Vulnerability Scanning with OWASP ZAP

18F In partnership with the Dept. of the Interior

What is vulnerability scanning, and why do it?

A scanner communicates with a web application through the web front-end to identify potential security vulnerabilities without knowledge of the source.

If it will be ATO’d, it will be scanned

What is OWASP ZAP?

- OWASP = Open Web Application Security Project (https://www.owasp.org)
- ZAP = Zed Attack Proxy
- Penetration testing toolkit with automated scanning capabilities designed for developers.

Passive Analysis

Quick Start

* Don’t run this on live sites without telling someone on the Infrastructure Team

Other Functionality

Resources

- https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
- https://pages.18f.gov/before-you-ship/security/dynamic-scanning/
- https://github.com/zaproxy/zap-core-help/wiki
- #compliance-toolkit
- Setting up the proxy: https://github.com/zaproxy/zap-core-help/wiki/HelpStartProxies
- Juice Shop, an intentionally insecure Web App: http://bkimminich.github.io/juice-shop/#/
- Fuzzing data: https://github.com/minimaxir/big-list-of-naughty-strings

Questions?

18F