Document Generated: 05/04/2026

Learning Style: On Demand

Technology:

Difficulty: Beginner

Course Duration: 4 Hours

OWASP: Threats Fundamentals

About this course:

The OWASP: Threats Fundamentals course is part of a series of training courses on the Open Web Application Security Project (OWASP). This course covers the fundamental concepts and techniques to identify different types of threats. The course also teaches the students to improve the security by avoiding misconfigurations, data exposure and insecure cryptography.

The OWASP Foundation was established with a purpose to secure the applications in such a way that they can be conceived, developed, acquired, operated, and maintained in a trusted way. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security. This course along with the other courses in the series on OWASP provides a basic overview of the concepts that form an integral part of the OWASP core values.

The average salary of a Information Security Analyst is **$89,000** per year.

Course Objective:

- Understand the top 10 threats to any application
- Learn and identify authentication and session threats
- Avoid security misconfiguration threats
- Prevent sensitive data exposure
- Use function level access control to improve security

Audience:

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

Prerequisite:

- The course requires basic knowledge of web applications and network security. Prior experience of working in a development environment is recommended but not required.

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

Credly Badge:

Display your Completion Badge And Get The Recognition You Deserve.

Add a completion and readiness badge to your Linkedin profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:

- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific

skills you developed.

Badges are issued by QuickStart and verified through Credly.

Find Out More or See List Of Badges