**Web Security**

Overview

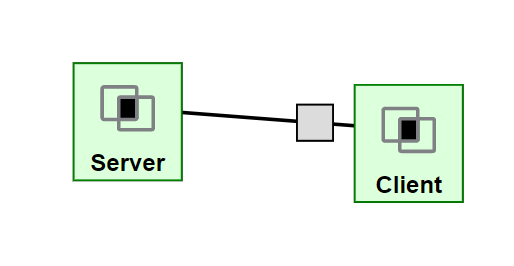
This tutorial will help you to get familiar with several Web attacks, including Cross-site Scripting and SQL injection.

Lab Environment

RSPEC file:

<https://raw.githubusercontent.com/DrVoyager/EdGENI/master/Rspec-Files/WebGoat-Rspec.txt>

Lab Topology:



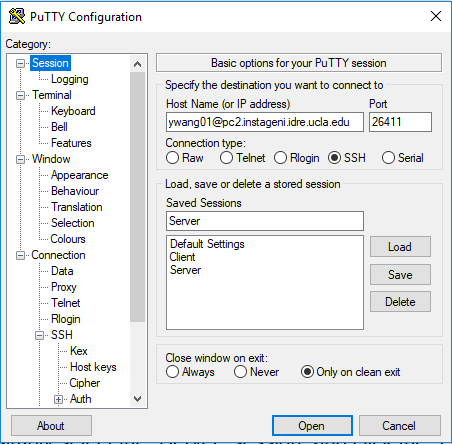
For this lab, our topology will consist of two hosts. We will have a Server machine, where the WebGoat Web server is hosted. We also have a Client machine, where user can launch Firefox to visit the WebGoat Web server and run Zap, the HTTP Proxy tool to manipulate the HTTP transaction.

Preparation

This lab will use the GENI environment that you set up. If you haven’t set up the environment, please refer to the instruction to setup the lab.

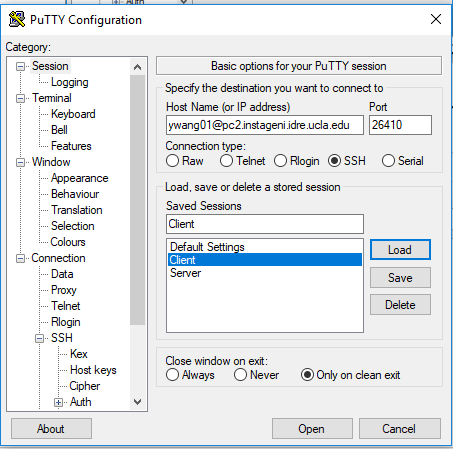
**How to resume your VNC desktop?**

**If you are using your own Windows computer,** you will have the Server and Client session saved on your Putty, as follows.



With the saved sessions on PuTTY, exiting and resuming your VNC desktop are easy.

To resume your Client machine desktop, open PuTTY and load the *Client* session you have saved and click Open button to connect.



Type in your passphrase. Open vncviewer, connect with the address 127.0.0.1:5901. You will get to the resumed desktop

To resume your Server machine desktop, open PuTTY and load the *Server* session you have saved and click Open button to connect. Type in your passphrase. Open vncviewer, connect with the address 127.0.0.1:5902. You will get to the resumed desktop

**If you are using Citrix Virtual Desktop or Mac/ Linux Computer**

Server and Client session might not be saved on your Putty. You need to follow the instruction in “connect to virtual machine” to connect to Client or Server. Do not execute the vncserver or vncserver :2 command again, unless you have to restart the VNC server or VM, since you have already started it in Lab 1. If you have to do so, check the “vPark Lab Environment FAQ” document.

**How to exit your Lab desktop?**

Simply close the PuTTY/SSH program and VNC viewer.

**Other issues about the vPark Environment?**

For other vPark Environment issue, please check the “vPark Lab Environment FAQ” document.

Task 0 – Start and Visit WebGoat

**NOTE**: This lab is reusing the environment in Lab 4. If you have started the WebGoat and Firefox, you can skip Task 0. However, you still need to take screenshots required in Task 0 B and Task 0 D to earn the points.

1. Open a terminal on the Server machine, type in command ifconfig to find out its IP address. It should be in the format of 10.10.x.x. Normally it is 10.10.1.2.
2. On the terminal of the Server, type in the following two commands

cd /vPark

java -jar ./webgoat-server-8.0.0.M24.jar --server.address=<Server IP>

, where <Server IP> is the IP address you found in Task 0A. Wait for a while. The WebGoat is ready when you see the message “Started StartWebGoat in xx.xxx seconds(……)”.

Take a screenshot to show you have set up the WebGoat on the Server machine.

1. On the Client machine, type in command firefox & in a terminal to start Firefox.
2. Type in the following address in firefox of Client machine: http://<Server IP>:8080/WebGoat, where <Server IP> is the IP address you found in Task 0A. Take a screenshot showing you can visit the WebGoat on the Client machine.
3. Register an account on WebGoat and log in with your registered account. Remember the account. You will also use it in next week’s lab.

The following labs are all performed on the Client Machine

Task 1 – Cross-Site Scripting (XSS)

1. Under the “Cross-Site Scripting(XSS)” tab of WebGoat (on the left bar), click on the “Cross Site Scripting”.
2. Go through page 1-6 in WebGoat to learn more knowledge about XSS.
3. On page 2 in WebGoat, answer the question in the page bottom and submit. Make screenshot for the response page of your answer. Notice that the firefox in VNC is a little different from what the WebGoat describes. You cannot execute javascript:alert(document.cookie); on the address bar. However, you can execute the command at the Web Console, which can be found by selecting Firefox menu (the  icon to the right of the address bar) 🡪Web Developer🡪Web Console.

1. Work on the challenge on page 7 in WebGoat. Try to fill in web form with the script payload and trigger the alert box. Describe how you filled in the web form. Take a screenshot to show you have successfully triggered the alert box.
2. Learn the stored XSS on page 12 in WebGoat and complete the challenge on page 13. Notice that to call the function webgoat.customjs.phoneHome, simply using the JavaScript statement webgoat.customjs.phoneHome(); The function output can be seen at the Web Console, which can be found by selecting Firefox menu (the  icon to the right of the address bar) 🡪Web Developer🡪Web Console. Answer the question at the bottom of page 13 in WebGoat and submit. Describe how you fill in the form to achieve the goal. Make screenshot for the response page of your answer.

Task 2 – SQL Injection

1. Under the “Injection Flaws” tab of WebGoat (on the left bar), click on the “SQL Injection” item (the second item).
2. Study materials from page 1 to 6 in WebGoat.
3. Complete the challenge on page 7 in WebGoat. Describe what did you type in the box and make a screenshot to show that you have succeeded.
4. Complete the challenge on page 8 in WebGoat. Describe what did you type in the box and make a screenshot to show that you have succeeded.