Certified Secure Web Application Engineer

Modality: On Demand

Duration: 7 Hours

About this course:

The Certified Secure Web Application Engineer course is designed to provide knowledge and skills to individuals about identifying, mitigating, and defending any possible attacks. Through the course, an individual can learn about designing and building secure systems, which are resistant to failures. The Certified Secure Web Application Engineer course will also enlighten an individual to develop an application without any vulnerabilities securely. Moreover, the course will also focus on testing techniques to validate security, reliability, and resistance to application against attacks.

The Certified Secure Web Application Engineer course will cover the following topics.

- Web Application Security
- Secure SDLC
- OWASP TOP 10
- Risk Management
- Threat Modeling
- Authentication and Authorization of Attacks
- Session Management
- Security Architecture
- Input Validation and Data Sanitization
- AJAX Security
- Insecurity Code Discovery and Mitigation
- Application Mapping
- Cryptography
- Testing Methodologies

Course Objective:

The objectives of the Certified Secure Web Application Engineer course are as follows.

- Provide understanding and concepts of web application security.
- Provide an understanding of threat modeling and risk management.
- Provide knowledge and skills to implement authentication and authorization policies.
- Provide knowledge and skills to prevent session management attacks.
- Provide knowledge and skills in regards to writing and reviewing codes for security testing.
- Provide knowledge and skills to perform web application penetration testing.
- Provide an understanding of secure SDLC.
- Provide an understanding of cryptography.

Audience:

Following can take up the Certified Secure Web Application Engineer course.

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

Prerequisite:

- Strong knowledge of networking, operating systems, programming, and open shell.
- Minimum two years of working experience in the field of cloud environment.

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