OWASP: Threats Fundamentals

Modality: Self-Paced Learning

Duration: 4 Hours

About this course:

The Open Web Application Security Project (OWASP): Threats Fundamental course is among the learning courses under the OWASP series that was designed to enhance the security of the applications. With OWASP, a reliable way is offered for developing, operating, acquiring, maintaining, and deploying the applications. OWASP tools, documents, forums, and chapters are available to all free of charges to improve application security. Under this course, a candidate can get an outline of the fundamental concepts, which are vital to the OWASP core values.

The OWASP: Threats Fundamental course is designed to offer essential fundamental techniques and concepts, which are necessary to recognize different sorts of threats. The course additionally offers understanding and knowledge concerned to cryptography and data exposure together with ideas to improve security by elimination risk of misconfiguration.

Salary Estimate:

The professional after the completion of this course can expect to make $89,000/- per annum.

Course Objective:

This course is intended to offer the following knowledge to the candidate;

- Knowledge in terms of preventing security misconfiguration threats.
- Knowledge of the top 10 threats in in regards of an application.
- Knowledge regarding the prevention of sensitive data from exposure.
- Knowledge of session and authentication threats as well as identification process.
- Use of functional level access control to improve security.

Audience:

The course is advantageous for the following;

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

Prerequisite:

The candidate attempting this exam are required to have fundamental knowledge of web applications and network security. The course is also helpful 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