

TRAINING | Developer



**Developer Edition**

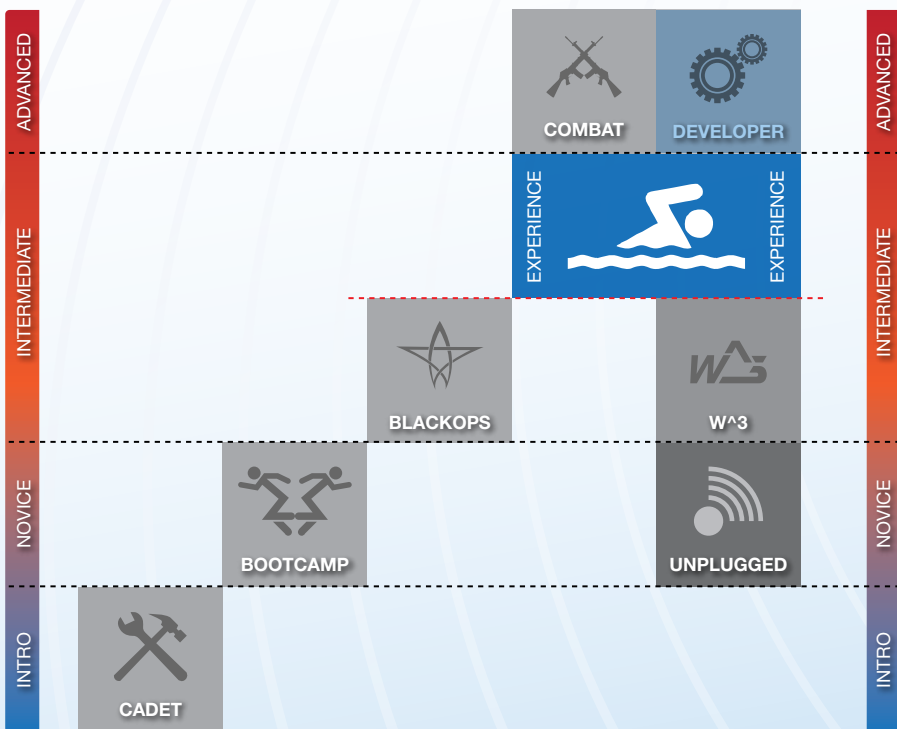
“Developer Edition” introduces a wide array of common (and not so common) web application security vulnerabilities. Students will be given hands-on lab exercises allowing them to attack vulnerable applications and to fully explore the impact of potentially vulnerable code.

The course is programming language neutral, aiming to equip developers with a security mindset more than a set of security functions or procedures, and will thus be of benefit to any developer who programs

for the web. Language and operating system specifics are included where required with the focus on the major development architectures currently used. Students will be exposed to the attack vectors commonly used, as well as techniques, processes and the mindset required to protect against them. Some of the “softer” issues surrounding secure development will also be covered.

Students should leave the course with a new mindset, aware of both the real nature of the threat and of the flaws in logic that normally make them possible.

**Training Overview**



**SensePost Information Security**

**Information Security**

As trusted advisors we deliver insight, information and systems to enable our customers to make informed decisions about Information Security that support their business performance.

SensePost is an independent and objective organisation specialising in Information Security Consulting, Training, Security Assessment Services and IT Vulnerability Management.

SensePost is about security. Specifically - Information Security. Even more specifically - measuring Information Security.

We’ve made it our mission to develop a set of competencies and services that deliver our customers with insight into the security posture of their information and information systems.

**Training Overview**

- Cadet Edition
- Cadet Online Edition
- Bootcamp Edition
- BlackOps Edition
- Combat Edition
- Unplugged Edition
- W^3 Edition
- Developer Edition

**What People Say**

“Good job! `<script>alert (“;-”)`  
`</script>`”

TRAINING | Developer

Content

1. Introduction

- Security Fundamentals.
- Fundamental principles for Application Hacking.
- Application Assessment Methodology.
- Vulnerabilities and Exploits.

2. Background Concepts

- HTTP.
- SSL.
- Firewalls and network Security.
- HTTP Methods and Error Codes.
- Web Servers and Web Server Technologies.
- HTTPS URLs.
- HTML Forms.
- HTTP on the Wire.
- Web Applications Languages.
- Database Technologies.
- SQL.

3. Web Application Attack Categories

- Tools for Web Application Hacking.
- Information Gathering.
- File System and Directory Traversal.
- Command Execution.
- SQL Query Injection.
- Cross Site Scripting.
- Impersonation Attacks.
- Parameter Passing Attacks.

4. Advanced Hacking Techniques

- Advanced SQL Hacking.
- Advanced thinking about Brute Forcing.
- XML Injection.
- LDAP Injection.
- Automated Application Testing.

5. Hacking "Thick" Applications

- Principles of Application Security.
- Attacking Java Applications.
- Attacking Web Services.

6. Defending Applications

- Application Defence Strategy.
- Application Defence Tactics.
- Secure Coding Techniques and Best Practice.
- Threat Modelling.

Each section details how attacks take place, why they take place and explains the mechanisms that need to be considered to prevent these attacks from taking place.

Context

This course can be taken independently of all the other HBN courses, although completion of "Cadet Edition" before hand is recommended. It should be noted that this is a course for capable web developers with development skills and experience.

Prerequisites

SensePost will provide fully configured laptop computers as well as CDs with all the tools and materials used on the course. Students are expected to be versed in basic programming or scripting, networking and Internet technologies and 'nix and Windows operating systems. No advanced skills are required, but students without a good, practical knowledge of these areas will fall behind in this fast-paced class. Students without the requisite technical skills are encouraged to consider "Cadet Edition".

Who Should Attend

Developers and Project Managers benefit hugely from this course by learning how to spot badly written code, how to prevent such errors and how to effectively integrate security and security testing into the development process for the future. Administrators and Security Consultants will benefit by learning how to securely deploy custom-written

applications, how to detect security errors and how to provide effective remedial advice.

More Training At SensePost



CADET

Cadet Edition

is an introductory course for technical students with no previous experience in the world of hacking. The course will present the student background information, technical skills and basic concepts required to get the student going.



BOOTCAMP

Bootcamp Edition

is the core of the HBN series. A highly practical course that teaches method-based hacker thinking, skills and techniques. This course continues to receive support and acclaim from all over the world.



BLACKOPS

BlackOps Edition

is a course to sharpen the student's skills in real scenarios before being shipped off to battle. "BlackOps" covers tools and techniques to brush up skills on data exfiltration, privilege escalation, pivoting, client-side attacks and exploit writing.



COMBAT

Combat Edition

is an unique concept - a series of carefully crafted Capture-The-Flag "missions", each designed to teach a specific hacking skill or concept. This course is all hack, no talk. "Combat" has been described as "Zen" for hackers.



UNPLUGGED

Unplugged Edition

is the ultimate wi-fi hacking course. With a strong focus on obtaining results in offensive scenarios for wi-fi hacking. Presents students with the background knowledge, methodologies, tools and thinking skills required.



W^3

W^3 Edition

is an intermediate web application hacking course for students with some experience in penetration testing. "W^3" is a hands-on, highly practical course which aims to enable students to understand the trade and not the trick of breaking webapps.



DEVELOPER

Developer Edition

introduces a wide array of common (and not so common) web application security vulnerabilities. Students are given hands-on lab exercises allowing them to attack vulnerable applications and to fully explore the impact of potentially vulnerable code.