Introduction

Module 1 - Web Application Security challenges

The module is not about how the code is written securely or how the application is tested in depth. The module speaks about the real time scenarios and challenges which are faced during managing the application security program.

Module 2 – Advanced Web application attacks and remedy

The module explains what are all the advanced attacks which can be placed and there basic root cause. This module also covers the best practices to mitigate the attack.

Module 3 – Secure Software Development Life Cycle (SDLC)

This module speaks about how the security can be incorporated or identified in the software engineering principles. This explains the engagement of security best practices with the water fall model of Software design life cycle.

Module 4 – Threat modelling and Pursuit of security threats

This module is about the approach for analyzing the security of an application. It defines structured approach that enables you to identify, quantify, and address the security risks associated with an application

Module 5 – Web server security

The World Wide Web (WWW) is a system for exchanging information over the Internet. Web server is the most targeted and attacked host on most organizations' network. As a result, it is essential to secure Web servers and the network infrastructure that supports them. This module covers the best practices to secure a web server.

Module 6 – Secure architecture of web sites and web deployment infrastructure

To build a secure Web application, you need an appropriate architecture and design. The cost and effort of retrofitting security after development are too high. An architecture and design review helps you validate the security-related design features of your application before you start the development phase.

Module 7 – Security Auditing and fault tolerance

Most of the organizations doesn’t care about the policies and procedures unless some attacker forces them to hire a auditor. This module speaks about some best practices and principles regarding the security audit.

Module 8 – Code obfuscation attack scenarios

The module covers the basics of Code obfuscation techniques and related attacks and mitigations which are spread to different platforms.

Module 9 – Memory corruption attacks and Security configurations

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts

Module 10 – Authentication, Cryptography and Digital Signatures

Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages

Module 11 - Web DDOS attack and its prevention

Module 12 - Mitigation of Business critical risk areas

Module 13 - Creating Fault Tolerance

Module 14 - Incident Response