



## **Understanding the OWASP® Top 10 Security Threats** (SKF100)

Equip yourself to identify and address security risks, protect information & ensure online integrity.

## Duration: 2 Days

## **Prerequisites for this course**

- Basic Knowledge of Web Technologies: You should have a fundamental understanding of web technologies such as HTML, CSS, JavaScript, and server-side scripting languages. This knowledge will provide a foundation for understanding web application security concepts.
- Familiarity with Web Application Architecture: A basic understanding of how web applications are structured and function is essential. You should be familiar with concepts such as client-server architecture, HTTP protocols, and how data is transmitted between the client and server.
- Basic Programming Skills: While not mandatory, basic programming skills would be beneficial. Familiarity with a programming language such as Python, Java, or JavaScript will enable you to better grasp the technical aspects of web application vulnerabilities and their exploitation.
- General Cybersecurity Awareness: You should have a basic understanding of cybersecurity principles, including concepts such as confidentiality, integrity, and availability. Familiarity with common security terms and practices will aid in comprehending the importance of web application security.

## **Outline for this course**

- Chapter 1 Course Introduction
- Chapter 2 Introduction to Web Application Security
- Chapter 3 Broken Access Controls
- Chapter 4 Cryptographic Failures
- Chapter 5 Injection
- Chapter 6 Insecure Design
- Chapter 7 Security Misconfiguration
- Chapter 8 Vulnerable and Outdated Components





- Chapter 9 Identification and Authentication Failures
- Chapter 10 Software and Data Integrity Failures
- Chapter 11 Security Logging and Monitoring Failures
- Chapter 12 Server-Side Request Forgery (SSRF)