OWASP WebGoat – Web Application Security Lessons

Professor Yeali S. Sun

Project Description

Web application security is difficult to learn and practice. Not many people have full experience in exploiting vulnerability. WebGoat is a deliberately insecure web application maintained by OWASP designed to teach web application security lessons. You should install and practice with Webgoat, and learn how popular web attacks actually work. In each lesson, you should demonstrate your understanding of a security issue by exploiting a real vulnerability in the WebGoat. It is intended to let you learn where vulnerability may exist and how exploitation occur, and most important of all, to think about how to defense such web attack.

The operation of HTTP, web browser and certain web attacks will be covered in the lecture, and the first few lessons will be demonstrated in the class as well, including the basic usage of WebGoat and the tools for exploiting and testing. WebGoat v5 provides more than 30 lessons. Please follow the lesson instructions, hints, and solutions to complete as more lessons as possible on your own. If you are unable to comprehend a lesson, walkthrough videos are available on the Internet.

The final term report should include a) how to install WebGoat and what additional security tools you install, b) the detail solution to three designed lessons for final term paper (see requirement below) and c) the detail solution to three lessons up to the draw by the TA for each team. The detail solution to each lesson in the final report should include 1) the steps to exploit the vulnerability in the lessons, 2) the reason why the exploitation works, and 3) your suggestion to stop such exploitation in detail.

You should demonstrate the solution to the two designed lessons to TA. The successfulness of you solution depends on the standard WebGoat scorecard. You will need to demonstrate your solution to a new lesson to TA as well. Please register your demonstration time in prior.

Grading

- Final term paper: 50%
  - Installation and tools: 14%
  - The solution to three designed lessons for the term paper: 18%
  - The solution to three random lessons: 18%
- Demonstration: 50%
  - Two designed lessons for the demonstration: 36%
  - One new lesson: 14%

Requirement and Notice

- At most, two students form a team to do this term project.
- You should install WebGoat v5.2 and finish as more lessons as possible. Note that learning the designed lessons does not guarantee you a high score in the final demonstration, especially for the new lesson.
- The three designed lessons for the final term paper are: Access Control Flaws, LAB: Cross Site Scripting, and LAB: SQL Injection.
- The two designed lessons for the demonstration are: AJAX Security, Session Management Flaws.

Useful Links

- OWASP ebGoat Project, https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project
- WebGoat User and Install Guide, https://www.owasp.org/index.php/WebGoat_User_and_Install_Guide_Table_of_Contents
- OWASP WebGoat v5.4 Web Hacking Simulation WalkThrough Series, http://webappsecmovies.sourceforge.net/webgoat/