Security not just for security people.

Security for developers.

A unique spin to wargaming, focusing on developer education.

Problem Statement and Goals

Developers write the code that go into production software. They are the wizards that transform our lives with the convenience that modern applications provide. At the same time, they aren’t perfect. Bugs are introduced. Code becomes defective. The security of an application is often compromised by the very same people that shape it.

In fact, up to 90% of bugs can be prevented through secure coding best practices [1]. However, inexperienced developers often turn towards online resources like StackOverflow, which often lead to less secure code [2].

It is time we focus on the developers – they must learn to identify security bugs in their own code, and correctly fix them.

Approach

We created an onboarding program designed to teach new developers vulnerabilities listed on the OWASP Top 10 with Capture-the-Flag (CTF) elements built on top of Splunk’s existing training infrastructure.

Structure

For each vulnerability, we have the following:

- Description of vulnerability
- Case study of vulnerability based on real issues previously found in Splunk’s codebase
- Offensive practicum (a la CTF)
- Defensive practicum (where we automatically test if the vulnerability has been fixed correctly)

Results

- 2 trial runs completed, well received by participants
- 11 different web vulnerability categories covered: (XSS, CSRF, SSRF, and more)
- All participants thought it was useful in understanding the vulnerabilities, although 60% felt that the difficulty scaling could be better (hints were too direct)
- Balancing learning outcomes vs. time taken is hard!
- Officially put into production since Q4 2019
- Future Work: better hint system, verification with remote environments, refresher courses

Acknowledgements

- Project mentor: Teja Myneedu
- Project in-charge: Jayson Grace
- Splunk’s ProdSec team + newcomers who beta tested the platform!


Wai Tuck Wong
Carnegie Mellon University, Information Networking Institute
Splunk Inc.