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

**Project 3 XSS ATTACK**

**Part 1**

This project will help you to understand the cross-site scripting attacks on a web server. You need to accomplish the following tasks.

**Step 1**. Read the Wiki page about XSS attack.

<https://en.wikipedia.org/wiki/Cross-site_scripting>

Also, watch the video at Youtube on Reflected XSS attack at:

<https://www.youtube.com/watch?v=V79Dp7i4LRM>

Now you have prepared yourself with the basic knowledge. Let us try the experiment. In this experiment, you will set up WebGoat in your previously installed Windows XP virtual environment in Project 2.

**Step 2**. Install a state-of-the-art browser in your Windows XP virtual machine. I actually use Firefox version 42. If you go to here:

<https://support.mozilla.org/en-US/kb/install-older-version-of-firefox>

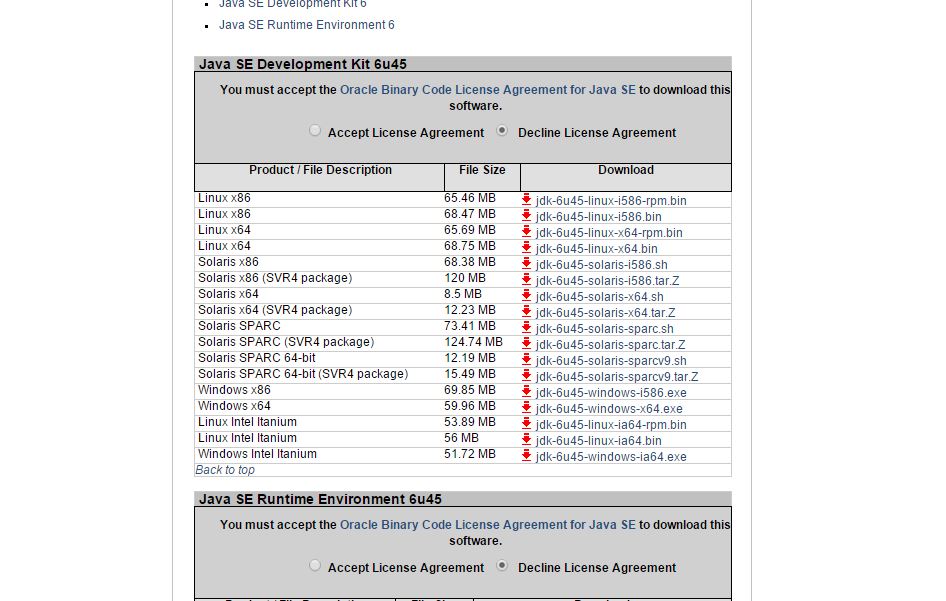
you can find almost all old versions of Firefox. You are more than welcome to try Firefox 49 (the very recent version that I have) and I would like to know the results.

**Step 3**.

In the Windows XP virtual machine, go to the following link by clicking or by copy-pasting it in your browser –

<http://www.oracle.com/technetwork/java/javase/downloads/java-archive-downloads-javase6-419409.html>

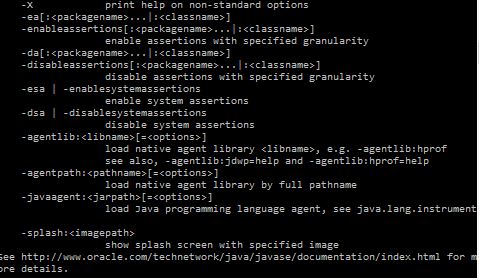
Scroll down to the ‘Java SE Development Kit 6u45’



Click on ‘Accept License Agreement’ radio button and then click on the ‘Windows x86 – jdk6u45-windows-i586.exe (69.85 MB)’. This is the 5th item from the bottom in the figure above. Oracle may need you to register an account to allow you to download. The download will begin shortly.

**Step 4.**

After the download is complete browse to the folder that you store the downloaded files and install the Java environment by running the executable file you just downloaded. After the installation is complete open a ‘Command Prompt’ window (Start -> Accessories -> Command Prompt) and type in ‘java’ in the command prompt window and press Enter. You should see something like this,



This means you have successfully installed Java. Close the command prompt.

**Step 5**

Now in your Windows XP virtual machine, browse to the following link by clicking or copy-pasting it in the browser-

<https://github.com/WebGoat/WebGoat-Legacy/releases/tag/v6.0.1>

Scroll to the bottom of the page and download the ‘WebGoat-6.0.1-war-exec.jar’ by clicking on the jar file. **After download rename the file to ‘WebGoat.jar’**.



**Step 6**

Now open Command Prompt again. Navigate to the folder where you downloaded the WebGoat jar file. Type in the command: *java –jar WebGoat.jar.* Wait for 1 to 2 minutes till the server is up and running. You should see the line “Starting Protocolhandler [http-bio-8080]” at the bottom.

**Step 7**

Open a browser window and type ‘http://localhost:8080/WebGoat/’ to start WebGoat in the browser. You should see something like this:

