Web Application Security Testing

Introduction

Skills-Factory's Web Application Security Testing course will be valuable to software developers and programmers like to code and develop highly secure applications and web applications.
.
.Net and JAVA are widely used by almost all organizations as the leading framework to build web applications. The course teaches developers how to identify security flaws and implement security countermeasures throughout the software development life cycle to improve the overall quality of products and applications.

Skills-Factory's Web Application Security Testing lays the foundation required by all application developers and development organizations to produce applications with greater stability and fewer security risks to the consumer. The Skills-Factory's Web Application Security Testing standardizes the knowledge base for application development by incorporating the best practices followed by experienced experts in the various domains.

This course is purposefully built with labs peppered throughout training, offering participants critical hands on time to fully grasp the new techniques and strategies in secure programming as well as in security testing.

Minimum qualification for certification

Aspirant candidates from all IT and Non IT educational background Under graduates/ Post Graduate, who's having eager to work in information security field…

Duration of the Course
Total 40 hours learning

The Course
The changing business environment is compelling organizations to rely on an increasingly complex information technology infrastructure. While it can provide avenues to make information flow faster and cheaper, it may expose organizations to new and varied business risks and challenges. For starters, it can complicate the process of discovering electronic facts when organizations need it the most.

(i) To impart up-to-the-minute knowledge to faculty so that they can transmit relevant and current technologies to the participants in the most effective manner, particularly those skills that match practical practices in Web Application Security Testing.

(ii) Programming Security procedures and highly productive policies for Code writing, Code testing, SDLC, Threat modelling, Development modelling and delivery of software product.

(iv) Tooling support for investigations and disputes of information threats and vulnerabilities (Identification and mitigation). This training will propose of in detail procedures for collection, segregation, categorisation, preservation and procedurals as well as practical implementation of variety of Information Security standards, Network Security standards and equipment's.

What you will achieve
Upon successful completion of this course, participants will be able to:

The content gives a comprehensive picture of the latest technologies employed Secure Testing of Web Applications and provides the relevant updating that are necessary and crucial enough to be transmitted to participants, so that participants are fully equipped to deal with all types of Web application security and fault acquisition issues when they come out for the network security and cyber related cases and needs for Web Application security testing and secure programing.

will enable to implement upgradations in their real and virtual infrastructure in terms of hardware, software, systems and processes, with special emphasis on procedure and policy implementation through advanced and upgraded knowledge of Web Application Security Management System.

What you can become

Web Application Security Testing
A highly trained cyber security professionals and Network Security Expert as well niche experts to meet the huge and rising demand for knowledgeable and skilled professionals who can implement and initiate effective Information Security Management System (ISMS) and inject specialised knowledge in their respective works. The teachings have to be practical-oriented and immediately implementable in any environment.

Employment/Career prospects
The content gives a comprehensive picture of the latest technologies employed Secure Testing of Web Applications and provides the relevant updating that are necessary and crucial enough to be transmitted to participants, so that participants are fully equipped to deal with all types of Web application security and fault acquisition issues when they come out for the network security and cyber related cases and needs for Web Application security testing and secure programing ; it will enable to implement upgradations in their real and virtual infrastructure in terms of hardware, software, systems and processes, with special emphasis on procedure and policy implementation through advanced and upgraded knowledge of Web Application Security Management System.

Content (in brief)

Module 1	Web Application Security challenges
Module 2	Advanced Web application attacks and remedy
Module 3	Secure Software Development Life Cycle (SDLC)
Module 4	Threat modelling and Pursuit of security threats
Module 5	Web server security
Module 6	Secure architecture of web sites and web deployment infrastructure
Module 7	Security Auditing and fault tolerance
Module 8	Code ofsecution attack scenarios
Module 9	Memory corruption attacks and Security configurations
Module 10	Authentication, Cryptography and Digital Signatures
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