Orange Cyberdefense

SensePost Training

Applied Web Application Hacking

INTERMEDIATE TO ADVANCED LEVEL

Overview

Most organisations utilise web applications. Due to the exposed nature of web applications and complex business logic they contain, they are a valuable target for attackers. Throughout this course focus will be placed on the various vulnerabilities that could affect web applications.

This course will teach you how to analyse web applications for vulnerabilities and teach you how to exploit them in order improve your understanding of the inner workings and the associated risks.

Practical exposure to hacking web application will provide developers a deeper understanding of the potential threats and issues that could find its way into the development lifecycle and furthermore ensure that penetration testers are well versed with the discovery and exploitation of web related issues.

Who should attend

This course is for anyone who wants to understand how to attack and defend web applications and the related technologies.

This course is also ideal for any developer looking to further their understanding of where issues can come into play and to widen their understanding of vulnerabilities in web applications.

Skills you'll learn

- Enumeration
- Vulnerability Discovery
- Exploiting Techniques
- Attacking Applications

Training in a glance

16 core training modules

50 sub-modules and learning objectives

20 hands-on practicals

16 hours of training

Why our training is great

- Our training is provided by active penetration testers and security analyst
- Our training is hands-on with a course spilt of 40% theory and 60% practical
- We teach offensive methodologies to proactively enhance defensive thinking
- Each student gets their own lab environment during the course to practice real-world attacks

training@orangecyberdefense.com

orangecyberdefense.com

Orange Cyberdefense

SensePost Training

Applied Web Application Hacking

INTERMEDIATE TO ADVANCED LEVEL

Course Modules

1. Introduction To Web Technologies
2. Cookies And Session Management
3. Introduction To Web Vulnerabilities
4. Client And Server Side Attacks
5. Broken Authentication And Authorization
6. Enumeration
7. Session Identifier Disclosure
8. Insecure Direct Object References (IDOR)
9. Local File Inclusion (LFI) Vulnerabilities
10. Insecure File Upload Vulnerabilities
11. Injection
12. Cross-Site Scripting (XSS)
13. Cross Site Request Forgery (CSRF)
14. Command Injection
15. SQL Injection
16. Java Deserialization

All modules contains several sub-modules and practical exercises.

The above provides a summarised course outline, full course outline available on request.

Key take-aways

Greater understanding of the risks associated with web applications

A good understanding of the tools and techniques for examining web applications

Practical skills to exploit a wide variety of web application vulnerabilities

Prerequisites

A strong familiarity with Linux command line usage and basic security concepts.

A base understanding of web applications and technologies is a must. Development experience isn't a requirement but can help.

What you'll need

A laptop with a modern browser (Chrome or Firefox)

Zoom and/or Microsoft Teams installed

A Discord account

What you'll get

Lifetime access to our online class portal with the course resources and practical answer guides

Access to our realistic web hacking lab environment during the training

Value for your organisation

Understanding the potential risks associated to web applications and the threats your organization may be susceptible to.

Practical exposure to exploitation of web related issues leading to faster identification and mitigation in organizational application development.

training@orangecyberdefense.com

orangecyberdefense.com