LAB SESSIONS: TOOLS REQUIRED

The second half of the Friday lectures will be a `lab session' in which some of the security theory is applied by performing some basic security attacks. You can prepare your computer for the lab sessions by installing the required software. Guidelines on where to find the software and how to install it are given below.

A. MOZILLA FIREFOX

Mozilla Firefox will be the reference browser we will use during the lab sessions. Download and install the latest version that you can find here: http://www.mozilla.org/en-US/firefox/new/

B. MOZILLA ADD-ONS TAMPER DATA

A tampering tool is one of the most important means needed to exploit web application vulnerabilities. For our exercises we need *Tamper Data*, a Firefox Add-Ons you can download at the following address: https://addons.mozilla.org/en-US/firefox/addon/tamper-data/

Be sure to correctly install it and to restart your browser once finished. The tool will allow you to intercept every HTTP request/response that you send or receive during your browsing session. To start *TamperData* click on Firefox Menu Bar, Tools→ Tamper Data. This will open a new window where you can observe your HTTP traffic. As shown in Figure 1 *tampering* can be started and stopped according to your needs (e.g. tampering is needed to solve exercises but you can stop it during normal browsing). The *TamperData* plugin does not only allow you to see the content of the requests/responses, but also to modify them. For example you can change the parameters of a request by just typing the new values, as shown in Figure 2.

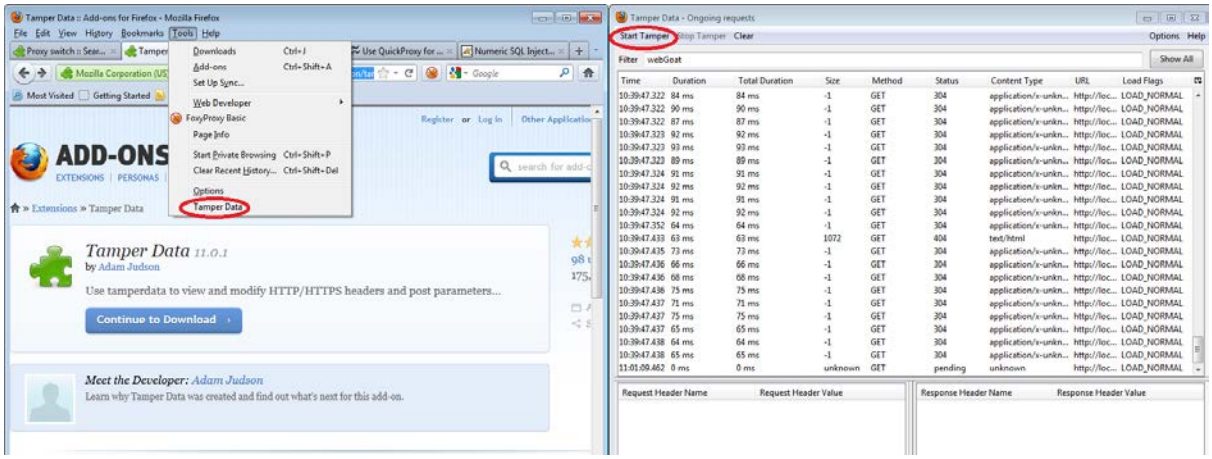

Figure 1: Tamper Data Add-On

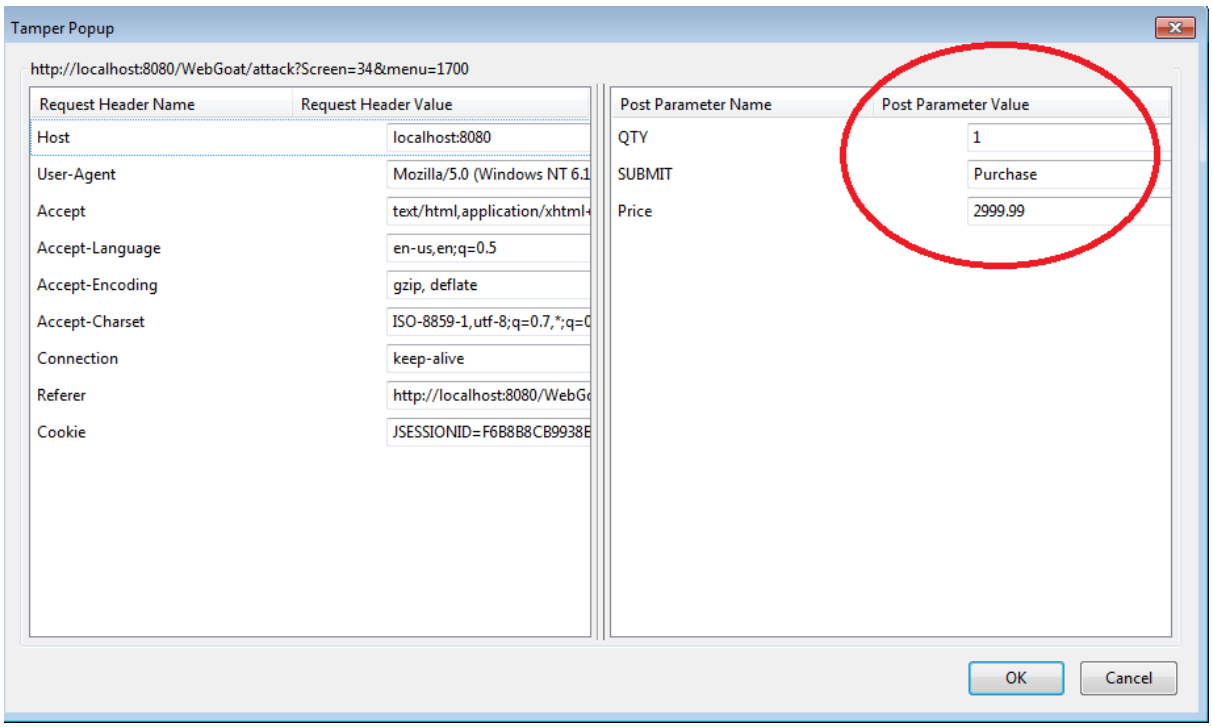

Figure 2: Modifying Request Parameters by using Tamper Data

C. WEB GOAT

WebGoat[1] is a deliberately insecure web application, designed to teach web application security lessons. You can download the version 5.4 of WebGoat here: http://code.google.com/p/webgoat/downloads/detail?name=WebGoat-5.4-OWASP_Standard_Win32.zip&can=2&q=

This is a stand-alone version, which means you will get all you need to run the web application on your machine. Once you downloaded the .zip file, extract it on the Desktop. At this point you will have a folder structure looking like the one in Figure 3. Run the file *webgoat_8080.bat* to start you application, and type http://localhost:8080/WebGoat/attack in your address bar.

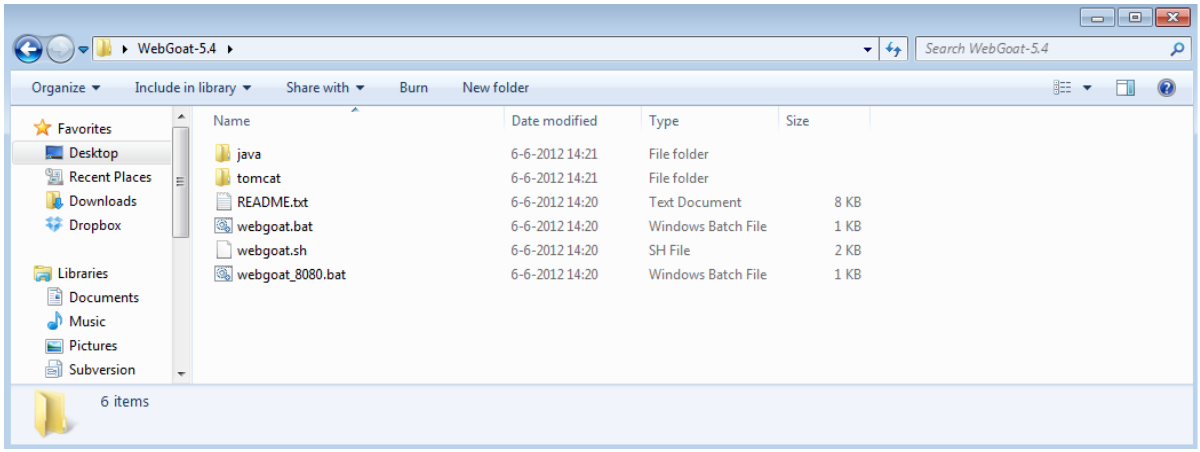

Figure 3: Folder Structure

[1] https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project

If the address http://localhost:8080/WebGoat/attack does not work you might need to start the tomcat service by yourself. To do so start the service **WebGoat-5.4\tomcat\bin\startup.bat** and browse to http://localhost/WebGoat/attack.

If everything went fine you will be asked for your credentials: insert the word *guest* for both username and password, and you will see the page of Figure 4. Press the *Start WebGoat* button: you are ready to begin the lab session.

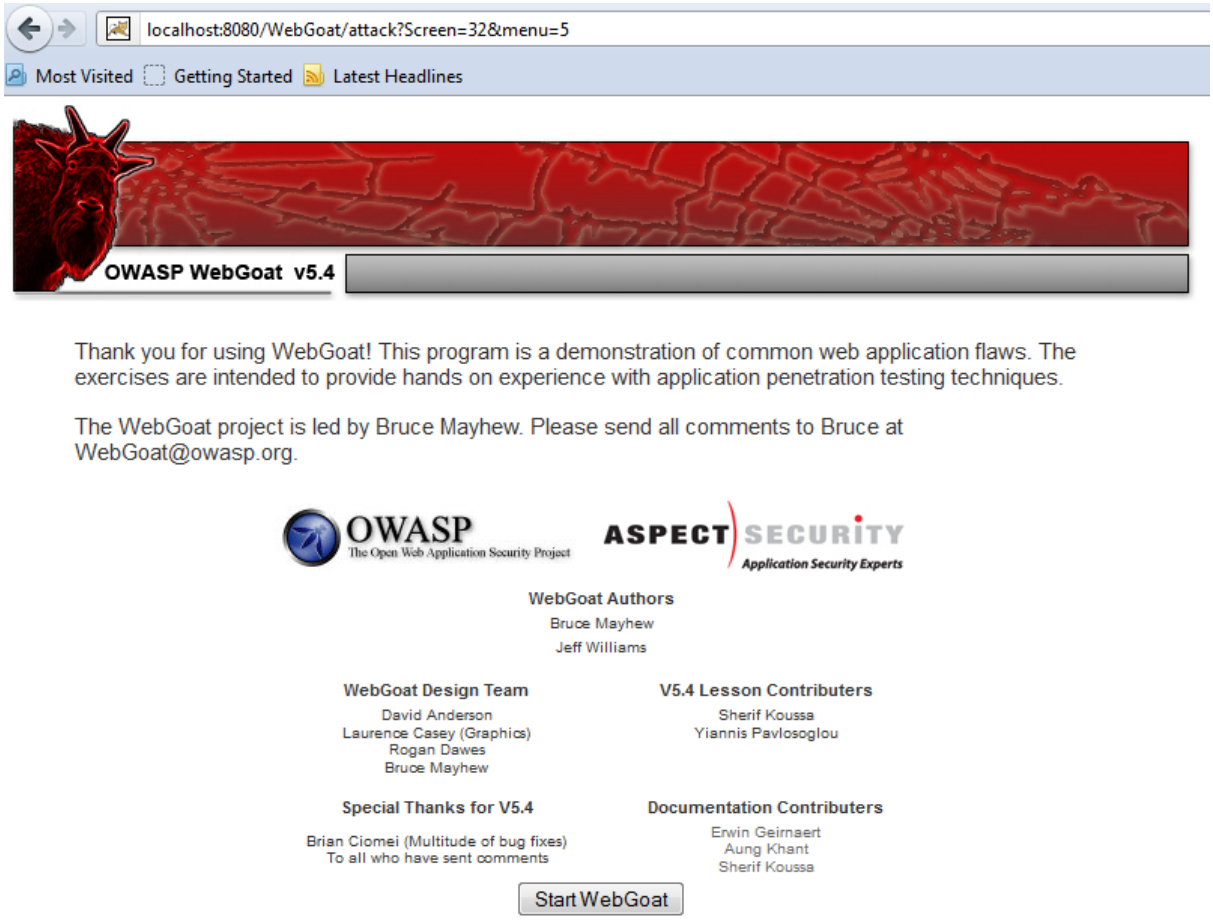

Figure 4: WebGoat Home Page