

OWASP: Proactive Controls

Modality: Self-Paced Learning

Duration: 3 Hours

SATV Value:

CLC:

NATU:

SUBSCRIPTION: Learn, Master

About this course:

The OWASP: Proactive Controls is a collection of learning courses on the OWASP. The Open Web Application Security Project top 10 Proactive Controls is a list of security methods that need to be incorporated in overall software development project. They are highly important, with control number one being the most significant. This program helps the engineers who are recently involve to secure development to assure application security.

The Open Web Application Security Project base was set up with a reason to protect the applications so that they can be developed, operated, acquired, maintained, and conceived reliably. The entirety of the OWASP documents, chapters, tools, and forums are open and free to any person engaged in enhancing application security. The OWASP series of courses offers a fundamental outline of the concepts that are very important to the OWASP essential values.

Salary Estimate:

The Information Security Analyst can earn an average salary of \$89,000 per annum.

Course Objective:

- Proactive Control One - Verify Security
- Proactive Control Two - Parameterize Queries
- Proactive Control Three - Encode Data
- Proactive Control Four - Validate Inputs
- Proactive Control Five - Identity and Authentication Controls
- Proactive Control Six - Implement Access Controls
- Proactive Control Seven - Protect Data
- Proactive Control Eight - Logging and Intrusion Detection
- Proactive Control Nine - Security Frameworks
- Proactive Control Ten - Exception Handling

Audience:

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

Prerequisite:

- Candidates needs to have a fundamental knowledge and understanding of network security and web applications. Past working experience in development environment is Recommended but not necessary.

Course Outline:

Chapter 01 - Controls 1-5

- Topic A: Overview - Part 1
- Overview - Part 2
- Overview - Part 3
- Topic B: Verify Security - Part 1
- Verify Security - Part 2
- Verify Security - Part 3
- Topic C: Parameterize Queries - Part 1
- Parameterize Queries - Part 2
- Parameterize Queries - Part 3
- Topic D: Encode Data - Part 1
- Encode Data - Part 2
- Encode Data - Part 3
- Topic E: Validate Inputs - Part 1
- Validate Inputs - Part 2
- Validate Inputs - Part 3
- Topic F: Identity and Authentication Controls - Part 1
- Identity and Authentication Controls - Part 2
- Identity and Authentication Controls - Part 3
- Review - Question

Chapter 02 - Controls 6-10

- Topic A: Implement Access Controls - Part 1
- Implement Access Controls - Part 2
- Implement Access Controls - Part 3
- Topic B: Protect Data - Part 1
- Protect Data - Part 2
- Protect Data - Part 3
- Topic C: Logging and Intrusion Detection - Part 1

- Logging and Intrusion Detection - Part 2
- Logging and Intrusion Detection - Part 3
- Topic D: Security Frameworks and Exception Handling - Part 1
- Security Frameworks and Exception Handling - Part 2
- Security Frameworks and Exception Handling - Part 3
- Review - Question