OWASP: Proactive Controls

Modality: Self-Paced Learning

Duration: 3 Hours

SUBSCRIPTION: Learn, Master, Master Plus

About this course:

The OWASP: Proactive Controls course is part of a series of training courses on the Open Web Application Security Project (OWASP). The OWASP Top Ten Proactive Controls is a list of security techniques that should be included in every software development project. They are ordered by order of importance, with control number 1 being the most important. This training assists the developers who are new to secure development to ensure application security.

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:

- Proactive Control 1: Verify Security
- Proactive Control 2: Parameterize Queries
- Proactive Control 3: Encode Data
- Proactive Control 4: Validate Inputs
- Proactive Control 5: Identity and Authentication Controls
- Proactive Control 6: Implement Access Controls
- Proactive Control 7: Protect Data
- Proactive Control 8: Logging and Intrusion Detection
- Proactive Control 9: Security Frameworks
- Proactive Control 10: Exception Handling

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 - 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