SecDev Course for Software Engineers

Web and mobile applications are a potentially vulnerable entry point into your corporate network as they can be leveraged by hackers to gain access to your IT infrastructure. This course will teach developers to understand how attackers work and to take security into account when writing code.

This training, specially designed by Navixia, allows you as a developer to improve your understanding of operational IT security in relation to the development of applications. The interactive and practical course includes various labs reflecting concrete issues. You will concretely experiment the various code-related risks and their consequences, learn how to write safe code and to adopt a security-oriented approach to IT development in general.

Relevant Training Modules

The course is tailored to address the security-related issues you are facing every day as a developer. The selection of modules we have assembled will let you handle the most important aspects of application-related security in a well-informed manner. You get to address vulnerabilities from the respective angles of the attacker (hacker) and/or the defender (developer).

Improved Corporate IT Security

There is a marked improvement in IT security once you, as a developer, are aware of code-related potential risks and know how to prevent them. This affords the company a more effective protection.

Why is this course useful ?

When coding software or applications, it is essential for a developer to know what kind of weaknesses hackers are looking for. This course will make you think like a hacker and give you the necessary tools to significantly improve code security.

Who should take part ?

This course is specially designed for **developers**, **software architects** or any person who is required to code or integrate web or mobile applications as part of their activities.

Highly Qualified Instructors

Navixia's instructors have an extended experience, both as pen testers and as developers. As a result, they have a pragmatic and concrete vision of the operational attack/defence procedures, and are thus able to give relevant advice adapted to the reality of the field.

Practical Details

- **Duration**: 2 days
- **Location**: Navixia's training centre in Ecublens
- **Language**: French (English on request)
- **Cost** : CHF 2'500 / person
- **Course fees include**: Training provided by a qualified instructor; (b) All equipment, machines and software used during the course; (c) Course documentation; (d) Lunch, including drinks; (e) Coffee breaks; (f) Attendance certificate.

The training takes place from 4 participants.

Course Syllabus

Footprinting

Understanding the importance of restricting as much as possible any information about internal infrastructure, framework and technologies used, so as not to provide attackers with information they can exploit to launch attacks related to specific tools or vulnerabilities. Learning to limit information provided by the code.

Injections (SQL / NOSQL)

Understanding how an attacker can exploit the specific properties of an application to communicate directly with the database and thus recover or inject data that would normally not be accessible. Analysing methods that sanitise input data. Learning to code safely and avoid these risks.

Authentication

Understanding how an attacker can exploit features related to login and identification procedures in order to access protected resources. Learning how to avoid such risks when coding.

Sensitive Data Exposure

Understanding how and where an application's confidential data is to be stored. Understanding the difference between user-accessible information and data that is exclusively kept on the server side.

Using Components with Known Vulns

Understanding what type of attacks can be executed from known public vulnerabilities and how to prevent such risks.

Broken Access Control

Understanding how an attacker can take advantage of flaws in the access control procedure to reach resources whose access is normally protected by authentication. Learning to counter such threats when coding.

Crypto : Hash Function

Understanding the crucial importance of hashing passwords in databases. Analysing the robustness of various existing hash functions and learning how to use them effectively.

Crypto : mastering SSL settings

Analysing SSL settings and the properties of an SSL certificate.

Secure API

Understanding how to build a robust application programming interface (API). Analysing, from the angle of security, the different authentication methods an API can use (password, key, token). Put these notions into practice.

Session Management

Understanding how to handle sessions on the client side and what are the best life cycle related practices (creation, verification, expiration). Analysing the various ways to manage a client side session and its properties (length, entropy, content).