Mastering Java Web Security: From Attacks to Fortification

Duration: *4 Day(s)*

Course Overview

Enhance your proficiency in Java Web security with our training that blends theoretical knowledge with practical application. This course is designed for Java web developers eager to expand their skill set in bug detection, ethical hacking, and the implementation of security measures. Expect real-world case studies and dynamic labs as you learn to protect your digital assets. Graduates will leave armed with the expertise to safeguard applications, improve debugging capabilities, and prevent security threats effectively.

Review this course online at https://www.alta3.com/courses/A3-8320-J

Objectives

- Understand secure coding principles to prevent exploits.
- Establish a defense plan for web application security.
- Implement ethical hacking techniques responsibly.
- Identify and remediate common software vulnerabilities.

Who Should Attend

- Experienced Java developers
- Software engineers focused on security
- Web application architects
- Security-focused IT professionals

Prerequisites

- Intermediate Java coding skills
- Experience in Java web development

Course Outline

Introduction to Bug Hunting

1. Importance of Bug Hunting
2. Cybersecurity Language
3. Evolution of Cybersecurity
4. Analyzing AppSec through SolarWinds

Ethical and Effective Bug Hunting

5. Ethical Guidelines for Bug Hunters
6. Importance of Privacy
7. Notifying Defects

8. Avoiding Common Pitfalls

Advancing Beyond Bug Hunting

9. Strategies for Bug Elimination
10. Overview of OWASP Top Ten
11. Understanding CWE and WASC
12. Microsoft's Security Perspective

Handling Unvalidated Data

13. Common Weaknesses in Unvalidated Data
14. Setting Trust Boundaries
15. Lists for Validation
16. Challenges with Inputs

Managing Access Control Breaches

17. Issues with Access Controls
18. Preventing Unauthorized Access
19. Metadata and Cookies Risks

Addressing Cryptographic Shortcomings

20. Identifying Data Protection Needs
21. Securing Data in Transit
22. Key Management Techniques

Ensuring Robust Injection Defenses

23. Common Injection Vulnerabilities
24. SQL Injection Misconceptions
25. Server and Client-Side Injection Tactics

Designing with Security in Mind

26. Shifting Left for Secure Processes
27. Actionable Practices for Security

Configuring Security Correctly

28. Hardening Systems
29. Secure Baseline Configurations
30. Container and Cloud Segmentation

Handling Vulnerable Components

31. Inventory and Manage Updates
32. Implement Virtual Patching

Strengthening Authentication Processes

33. Quality of Authentication Data
34. Multi-factor Authentication Practices
35. Hashing and Password Handling

Maintaining Data Integrity

36. Trusted Software Repositories
37. Serialization/Deserialization Risks

Enhancing Logging and Monitoring

38. Best Practices for Security Logs
39. Supporting Forensics through Safe Logging

Mitigating Server Side Request Forgeries

40. Understanding and Defending Against SSRF

Planning for Continued Security

41. Understanding Common Vulnerabilities
42. Establishing a Secure Development Lifecycle
43. Applying SDL Techniques in Practice