Document Generated: 12/16/2025

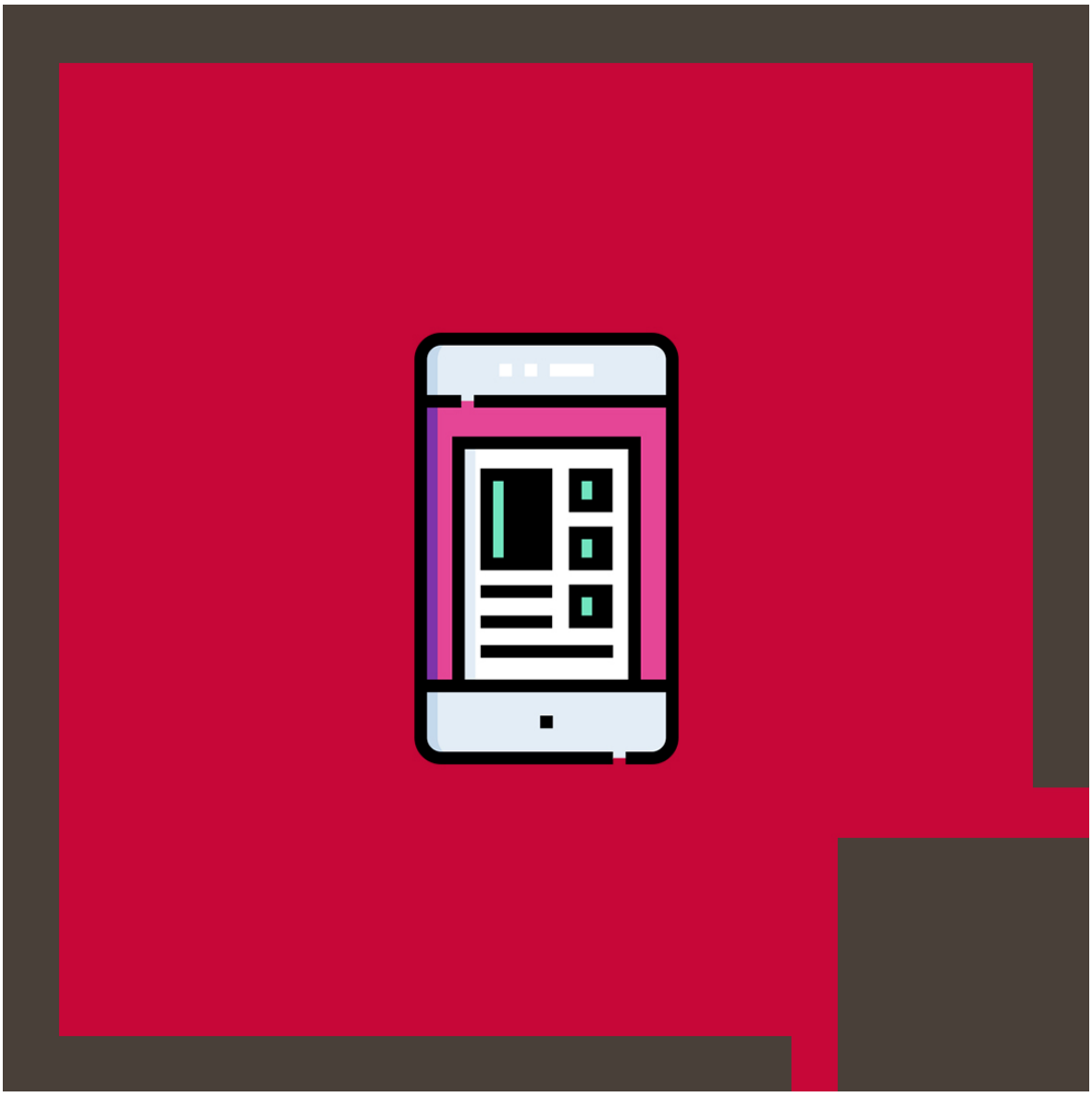
Learning Style: On Demand

Technology:

Difficulty: Intermediate

Course Duration: 7 Hours

Certified Secure Web Application Engineer



About this course:

This series covers everything you need to know about becoming a Certified Secure Web Application Engineer. Students will learn about web application security, secureSDLC, OWASP TOP 10, risk management, threat modeling, authentication and authorization attacks, session management, security architecture, input validation and data sanitization, AJAX security, insecurity code discovery and mitigation, application mapping, cryptography, and testing methodologies.

As a Secure Web Application Engineer you will know how to identify, mitigate and defend against security vulnerabilities in software applications, through designing and building systems that are resistant to failure. You will keep organizations safe when they are conducting business through the internet. Possessing secure coding skills is a necessity in today's world when the internet is one of the most dangerous places to do business, with countless cases of information being stolen from businesses because there was a vulnerability in their web applications.

Course Objective:

- Understand the concepts of web application security
- Learn about threat modeling and risk management
- Implement authentication and authorization policies
- Prevent session management attacks
- Write and review codes for security testing
- Perform web application penetration testing
- Understand secure SDLC
- Learn cryptography

Audience:

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

Prerequisite:

- The candidates opting to register for this course are required to have a minimum of two years of professional experience preferably in a cloud environment with strong knowledge of networking, operating systems, 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