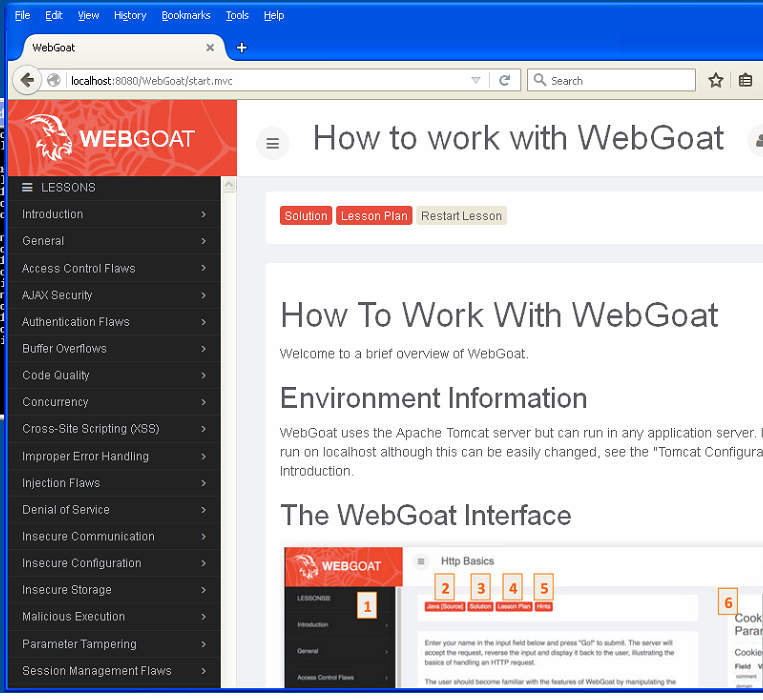
**ITIS 6200/8200 Principles of Information Security and Privacy**

**Project 3 XSS ATTACK**

**Part 2**

**Step 0: login to WebGoat with the Guest account (the login name and password are all “guest”.). You should see something like this.**



Now click on the Cross-site Scripting (XSS) attack in the left side, then click Stage 1.

**Stage 1 – Stored XSS Attack**

1. Using the drop-menu, you can login with ‘Tom Cat’ as Employee and password as tom
2. Click on View Profile.
3. Click on Edit Profile.
4. Change the text in the street field to **<script>alert(“XSS”);</script>**
5. Click on update profile.
6. Observe what happens.
7. Logout from Tom Cat

**Infecting Jerry with the script:**

1. Login with ‘Jerry Mouse’ as Employee and password as jerry
2. Click on Tom in left pane and then click on view profile in the right pane.
3. Observe what happens.

**Stage 3 – Stored XSS Revisited**

1. Login with ‘David Glambi(manager)’ as Employee and password as david.
2. Click on Bruce from the list and then click on view profile.
3. Observe what happens.

**Stage 5 – Reflected XSS**

1. Login with ‘Jerry Mouse’ as Employee and password as jerry.
2. Click on search staff.
3. Type **“><script>alert(“Test”);</script>** in the input field.
4. Click on find and observe what happens.

**Submission:**

Create a Word document, and write down answers to the following questions based on your observations from the activity:

1) What happens in a stored XSS attack? Explain using the project result.

2) What are some measures that can be taken to block a stored XSS attack?

3) Explain your observation and understanding about the vulnerability from stage 5.

Submit your report through Canvas by December 1st, 2016, before midnight.