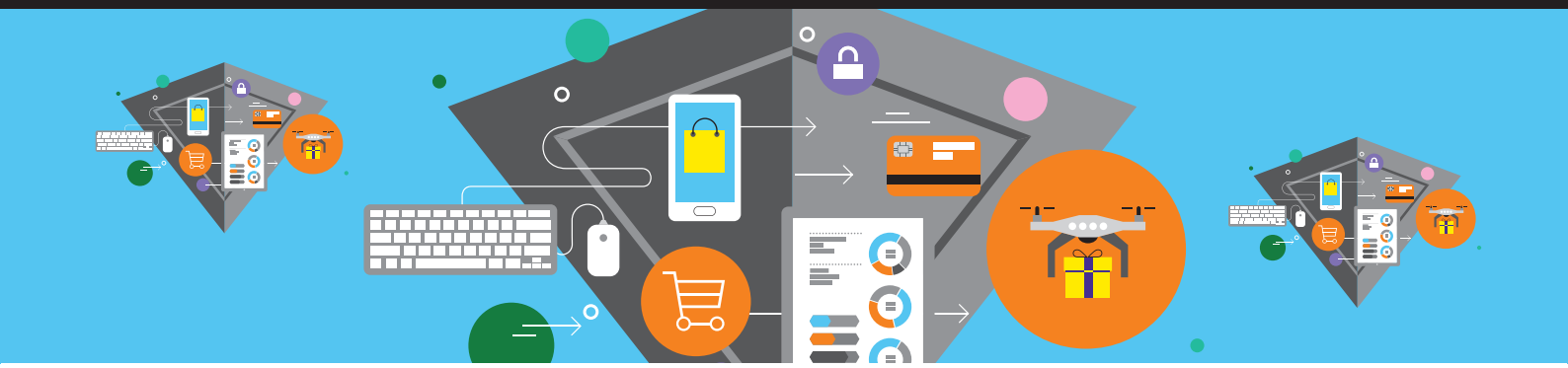
Orange Cyberdefense



SensePost training

Web Application Hacking

Key benefits

Understand
A general approach and methodology for hacking web applications.

Practical
Practical and practiced skills (there are a lot of pracs in this course).

Hands-on experience
A good understanding of the tools and techniques for examining web applications.

About the course

This course will teach you how to analyse web applications for vulnerabilities and exploit them.

SensePost has been conducting penetration tests against web applications for nearly two decades and has distilled its approach into this course. Providing a thorough and scientific approach, techniques to maximise coverage of an application will be taught. Whether you're a developer looking to better understand how to defend your applications or a penetration tester looking to enhance your web application bug hunting, this course is for you.

This course is highly practical, with over 22 different practical exercises. You'll learn how to hand exploit numerous common web vulnerabilities, and understand the theory behind them. You will be better able to help developers prevent these classes of attacks in their applications. We aim to teach you the trade not just the tricks, and while tools are covered and help, you will be taught how to exploit many of these vulnerabilities by hand.

Who is the course for

Defenders, developers or administrators looking to learn how to test web applications for vulnerabilities as well as penetration testers with limited web application experience looking to expand their skill set in this area.

Why Orange Cyberdefense

Cybersecurity specialists
Orange Cyberdefense specialises in cybersecurity services and solutions, with a 25-year track record of delivering managed services to some of the largest companies in the world.

Outstanding expertise
Our Managed Firewall service is delivered by our UK-based SOC - delivering immediate, 24x7x365 access to specialists who deal with device health incidents, requested and recommended changes, security optimisation and help ensure continuous availability.

Extensive security insight
Orange Cyberdefense's Threat Intelligence platform processes over 30 billion security events per month, giving us unparalleled access to current and emerging threats. SensePost, our elite consulting arm, is at the forefront of cybersecurity - providing insight into the criminal mind-set. We use this information to ensure our Managed Firewall customers are as secure as they possibly can be.

Vendor insights
Our close partnership with Check Point, Fortinet, Cisco and Palo Alto Networks provides superior access to their technical experts and product roadmaps - keeping our SOC's knowledge ahead of the game.

Complementary services
We offer a broad range of services that complement our Managed Firewall service and strengthen your security posture, including Managed IDS/IPS, Managed Threat Detection, Managed Vulnerability Scanning and Managed Compliance Monitoring.

What is covered

Introduction to web technologies

- Understanding the protocols that power the web and getting comfortable with how they look on the wire as well as intercepting and modifying them

Cookies and session management

- Understanding how sessions work in applications, and how cookies can be manipulated

Introduction to web vulnerabilities

- Theory on what a vulnerability is and an introduction to the OWASP Top 10

Client and server side attacks

- Understanding web architectures, and the threat models associated with them as well as several client and server-side vulnerabilities and related exploits

Indirect object references

- Identifying and exploiting poor authorisations controls
- Brute forcing for restricted data

Path traversal

- Exploiting path traversal vulnerabilities and bypass restrictions. Insecure file upload and file inclusion
- Introductions to web shells and code execution attacks. XSS/CSRF and DOM Injections and Cache Attacks
- Manipulating the DOM with various attacks
- The impact of CDNs and different browser headers

SQL and command injection attacks

- Understanding data store and operating system setups and how to exploit and explore them

Java deserialisation

- Exploiting deserialisation vulnerabilities with ysoserial

APIs, microservices and widgets

- Working with APIs, common formats, tools and vulnerabilities

Web assembly vulnerabilities

- Understanding wasm
- New attack surface exposed by wasm