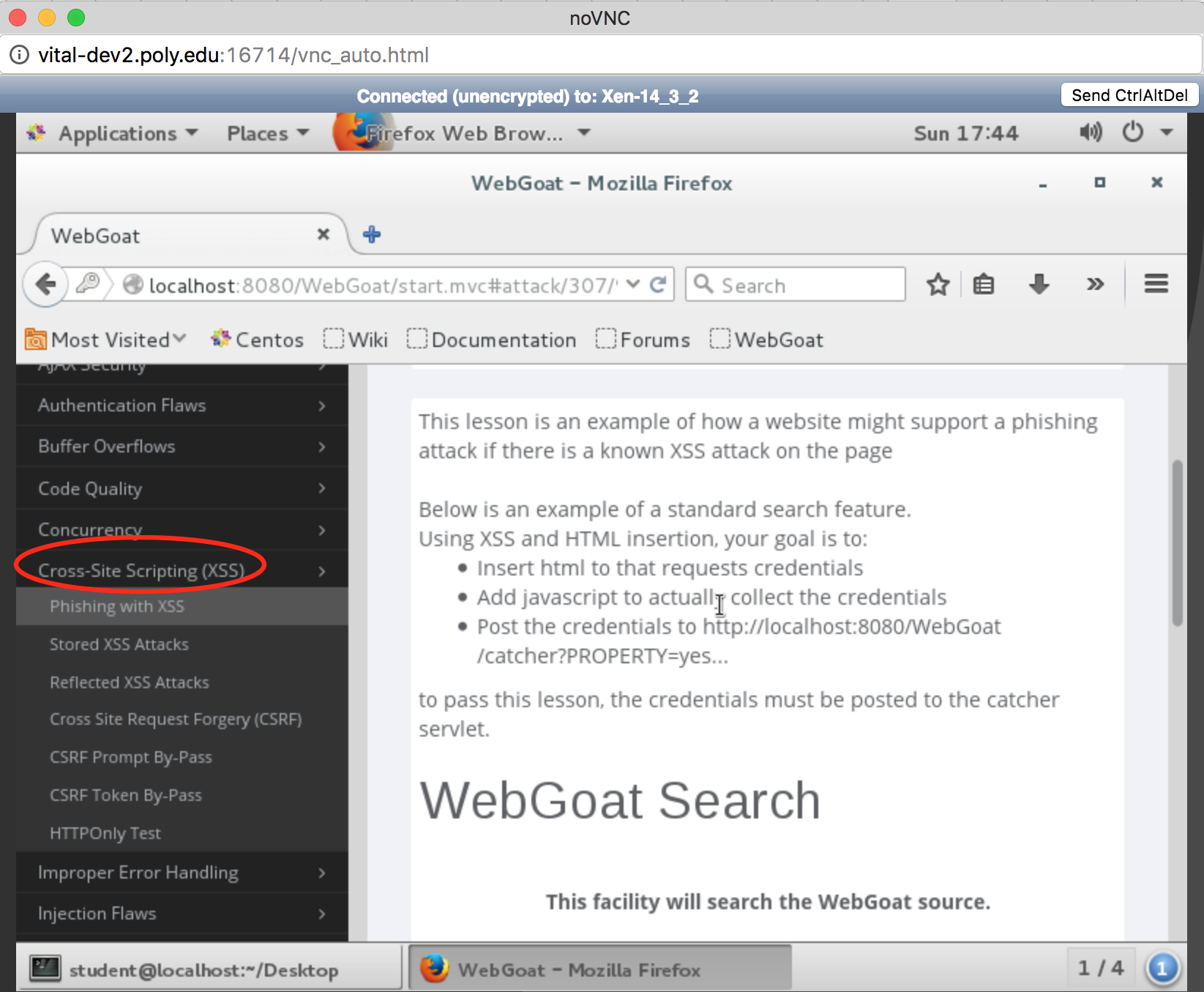
<http://localhost:8080/WebGoat>

Username: webgoat Password: webgoat



1. **Cross-Site Scripting (XSS)**

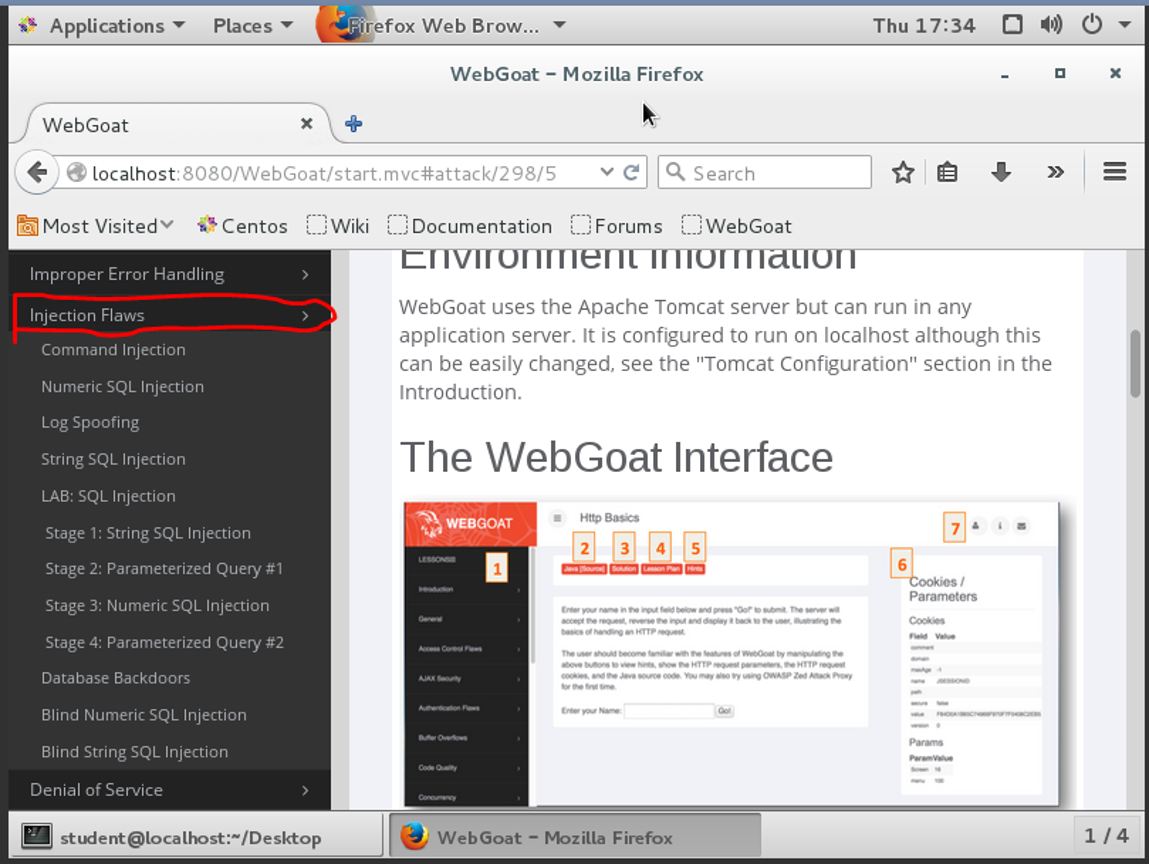
To start this part of the lab, click on the Cross-Site Scripting (XSS) tab:



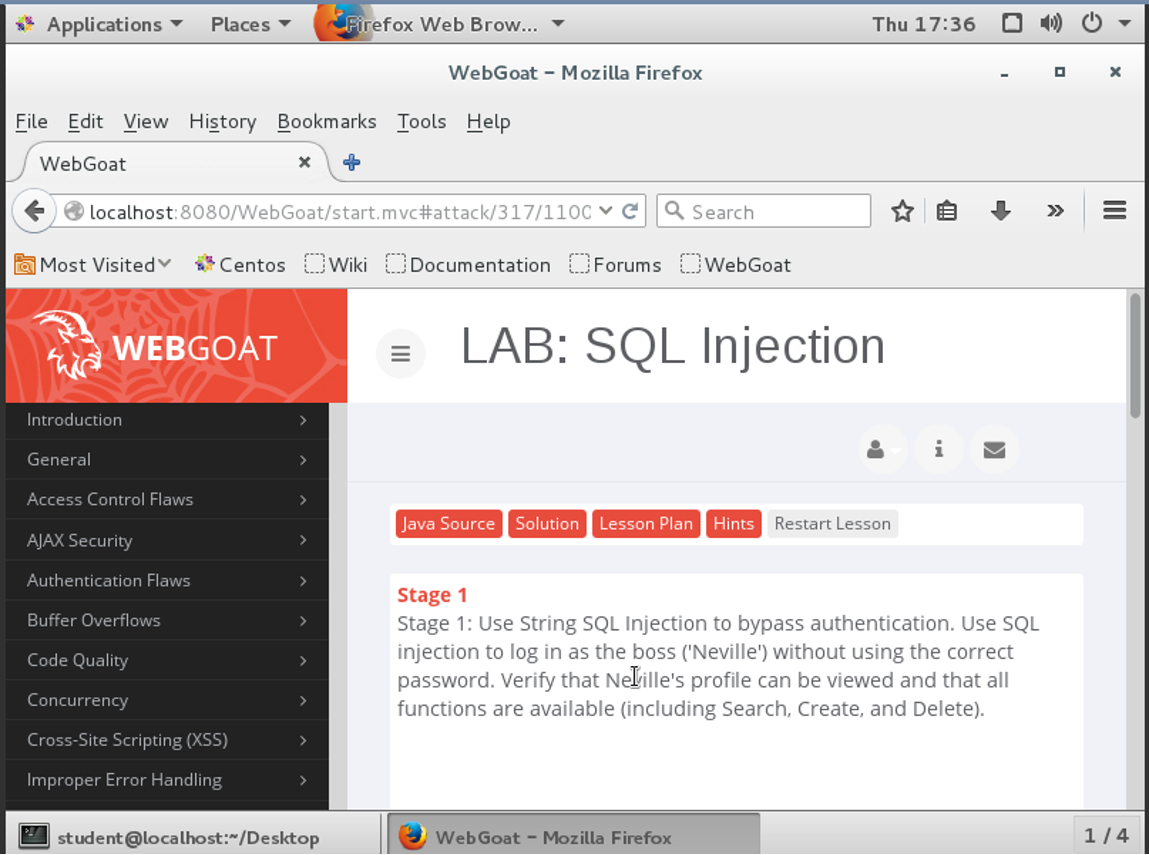
Complete the following two parts of the XSS Lab. For each part include the correct values used to successfully exploit the application for each stage.

1. Phishing with XSS (20 points)
2. Cross Site Request Forgery (CSRF) (30 points)
3. **SQL Injection Flaws**

You start this part by clicking on the “Injection Flaws” link:



Lab: SQL Injection



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

1. **Extra Credit:**

Blind Numeric SQL Injection (5 points)

Blind String SQL Injection (5 points)