Task 4 - An OWASP Exploit

Objective

The objective of this task is to introduce you to WebGoat for practicing web application security. You will choose a vulnerability in WebGoat from the OWASP Top 10 that you'd like to learn, and then exploit that vulnerability. You will also document the vulnerability, your exploit steps and some countermeasures to prevent future exploits of the vulnerability.

Background

WebGoat is a popular deliberately insecure web application for practicing web application security. The application is maintained by the OWASP Foundation. It contains many different lessons that focus on teaching the OWASP Top 10 and several other security problems in web applications. For each vulnerability, the application gives users the capability to view the lesson plan, hints on solving the lesson, the source code, and even the solution for the lesson.

Setup

Login to the Linux VM.

1. You will use a Docker container called comp3611/webgoat for this task. The image is already installed on the Linux VM. This image is simply an alias for webgoat/webgoat-7.1 on the Docker Hub. As such, you can read more about the image directly from the hub.
2. Start this container by typing the following command in a terminal on your Linux VM.

   ```
   docker run --detach --name task4 comp3611/webgoat
   ```

3. The docker run command will start the Docker container at the IP address 172.17.0.2. Open up a browser on the Linux VM and access the WebGoat interface using the URL - http://172.17.0.2:8080/WebGoat. Login to WebGoat using the following credentials -

   ```
   Username=guest
   Password=guest
   ```

Requirements

1. Once logged into the WebGoat web interface, read the page Introduction -> How to work with WebGoat to understand the WebGoat environment, the interface, and browse the list of the many lessons that are available to you for exploration.
2. In another browser window, open the OWASP Top 10 - 2017 Web Application Vulnerabilities report. Skim over this report and select a vulnerability that you find interesting, and would like to explore further.
3. Back in the WebGoat web interface, find a lesson that corresponds to the vulnerability you selected in Step 2. First, read the lesson objectives and play with the interface to understand how it works. Next, devise an attack to exploit the vulnerability described by the lesson objective. Try this exploit on the interface till you get it right. Upon successful exploitation, take a screenshot for the report. This screenshot MUST prove that your exploit has achieved the lesson's objective.

Cleanup

Stop and remove the container by typing the following command in a terminal on your Linux VM.

```
docker stop task4 && docker rm task4
```

Task Report

For this task, each student must submit a report with the following information:

1. Submit the screenshot(s) showing the successful exploitation of a `WebGoat` vulnerability.
2. Write a 1-2 page report explaining the vulnerability, all the steps that you took to exploit the vulnerability, and some countermeasures that can be implemented to prevent future exploitation of the vulnerability. Assume that you're writing this report for someone who's not technical, and focus on making the report easy to understand for anyone reading it.

Grading

- 60 points - Screenshot(s) showing the successful exploitation of a `WebGoat` vulnerability
- 40 points - Quality of the report documenting the vulnerability, the attack and possible countermeasures