OWASP: Threats Fundamentals

Modality: On Demand

Duration: 4 Hours

About this course:

The OWASP: Threats Fundamental course is one of the training courses under the Open Web Application Security Project (OWASP) series, which was established with the aim of enhancing the security of the applications. Through OWASP, a trusted way is provided for conceiving, acquiring, developing, operating and maintaining the applications. OWASP documents, tools, chapters and forums are open to all free of cost in order to improve application security. Through this course, an individual can get an overview of the basic concepts, which are integral to the OWASP core values.

The OWASP: Threats Fundamental course is outlined to provide basic fundamental concepts and techniques, which are required to identify various kinds of threats. The course also provides knowledge related to data exposure and cryptography along with concepts to improve security by eliminating risk of misconfiguration.

The expected annual salary of an Information Security Analyst is around **$89,000** per annum.

Course Objective:

The course is designed to provide the following knowledge to an individual;

- Understanding of the top ten threats in respect of an application.
- Understanding of authentication and session threats along with the identification process.
- Understanding in terms of avoiding security misconfiguration threats.
- Understanding about the prevention of sensitive data from exposure.
- Usage of functional level access control in order to improve security.

Audience:

The course is beneficial for the following;

- Network security engineers
- Application security engineers
- Ethical hackers
- Software developers

Prerequisite:

An individual undertaking the course must have basic knowledge of network security and web applications. The course is also beneficial for the developers already on job.

Course Outline:

Chapter 01 - Understanding Threats

- Topic A: OWASP Overview - Part 1
- OWASP Overview - Part 2
- OWASP Overview - Part 3
- Topic B: Top Ten Threats - Part 1
- Top Ten Threats - Part 2
- Top Ten Threats - Part 3
- Review - Question

Chapter 02 - Session Security

- Topic A: Authentication and Session Threats - Part 1
- Authentication and Session Threats - Part 2
- Authentication and Session Threats - Part 3
- Topic B: Threat Examples - Part 1
- Threat Examples - Part 2
- Threat Examples - Part 3
- Review - Question

Chapter 03 - Security Misconfiguration

- Topic A: Security Misconfiguration - Part 1
- Security Misconfiguration - Part 2
- Security Misconfiguration - Part 3
- Topic B: Misconfiguration Examples - Part 1
- Misconfiguration Examples - Part 2
- Misconfiguration Examples - Part 3
- Review - Question

Chapter 04 - Data Exposure and Cryptography

- Topic A: Sensitive Data Exposure - Part 1
- Sensitive Data Exposure - Part 2
- Sensitive Data Exposure - Part 3
- Topic B: Insecure Cryptographic Storage - Part 1
- Insecure Cryptographic Storage - Part 2
- Insecure Cryptographic Storage - Part 3
- Topic C: Function Level Access Control - Part 1
- Function Level Access Control - Part 2
- Function Level Access Control - Part 3
- Review - Question