CA501: Web Application Security

60 Instructional Hours 80 CPEs 20 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

ADVANCED

This course provides a comprehensive and practical exploration of web application security, focusing on the principles, methodologies, and tools required to identify, assess, and mitigate vulnerabilities. It covers foundational cybersecurity concepts, web technologies such as HTTP and APIs, and progresses into advanced security testing techniques including vulnerability assessment, penetration testing, and exploitation methods. Learners are introduced to industry standards such as OWASP, NIST, and PTES, and gain hands-on understanding of both manual and automated testing approaches. The course blends theoretical knowledge with real-world application, equipping learners with the skills needed to analyze, test, and secure modern web applications effectively.

You Will Be Able To

- Identify and analyze common web application vulnerabilities and attack vectors
- Perform structured vulnerability assessments and penetration testing activities
- Understand and manipulate HTTP protocols, requests, and responses for security testing
- Use industry-standard tools (e.g., Burp Suite, OWASP ZAP, Nessus) for web security testing
- Evaluate authentication, authorization, and session management mechanisms for weaknesses
- Apply security testing methodologies aligned with OWASP, NIST

Who Should Attend

This course is designed for individuals with a foundational understanding of cybersecurity who want to specialize in web application security. It is suitable for aspiring penetration testers, security analysts, and developers seeking to understand how applications are attacked and secured. The course is also valuable for IT professionals and engineers responsible for securing web-based systems and applications, as well as those preparing for roles in offensive or defensive cybersecurity.

Relevant Combat Roles

- Web Application Penetration Tester
- Security Analyst
- Application Security Engineer
- Red Team Operator
- Vulnerability Assessment Specialist
- Cybersecurity Consultant

Topics Covered

Cybersecurity & Web Fundamentals
(threats, vulnerabilities, risks, exploits, payloads, web architecture, HTTP protocol, APIs including REST/SOAP/GraphQL)

Security Testing Methodologies & Standards
(information gathering, enumeration, vulnerability assessment, penetration testing, OWASP Top 10, ASVS, NIST, OSSTMM, PTES, SAST/DAST tools)

Authentication, Authorization & Session Management
(OAuth, AWS Cognito, weak password policies, authentication bypass, privilege escalation, IDOR, session attacks, JWT, CSRF, brute force, cookie security)

Input Validation & Injection Attacks
(XSS—stored/reflected/DOM, SQL/NoSQL injection, command injection, SSRF, XXE, template injection, LDAP/XML/XPath injection, file inclusion, HTTP smuggling)

Client-Side & Server-Side Vulnerabilities
(CORS, clickjacking, browser storage, client-side manipulation, business logic flaws, WAF bypass, access control issues, error handling and misconfigurations)

Advanced Attacks & Security Risks
(RCE, insecure deserialization, DoS/DDoS, dependency confusion, zero-day hunting, advanced exploitation techniques)

Labs

Web Application Enumeration & Testing
(information gathering, endpoint discovery, basic vulnerability assessment)

Authentication & Access Control Attacks
(weak passwords, authentication bypass, IDOR, privilege escalation)

Session Management & Web Attacks
(session fixation, CSRF, cookie analysis, JWT attacks)

Injection Attacks Lab
(SQL injection, XSS (stored/reflected), command injection, file inclusion)

Client-Side & API Security Testing
(DOM XSS, CORS issues, API testing with REST/GraphQL)

Advanced Web Exploitation Lab
(SSRF, RCE concepts, WAF bypass techniques, security misconfigurations)