Bughunting bootcamp - Discovering 0day

Training Course

17th & 18th of October

Table of Contents

All training courses are two full days of intensive, hands-on learning and include complimentary morning tea, lunch and afternoon tea. Tickets can be secured buy going to the website https://appsecday.io/.

Course Abstract

This intense two day, lab based, course will teach you the skills to find new security bugs, evaluate the root cause, assess impact and write exploits to prove the existence of vulnerabilities in applications. The course will cover both manual and automated vulnerability hunting in web applications, source code and compiled binaries.

Additionally we will cover how to chain bugs together to achieve unauthenticated remote code execution, vendor notification, vulnerability disclosure and how to obtain a CVE. The training prioritizes real world vulnerabilities across several languages.

What attendees will learn?

Students will learn how to identify and exploit common security vulnerabilities in open and closed source software.

What attendees will be provided?

- Slides for the training course.
- Virtual Machine with all the required software and reference material.

What attendees should bring?

- A laptop that is capable of running a VMWare virtual machine (vmware player or workstation) to complete this course.

Pre-requisites

The course is aimed at beginners and security professionals alike, with a variety of targets to practice bug hunting skills, so the attendee will find something suitable for their skill level.

Students are expected to be somewhat familiar with the Linux command line as well as OWASP Top 10 & CWE-25. Basic scripting knowledge is recommended, but not required.

Detailed Outline

Day 1

Theory and web application security

- Choosing suitable targets
- Static and dynamic analysis
- Web application bugs
- Web application exploits
- OWASP top 10
- Logic bugs
- Chaining bugs

Day 2

Memory corruption bugs and exploits

- Shell code
- Fuzzing
- Triage
- Writing memory corruption exploits
- Dealing with disclosure
- Conclusion

Trainer Biography

Eldar Marcussen

https://www.linkedin.com/in/eldarmarcussen/

Eldar is a penetration tester and security researcher with HackLabs where he performs red teaming, and other pentests. He is also an assessor for CREST Australia. He has worked closely with bugcrowd in the past and was a recipient of the first CVE 10K candidate numbers. In addition to finding vulnerabilities he contributes to and maintain several open source projects in his spare time aimed at web application security and penetration testing. These include graudit, doona, lbmap, dotdotpwn, nikto and more.