Application Security (AppSec) Testing and Vulnerability Management Training Course

Professional Development Training Course Outline

Category	Defense and Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today’s fast-paced digital environment, organizations face increasing threats from cyberattacks, data breaches, and application-layer vulnerabilities. Application Security (AppSec) Testing and Vulnerability Management is essential to safeguard software applications, protect sensitive data, and ensure business continuity. Application Security (AppSec) Testing and Vulnerability Management Training Course equips participants with practical knowledge on identifying, analyzing, and mitigating security vulnerabilities across web, mobile, and cloud-based applications. It covers the latest techniques in static and dynamic application security testing, penetration testing, secure coding practices, and risk management strategies.

Participants will gain hands-on experience in vulnerability assessment, remediation planning, and compliance with security standards such as OWASP Top 10, NIST, and ISO 27001. The training emphasizes integrating security into the software development lifecycle, automating testing processes, and prioritizing vulnerabilities based on impact and risk. By the end of this course, learners will be able to implement robust AppSec frameworks, improve organizational resilience, and reduce the likelihood of security incidents affecting applications and infrastructure.

Programme Curriculum

Application Security (AppSec) Testing and Vulnerability Management Training Course

Introduction

In today’s fast-paced digital environment, organizations face increasing threats from cyberattacks, data breaches, and application-layer vulnerabilities. Application Security (AppSec) Testing and Vulnerability Management is essential to safeguard software applications, protect sensitive data, and ensure business continuity. Application Security (AppSec) Testing and Vulnerability Management Training Course equips participants with practical knowledge on identifying, analyzing, and mitigating security vulnerabilities across

web, mobile, and cloud-based applications. It covers the latest techniques in static and dynamic application security testing, penetration testing, secure coding practices, and risk management strategies.

Participants will gain hands-on experience in vulnerability assessment, remediation planning, and compliance with security standards such as OWASP Top 10, NIST, and ISO 27001. The training emphasizes integrating security into the software development lifecycle, automating testing processes, and prioritizing vulnerabilities based on impact and risk. By the end of this course, learners will be able to implement robust AppSec frameworks, improve organizational resilience, and reduce the likelihood of security incidents affecting applications and infrastructure.

Course Objectives

1. Understand key concepts and principles of application security and vulnerability management.
2. Identify common application vulnerabilities using OWASP Top 10 and other standards.
3. Conduct static application security testing (SAST) and dynamic application security testing (DAST).
4. Perform penetration testing on web, mobile, and cloud-based applications.
5. Analyze and prioritize vulnerabilities based on risk, impact, and exploitability.
6. Apply secure coding practices to prevent common application security flaws.
7. Integrate security testing into the software development lifecycle (SDLC).
8. Use automated vulnerability scanning tools effectively.
9. Develop remediation strategies and patch management processes.
10. Ensure compliance with security standards and regulatory requirements.
11. Monitor and report on application security metrics and key performance indicators.
12. Build an organizational culture of security awareness and proactive risk management.
13. Implement continuous improvement processes for AppSec programs.

Organizational Benefits

- Improved identification and mitigation of application vulnerabilities
- Reduced risk of data breaches and cyberattacks
- Enhanced compliance with industry security standards
- Strengthened secure software development lifecycle processes
- Increased efficiency through automated vulnerability scanning
- Better risk prioritization and remediation planning
- Stronger incident response and recovery capabilities
- Improved stakeholder trust and client confidence
- Enhanced security awareness among development and IT teams
- Reduced financial and reputational losses due to security incidents

Target Audiences

- Software developers and application engineers
- Security analysts and IT auditors
- Penetration testers and ethical hackers
- IT operations and DevOps professionals
- Risk management and compliance officers
- Cybersecurity managers and team leads
- Software quality assurance (QA) testers
- Security consultants and advisors

Course Duration: 5 days

Course Modules

Module 1: Introduction to Application Security

- Overview of AppSec principles and frameworks
- Importance of security in the software development lifecycle
- Threat landscape and emerging application risks
- Key compliance standards and regulations
- Roles and responsibilities in application security
- Case Study: Security breach in a financial application

Module 2: Understanding Vulnerabilities and Threats

- Common application vulnerabilities (OWASP Top 10)
- Exploit techniques and threat modeling
- Risk assessment and vulnerability scoring
- Identifying weak spots in web, mobile, and cloud applications
- Tools for vulnerability identification and reporting
- Case Study: Exploitation of SQL injection in an enterprise app

Module 3: Static Application Security Testing (SAST)

- Principles and methodology of SAST
- Integrating SAST into development pipelines
- Identifying insecure code patterns and logic flaws
- Configuring and running SAST tools
- Reporting and tracking SAST findings
- Case Study: Using SAST to identify vulnerabilities in open-source software

Module 4: Dynamic Application Security Testing (DAST)

- Fundamentals of DAST and runtime analysis
- Detecting vulnerabilities in running applications
- Automated scanning versus manual testing
- Prioritizing findings based on risk and impact
- Integration of DAST with continuous integration (CI/CD)
- Case Study: DAST identifying cross-site scripting in a web app

Module 5: Penetration Testing Techniques

- Planning and scoping penetration tests
- Manual testing methodologies for web and mobile apps
- Exploiting vulnerabilities safely in a controlled environment
- Reporting findings and remediation guidance
- Ethical and legal considerations in pen testing
- Case Study: Penetration testing for a mobile banking application

Module 6: Secure Coding Practices

- Principles of secure coding and input validation
- Avoiding common vulnerabilities (e.g., XSS, SQLi, CSRF)
- Secure authentication and session management techniques

- Code review and pair programming for security
- Integration of secure coding in agile development processes
- Case Study: Refactoring vulnerable code in a legacy system

Module 7: Remediation and Patch Management

- Prioritizing vulnerabilities for remediation
- Patch deployment best practices
- Change management and testing for security fixes
- Continuous monitoring for new threats
- Documentation and reporting for compliance purposes
- Case Study: Patch management to mitigate zero-day exploits

Module 8: AppSec Program Implementation

- Building organizational AppSec strategy and policies
- Metrics and KPIs for security performance
- Staff training and awareness programs
- Security governance and oversight mechanisms
- Continuous improvement and audit readiness
- Case Study: Launching a corporate AppSec program

Training Methodology

- Instructor-led sessions with interactive discussions
- Hands-on labs with SAST, DAST, and penetration testing tools
- Case study analysis of real-world application security incidents
- Group exercises for threat modeling and risk assessment
- Practical exercises in remediation planning and patch management
- Knowledge assessments and feedback sessions

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
02 Nov 2026	06 Nov 2026	Online	$1,000
02 Nov 2026	06 Nov 2026	Physical	$1,500
02 Nov 2026	06 Nov 2026	Physical	$3,000
02 Nov 2026	06 Nov 2026	Physical	$3,000
02 Nov 2026	06 Nov 2026	Physical	$6,000
02 Nov 2026	06 Nov 2026	Physical	$4,500
02 Nov 2026	06 Nov 2026	Physical	$6,000
02 Nov 2026	06 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com