# Secure Web Application Development and Testing For Devops

Learn via: **Classroom / Virtual Classroom / Online**

Duration: **3 Day**

**https://bilginc.com/en/training/secure-web-application-development-and-testing-for-devops-349-training/**

## Overview

Protecting applications that are accessible via the web requires well-prepared security professional who are at all time aware of current attack methods and trends. Plethora of technologies and environments exist that allow comfortable development of web applications. One should not only be aware of the security issues relevant to these platforms, but also of all general vulnerabilities that apply regardless of the used development tools.

The course gives an overview of the applicable security solutions in web applications, with a special focus on understanding the most important cryptographic solutions to be applied. The various web application vulnerabilities are presented both on the server side (following the OWASP Top Ten) and the client side, demonstrated through the relevant attacks, and followed by the recommended coding techniques and mitigation methods to avoid the associated problems. The subject of secure coding is wrapped up by discussing some typical security-relevant programming mistakes in the domain of input validation, improper use of security features and code quality.

Testing plays a very important role in ensuring security and robustness of web applications. Various approaches – from high level auditing through penetration testing to ethical hacking – can be applied to find vulnerabilities of different types. However if you want to go beyond the easy-to-find low-hanging fruits, security testing should be well planned and properly executed. Remember: security testers should ideally find all bugs to protect a system, while for adversaries it is enough to find one exploitable vulnerability to penetrate into it.

Practical exercises will help understanding web application vulnerabilities, programming mistakes and most importantly the mitigation techniques, together with hands-on trials of various testing tools from security scanners, through sniffers, proxy servers, fuzzing tools to static source code analyzers.

## Prerequisites

There are no prerequisites for this course.

## Who Should Attend

Web developers, architects and testers.

## What You Will Learn

- Understand basic concepts of security, IT security and secure coding
- Learn Web vulnerabilities beyond OWASP Top Ten and know how to avoid them
- Learn about XML security
- Learn client-side vulnerabilities and secure coding practices
- Have a practical understanding of cryptography
- Understand essential security protocols
- Understand security testing approaches and methodologies
- Get practical knowledge in using security testing techniques and tools
- Get sources and further readings on secure coding practices

## Outline

- IT security and secure coding
- Web application security
- Client-side security
- Practical cryptography
- Security protocols
- Security testing
- Security testing techniques and tools

- Principles of security and secure coding
- Knowledge sources