Secure Coding for Web & App Developers

Developers don't have the skills or resources to code securely.
— FORRESTER

WHY YOU NEED SECURE CODING

Improve pass rate of penetration testing and security audits

Shorten time-to-market by proactively preventing security flaws

Comply with CERT Secure Coding Standards and secure coding requirements from suppliers

According to Forrester*, web applications and software vulnerabilities are the top two ways external attacks are carried out. Research found that even top universities either don't offer secure coding education as part of their curriculum, or don't require secure code training to graduate with a computer science degree.

The most cost-effective way to protect organizations from dangerous attacks and undesired data breaches is to equip developers with secure coding skills.

42% of external attacks involve software exploitation*

35% involve web application vulnerabilities*

3.86M average cost of a data breach in 2020**

*Forrester Analytics Global Business Technographics Security Survey, 2019.
** IBM and Ponemon Institute, Cost of a Data Breach Report 2020

CURRICULUM

1. **INFORMATION SECURITY CONCEPTS**
   Encryption, data protection, patch management, release management, etc.
2. **OWASP TOP 10 WEB APPLICATION SECURITY RISKS**
   Injection attacks, security misconfigurations, broken access control, etc.
3. **SECURE CODE REVIEW**
   Secure code review process, manual vs automated, peer review.
4. **OWASP SECURE CODING BEST PRACTICES**
   Input validation, sanitization, parameterized queries, etc.
5. **APPLYING CODING BEST PRACTICES INTO DAILY PROCESSES**
   Cheat sheets, techniques, efficient implementation, etc.

Secure Code Training for Your Web and Application Developers

In this short course, developers will enhance their software security skills and learn to recognize potential vulnerabilities in web applications and implement secure coding practices throughout the software development lifecycle. Through a unique combination of 7 hours of live sessions, 25 hours of self-paced learning, plus an 8-hour capstone project, developers will gain the skills to increase resilience of their web applications and avoid costly data breaches.

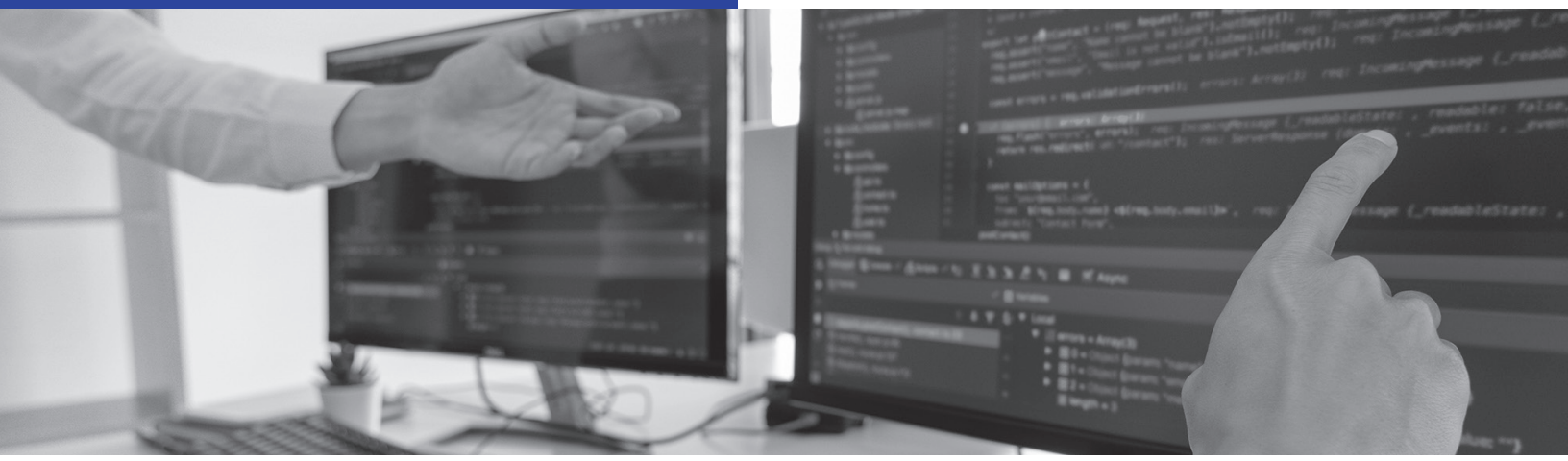
Workshop Requirements

Participants must be familiar with HTML, CSS, JavaScript, and preferably one of the following programming languages: Python, Java, NodeJS, php, C#.

Capstone Project — Security Architecture

Through an 8-hour capstone project, participants will apply what they learn to a real world project from the day to day job and bring immediate and tangible value to their organization. Each learner will create an high level design (HLD) for a web application, for which they will design their own architecture, assess potential risks, and implement security countermeasures.

Course Fee: Php 30,000 (VAT EX.)



XEPTO™ Cybint MANTUA CYBERSECURITY