# Certified Secure Web Application Engineer

**Modality: On Demand**

**Duration: 7 Hours**

## About this course:

This arrangement covers all that you have to think about turning into a Certified Secure Web Application Engineer. Learners will find out about the security of web application, secure SDLC, threat modeling, risk management, session management, OWASP TOP 10, authentication and authorization attacks, input validation and data sanitization, security architecture, insecurity code discovery and mitigation, AJAX security, cryptography, application mapping, and testing methodologies.

As an engineer of Secure Web Application, you will realize how to recognize, defend and mitigate against security vulnerabilities in software applications, through planning and building frameworks that are impervious to failure. You will guard associations when they are directing business through the web. Having secure coding aptitudes is a need in this day and age when the web is one of the riskiest spots to work together, with incalculable instances of data being taken from organizations in light of the fact that there was powerlessness in their web applications.

## Course Objective:

- Comprehend the concepts of the security of web applications.
- Implement authorization and authentication policies
- Learn about risk management and threat modeling.
- Forestall meeting the board assaults
- Understand secure SDLC
- Review and write codes for security testing
- Perform penetration testing of web application
- Learn cryptography.

## Audience:

- Web application engineers
- Application developers
- IT managers
- Computer programmers

## Prerequisite:

The applicants picking to enlist for this course are required to have at least two years of expert

experience ideally in a cloud situation with solid information on operating systems, networking, programming, and open shell.

## Course Outline:

- Module 01 - Web Application Security
- Module 02 - Secure SDLC
- Module 03 - OWASP TOP 10
- Module 04 - Risk Management
- Module 05 - Threat Modeling
- Module 06 - Authentication and Authorization Attacks
- Module 07 - Session Management
- Module 08 - Security Architecture
- Module 09 - Input Validation and Data Sanitization
- Module 10 - AJAX Security
- Module 11 - Insecurity Code Discovery and Mitigation
- Module 12 - Application Mapping
- Module 13 - Cryptography
- Module 14 - Testing Methodologies