WebGoat

Lab Prep

- **Open Kali VM from earlier with 4+GB of RAM on a Bridged Connection**
  - X:\VMS\S22\SEC-260\Kali_VM.ova
  - user: student + pass:2616
- **Can use own hardware, or VPN | Viewportal + RDP into cyber.local solution**

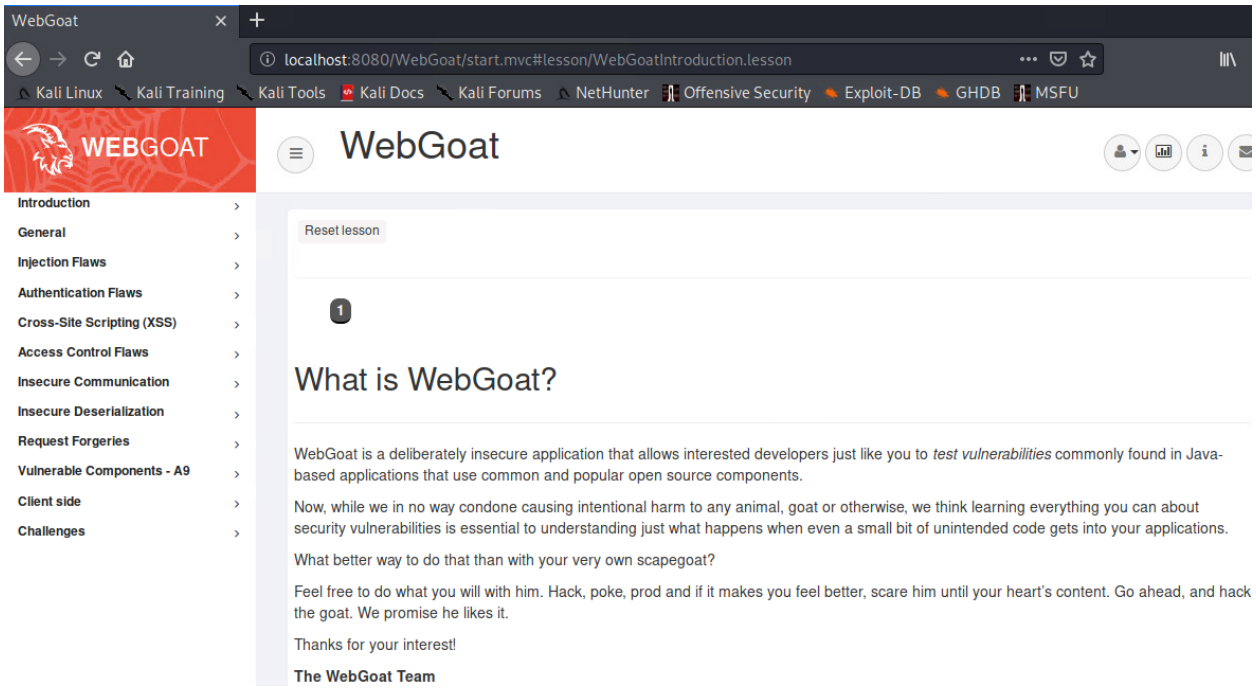
1. **Downloading and Installing Webgoat**
   a. Open up the command terminal
   b. Download WebGoat:
      i. wget https://github.com/WebGoat/WebGoat/releases/download/v8.0.0.M24/webgoat-server-8.0.0.M24.jar

   c. *Optional*: Depending on your Kali version, you might need to ensure Java version 11 is installed with "java -version" which is required to set up WebGoat. If you have a version under that, then you'll need to upgrade/install.

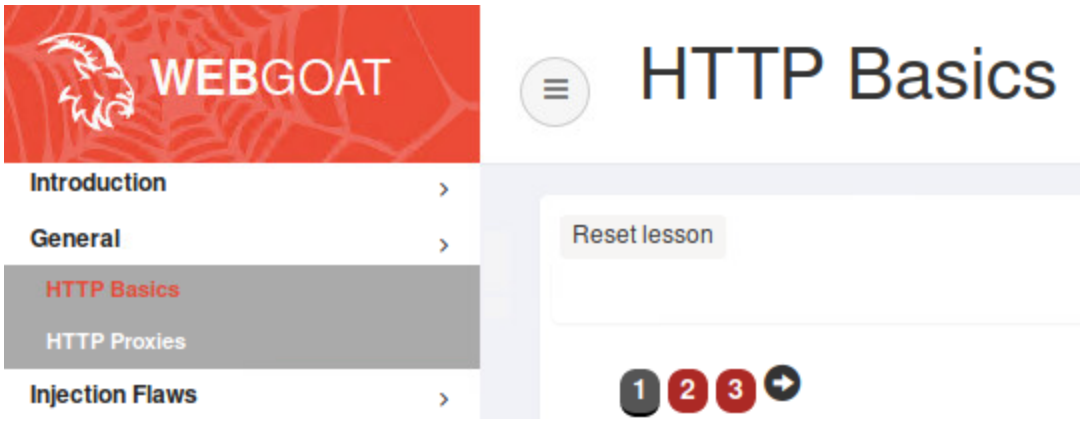
   d. Install and Run WebGoat (May take a few moments, and it will be ready once the console stops adding output with the last line displaying "Started StartWebgoat").
      i. java -jar webgoat-server-8.0.0.M24.jar --server.port=8080 --server.address=localhost

FYI: Keep Command Console open, similar to other Linux apps.

2. **Getting Started in Webgoat**
   a. Open a Web Browser within Kali
   b. Navigate to the webpage http://localhost:8080/WebGoat/login
   c. Click "Register a new user" and create a user using the syntax <first name + last name>.
      i. Make sure the password is not anything you do not want seen in deliverables! :)



General: HTTP Basics Module



a. Read concepts
b. Go through the "Try it" section, and "The Quiz".

Hint: For the quiz section, insert & submit the correct answer for 1st question, which then creates a POST with a very obvious filename viewed via Inspect Element's Network tab. This file contains the answer via a Parameter for the 2nd question.

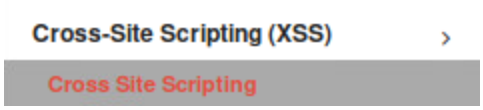
Deliverable 1: Screenshots of the “Try It” section, and of successful Quiz output.

Injection Flaws: SQL Injection

c. Read concepts
d. Go through the two “Try It” sections: String and Numeric SQLi.

Deliverable 2: Screenshots of dumped data from both “Try it” sections for SQL Injection.

Cross Site Scripting (XSS): Cross Site Scripting



e. Go through the first 2 “Try It” Sections: Reflected + Stored
    i. Reminder: Open Fields == Potential entries :)

Deliverable 3: Screenshots of first 2 “Try It” Sections completed.