OWASP WebGoat Village

Brian Cameron

Objective

- Install and setup WebGoat for hands on practical experience
- Engage in OWASP tools to strengthen security skills
- Work with complementary tools

Agenda/Overview

- This village will be focused on educating people about what is OWASP, WebGoat and ZAP.
- During this session we will run through the WebGoat exercises on a screen and use audience participation to work through the lessons that come with WebGoat which primarily cover OWASP Top 10 exploits and exercises to learn how to use features in ZAP.
- OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications. The list may be found here: https://owasp.org/www-project-top-ten/
- We will also be helping interested people install this software on their laptops if there is an interest. If there are people who want to work through the lessons by themselves or in small groups after installing the tools, we will provide them with a place to work and provide them with support if they get stuck, etc.
- No particular advance training is needed, though being familiar with the OWASP Top 10 beforehand would be smart for those who want to prepare. Past pen-testing experience is not necessary, but would probably make the lessons more straightforward.

WebGoat Lesson Plans

The WebGoat lesson plans are documented here in the “Lessons” tab:
https://owasp.org/www-project-webgoat/

Lessons
WebGoat 8 contains lessons that cover aspects of 9 of the OWASP Top 10 vulnerabilities (all except A10 Insufficient Logging & Monitoring)

1. Standalone

Download the latest WebGoat release from
https://github.com/WebGoat/WebGoat/releases

```
java -jar webgoat-server-8.0.0.VERSION.jar [--server.port=8080] [--
server.address=localhost]
```

The latest version of WebGoat needs Java 11. By default WebGoat starts on port 8080 with `--server.port` you can specify a different port. With `server.address` you can bind it to a different address (default localhost)

Getting started with ZAP

ZAP installation instructions and browser proxy setup links:

- https://www.zaproxy.org/getting-started/
- https://www.zaproxy.org/docs/desktop/start/proxies/

A series of short videos about different ZAP features

- https://www.zaproxy.org/zap-in-ten/

Additional resources

- This link points to some YouTube videos that are helpful for getting into WebGoat and might be worth reviewing before the Village for those who want to do more preparation:
    - https://www.youtube.com/watch?v=33VZ7RvMkgM&list=PLrHVSJmDPvlqxCfBhPuksHdpViPyeZTsF

Q&A