COURSE SYLLABUS

Web Application Security Fundamentals

Ten hours on web application security for technical and oversight staff alike — the policy landscape, the OWASP Top 10, secure development, access control, and monitoring. No lab required.

Group classes (Live Online) and onsite training are available for this course. For more information, email corporate@nobledesktop.com or visit: https://www.nobledesktop.com/classes/web-application-security-fundamentals



hello@nobledesktop.com • (212) 226-4149

Course Outline

Module 1

- Foundations of Web Application Security and the Federal Policy Landscape
- What a web application is and why it is a common attack surface
- The CIA triad applied to federal systems
- Threat actors from nation-state to insider
- Shared responsibility across developers, system owners, ISSOs and users
- FISMA, the Risk Management Framework and the authorization process, Executive Order 14028 and its amendments, and Cybersecurity Framework 2.0
- How to tell when a policy has been superseded

Module 2

- Common Web Application Vulnerabilities
- How the OWASP Top 10 is developed and why federal secure-coding guidance references it
- The 2025 edition categories including broken access control, cryptographic failures, injection, insecure design and misconfiguration, software supply chain failures, authentication failures, mishandling of exceptional conditions, and logging and alerting failures
- Why each is consequential for federal systems

Module 3

- Secure Development Practices and the Secure SDLC
- The phases of a secure development lifecycle
- Input validation, output encoding, least privilege, secure defaults and failing securely
- Security requirements and threat modeling before code is written
- Static and dynamic testing at a conceptual level
- Open-source and software supply chain risk
- How secure development supports the path to an authorization to operate

Module 4

- Authentication, Access Control, and Data Protection
- Authentication versus authorization
- Multifactor authentication and federal digital identity assurance levels
- Role-based and attribute-based access control and least privilege
- Zero Trust principles applied to web applications
- Protecting data at rest and in transit including FIPS-validated encryption
- Common mistakes such as exposing sensitive data in URLs and weak session management

Module 5

- Monitoring, Incident Response, and Ongoing Compliance
- Continuous monitoring under the Risk Management Framework
- Federal event-logging expectations for incident investigation
- Recognizing and reporting a suspected web application incident
- How FISMA reporting and periodic reauthorization keep systems accountable
- What any employee should do on suspecting a compromise