Web Hacking Essentials: Applying a hacker's mindset

Training Course

30th & 31st 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 by going to the website https://appsecday.io/.

Course Abstract

The course focuses on core web application penetration testing skills from the offensive side. This course is suitable for developers, anyone new to penetration testing or anyone wishing to explore the area by gaining real hands on skills. The aim of the course is to provide attendees with a hacker's mindset and the methodology and skills required for testing web application security. Students who complete the course will actively detect and exploit the OWASP Top Ten on their own laptops in class.

The structure of the two day course includes a deep drive into each topic, followed by alternating hands on learning exercises to support the learning. Each topic is also supported by coverage of the latest research in the field with references for post course development and progression.

The guided hands on exercises support students in developing a hacker's mindset and thinking in abuse cases rather than use cases.

What attendees will learn?

- OWASP Top Ten.
- Detection and exploitation of security issues.
- Learn how to think like an attacker.
- A solid methodology and skillset for continuing the journey into advanced web application hacking and bug bounties.

What attendees will be provided?

- Slides for the training course.
- Virtual Machine(s) with all the required software and reference material.
- Access to online exercises during the class.

What attendees should bring?

- A laptop where you are the administrator or have root access.

- The laptop should have enough RAM and CPU to run two virtual machines at the same time and have the ability to copy from a USB.
- On some machines you will need to have the ability to enable virtualisation in the BIOS.
- Please download, install and test the latest installation of Oracle VM VirtualBox.
- Please download, install and test the Kali Linux operating system OVA file for VirtualBox.
- A willingness to cover a lot of ground in two days!

Pre-requisites

Introductory knowledge of web application development and Linux will help but is not essential. Introductory knowledge of the command line on your platform of choice.

Detailed Outline

Day 1

- **Introduction**
  - Thinking like a hacker
  - The information security community
  - How to start your journey
- **Information gathering**
  - How attackers research a target company
  - How attackers research a target company's employees
  - Discovering domains, subdomains and IPs for a target company
  - Discovering the technology stack of components
  - Using existing password leaks
  - Using automated and manual techniques
- **Introduction to web application testing, issues and tools**
  - Overview of network protocols
  - Overview of the TCP protocol
  - Overview of common languages and frameworks you will encounter when testing
  - Overview of the OWASP Top Ten
  - Introduction to the Burp Web Application proxy
- **Cross Site Scripting (XSS) detection and exploitation**
  - Overview of XSS and the associated risks
  - Using a methodology to test for XSS manually
  - How to detect XSS manually within a target web site
  - Thinking like an attacker when bypassing defences such as WAFs
  - How to exploit XSS using the Browser Exploitation Framework (BeEF)
  - How to prevent and remediate XSS
- **SQL Injection (SQLi) detection and exploitation**
  - Overview of SQLi and the associated risks
  - Using a methodology to test for SQLi manually
  - How to detect SQLi manually within a target web site
  - Thinking like an attacker when bypassing defences such as WAFs

- How to exploit SQLi manually
- How to exploit SQLi automatically using tools
- Observe that automated tools do not find all the issues
- How to prevent and remediate SQLi

Day 2

- **Broken Access Control**
  - Overview of access control and what can go wrong
  - Insecure Directory Object References (iDOR) and the associated risks
  - How to test for broken access control and iDOR manually within a target web site
  - How to prevent broken access control and iDOR
- **Exploiting insecure file uploads**
  - Overview of insecure file uploads and the associated risks
  - How to detect insecure file uploads within a target web site
  - Thinking like an attacker when bypassing defences
  - How to exploit insecure file uploads manually
  - How to prevent insecure file upload issues
- **XML External Entity (XXE) detection and exploitation**
  - Overview of XXE attacks and the associated risks
  - Using a methodology to test for XXE manually
  - How to detect XXE manually within a target web site
  - How to exploit XXE manually
  - How to prevent and remediate XXE
- **Insecure deserialisation detection and exploitation**
  - Overview of insecure deserialisation attacks and the associated risks
  - How to detect insecure deserialisation manually within a target web site
  - How to exploit insecure deserialisation manually
  - How to prevent and remediate insecure deserialisation
- **Bug Bounty Methodologies, CTFs and putting it all together**
  - Strategies for using your new testing knowledge
  - Strategies for applying your new testing knowledge within your organisation
  - How to continue your journey

Trainer Biography

Dr. Pamela O'Shea

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

Pamela O'Shea is director of Shea Information Security. Pamela started as a software developer in PHP, Java and C# for companies such as an internet service provider, Discovery Channel Animal Planet and the London Stock Exchange.

Since then, Pamela has worked as a security consultant for the last ten years. Eight of these have been as a full-time penetration tester for some of Australia's largest companies across the financial, government, media, resources and telecommunications sectors.

Pamela is also a university lecturer for the practical ethical hacking module in the RMIT master's in cyber security programme.

Pamela is on the paper review boards for Black Hat Asia, BSides Canberra and OWASP Melbourne and has taught workshops at hacking conferences such as 0xCC, BSides Canberra, Ruxcon, OWASP Melbourne and Platypuscon.

In her spare time, Pamela loves radios and is the founder of CyberSepectrum Melbourne, a meetup with a focus on software defined radio (SDR) and security of the airwaves.

Pamela has also been featured in the Sydney Morning Herald and The Age newspapers for careers in cyber security, as well as being interviewed on the Risky Business security podcast on web application security.