- Menu
- Menu
- Home
- About
  - BSidesPDX
  - Code of Conduct
  - Contact
  - Past Events
- CFP
  - CFP
  - Review Board
- BsidesPDX 2019
  - Register
  - Schedule
  - Speakers
  - Sponsors
  - Contests and Events
  - Venue
  - Volunteer
  - Workshops
  - Review Board

Workshops

OWASP Top Ten Lab Featuring OWASP Juice Shop

David Quisenberry (@quizsec)

The OWASP (Open Web Application Security Project) Top 10 is a powerful awareness document for web application security. It represents a broad consensus about the most critical security risks to web applications. Injection, Broken Authorization, Sensitive Data Exposure are just some of the categories it covers. This training will provide those unfamiliar with the OWASP Top Ten an opportunity to learn about the categories hands on through the OWASP Juice Shop - an intentionally insecure web application.

David Quisenberry (@quizsec) is a backend developer and security champion with Daylight Studio, a local Portland boutique web agency. He serves on the Portland OWASP board and does what he can to up the involvement of established and emerging software developers in security conversations.

Introduction to Binary Exploitation

Aaron Esau (@arinerron), Aaron Jobé (@dirtyc0wsay)

Ever wondered how vulnerabilities like BlueKeep and Eternal Blue work, or are you just interested in learning about the binary exploitation Capture The Flag (CTF) category? This workshop will walk students through exploiting their first buffer overflow vulnerabilities. It will teach them how to develop their own exploits and obtain RCE by redirecting the flow of code execution to shellcode or libraries with or without ASLR enabled. Students should have some experience with Python and Linux and are expected to bring a laptop with VirtualBox and an SSH client installed (a VM will be provided).

"Aaron Esau (@arinerron) is a 17 year old security researcher, CTF player, bug hunter, intern at Summit Security Group, a software developer, and a full-time high school student. Although most of his experience relating to security is with web and binary exploitation, he is interested in many aspects of security and privacy.

Aaron Jobé (@dirtyc0wsay) is a high school senior. His interest in computers led him to binary exploitation. He participates in CTFs and various other security challenges to further expand his skills. After high school, Aaron plans to pursue a career in cyber security."

How to Rock Your BSides Presentation!

Olivia Stella

Have a cool security topic the world should know about? Have you wanted to present at BSides but didn't know where to start? The goal of this workshop is to arrive with an idea and leave with all you need for an amazing presentation that will keep your audience engaged. Topics covered include how a call for papers works, what to do when you're accepted, speech delivery basics and day of presentation tips and tricks. Participants will receive handouts that walks you through the presentation process tailored to security and tech specific presentations. All basic materials will be provided. Laptop optional, but take that next step and have a completed presentation when you leave!

Olivia Stella is a senior security analyst for a US airline. In her current role, she focuses on aviation security and vulnerability management including pen testing and coordinated disclosure. She has over ten years of experience in software development and information security. Previously, she worked at an in-flight entertainment company in product security supporting incident response, risk & compliance, and as the bug bounty lead. She holds a bachelor's degree in computer science, masters in software engineering, CISSP & CISM. When she's not wearing her security hat, she loves to curl and is an avid toastmaster. (That's right, ice curling.)

Investigation Basics Crash Course

William Peteroy and Alex Sirr

This workshop will get attendees smart on the foundations they need to perform an end-to-end investigation from network to host. We will cover triage and evidence collection for endpoint and network with a focus on key data points from each that allow us to pivot from endpoint to network data (and vice versa).

We will discuss basic topics, open-source and commercial tools, build an investigation timeline and triage report with a hands-on lab.

Attendees should have a basic understanding of network (ports, protocols, etc) and endpoint (logs, files, windows registry, file system) fundamentals to get the most out of the workshop.

William Peteroy is the Chief Technology Officer for Security at Gigamon where he leads security strategy and innovation efforts. William is also the founder and CEO of ICEBRG (acquired by Gigamon in 2018) and has previously held a number of business and technology leadership positions at Microsoft and in the US Department of Defense.