OWASP: Proactive Controls

Modality: On Demand

Duration: 3 Hours

About this course:

This course provides conceptual knowledge of 10 Proactive Controls that must be adopted in every single software and application development project. Listed with respect to priority and importance, these ten controls are designed to augment the standards of application security. This course is a part of the Open Web Application Security Project (OWASP) training courses designed Software Engineers, Cybersecurity Professionals, Network Security Engineers, and Ethical Hackers.

Identification of vulnerabilities and threats plays a crucial role in setting up a secure information system and neutralizing the weak links in a network and application. The Open Web Application Security Project (OWASP) focuses primarily on helping companies implement high-end security and develop and maintain information systems with zero vulnerabilities. This course is designed for network security engineers and IT professionals having knowledge and experience of working in network security and application development environment.

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

Course Objective:

- Security Verification
- Prepared Statement and Parameterized Queries
- Encoding Data
- Input Validation
- Identity Management and Authentication Controls
- Access Control Implementation
- Data Protection
- Intrusion and Logging Detection
- Exception Handling
- Security Frameworks

Audience:

- Software Engineers and Ethical Hackers
- Application Security Developers and Engineers
- Network Security Developers and Engineers

Prerequisite:

- Professionals with knowledge and understanding of Network Security and Web Application Development
- Professional development environment experience is highly recommended but not mandatory

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