Web Application Hacking and Security (WAHS) 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

Web applications are among the most targeted digital assets in today’s interconnected environment. Organizations face constant threats from hackers attempting to exploit vulnerabilities to gain unauthorized access, steal data, or disrupt services. Web Application Hacking and Security (WAHS) Training Course provides participants with a deep understanding of web application security principles, common attack vectors, threat modeling, and defense mechanisms. The course emphasizes practical approaches to detecting vulnerabilities, implementing protective controls, and securing web applications across multiple platforms and environments. Participants will gain hands-on experience in ethical hacking, penetration testing, and the use of advanced security tools to identify and mitigate risks effectively.

With the increasing complexity of web technologies and growing regulatory and compliance requirements, organizations need professionals who can assess security risks, manage vulnerabilities, and ensure resilience against cyber threats. This course enables participants to understand the latest hacking techniques, learn industry-standard best practices, and design robust security measures. By bridging theory and practice, learners will develop the expertise to strengthen web application security posture, protect sensitive data, comply with standards, and minimize potential breaches. The insights gained will empower participants to proactively secure organizational assets while staying ahead of evolving cyber threats.

Programme Curriculum

Web Application Hacking and Security (WAHS) Training Course

Introduction

Web applications are among the most targeted digital assets in today’s interconnected environment. Organizations face constant threats from hackers attempting to exploit vulnerabilities to gain unauthorized access, steal data, or disrupt services. Web Application Hacking and Security (WAHS) Training Course

provides participants with a deep understanding of web application security principles, common attack vectors, threat modeling, and defense mechanisms. The course emphasizes practical approaches to detecting vulnerabilities, implementing protective controls, and securing web applications across multiple platforms and environments. Participants will gain hands-on experience in ethical hacking, penetration testing, and the use of advanced security tools to identify and mitigate risks effectively.

With the increasing complexity of web technologies and growing regulatory and compliance requirements, organizations need professionals who can assess security risks, manage vulnerabilities, and ensure resilience against cyber threats. This course enables participants to understand the latest hacking techniques, learn industry-standard best practices, and design robust security measures. By bridging theory and practice, learners will develop the expertise to strengthen web application security posture, protect sensitive data, comply with standards, and minimize potential breaches. The insights gained will empower participants to proactively secure organizational assets while staying ahead of evolving cyber threats.

Course Objectives

1. Understand the fundamentals of web application architecture and security principles.
2. Identify and analyze common web application vulnerabilities (OWASP Top 10).
3. Apply ethical hacking and penetration testing techniques to detect security weaknesses.
4. Utilize security tools to assess and protect web applications.
5. Implement secure coding practices to prevent common attacks.
6. Conduct vulnerability assessments and risk analysis of web applications.
7. Understand session management, authentication, and authorization security.
8. Apply network and application-layer defense mechanisms.
9. Explore SQL injection, XSS, CSRF, and other common web attacks.
10. Analyze real-world web hacking case studies for practical insights.
11. Develop incident response strategies and mitigation plans.
12. Ensure compliance with web security standards and regulatory frameworks.
13. Strengthen organizational security posture through proactive web defense strategies.

Organizational Benefits

- Enhanced protection against web-based attacks and breaches
- Reduced operational and reputational risk from cyber threats
- Improved compliance with industry security standards and regulations
- Strengthened incident detection and response capabilities
- Increased staff awareness and technical expertise in web security
- Reduced financial losses from cybercrime and data breaches
- Enhanced confidence of clients, partners, and stakeholders
- Improved secure coding and development practices
- Better risk management across web applications and IT infrastructure
- Continuous monitoring and assessment of web security posture

Target Audiences

- Web developers and software engineers
- IT security officers and cyber defense teams
- Penetration testers and ethical hackers
- Network administrators and system architects
- Risk management and compliance officers

- Security auditors and consultants
- CTOs, CIOs, and IT managers
- Students and researchers in cybersecurity

Course Duration: 5 days

Course Modules

Module 1: Introduction to Web Application Security

- Overview of web applications and common architectures
- Introduction to web security principles and frameworks
- Threat modeling and risk assessment fundamentals
- Understanding attack surfaces and vectors
- Security standards and compliance overview
- Case Study: Security assessment of a web portal in a financial institution

Module 2: Ethical Hacking and Penetration Testing

- Principles of ethical hacking and legal considerations
- Reconnaissance and footprinting techniques
- Scanning and enumeration of web applications
- Exploitation methodologies and reporting findings
- Prioritizing vulnerabilities based on impact and risk
- Case Study: Penetration test on an e-commerce platform

Module 3: OWASP Top 10 Vulnerabilities

- Understanding common vulnerabilities (SQLi, XSS, CSRF, etc.)
- Practical detection and exploitation techniques
- Tools for identifying OWASP vulnerabilities
- Impact assessment of each vulnerability type
- Remediation strategies and prevention measures
- Case Study: Remediation of SQL injection vulnerabilities in a banking web app

Module 4: Secure Coding Practices

- Principles of secure software development
- Input validation and output encoding techniques
- Authentication and session management best practices
- Secure handling of sensitive data and secrets
- Continuous integration of security in development lifecycle
- Case Study: Secure coding implementation in a SaaS application

Module 5: Web Application Attack Techniques

- SQL injection, cross-site scripting, and cross-site request forgery
- Directory traversal and file inclusion attacks
- Session hijacking and cookie-based attacks
- Exploiting misconfigured servers and APIs
- Use of automated attack tools and scripts
- Case Study: Real-world exploitation scenario of a public-facing portal

Module 6: Web Application Security Tools

- Vulnerability scanners and penetration testing frameworks
- Web proxy tools for request and response analysis
- Security plugins and browser extensions
- Network and server monitoring tools
- Automation and reporting features of security tools
- Case Study: Tool-assisted security audit of a corporate website

Module 7: Incident Response and Mitigation

- Establishing incident response policies for web attacks
- Containment, eradication, and recovery procedures
- Root cause analysis and lessons learned
- Integration with organizational risk management
- Reporting and compliance requirements
- Case Study: Response to a compromised web application

Module 8: Advanced Web Security Measures

- Web application firewalls and intrusion detection systems
- Encryption, SSL/TLS, and secure communication protocols
- Multi-factor authentication and access control measures
- Monitoring, logging, and alerting best practices
- Future trends in web application security
- Case Study: Implementing layered defense in a high-traffic web service

Training Methodology

- Instructor-led theoretical sessions on web security fundamentals
- Hands-on labs with real-world web applications
- Practical exercises on ethical hacking and penetration testing
- Interactive group discussions and vulnerability analysis exercises
- Case study evaluations and lessons learned presentations
- Tool demonstrations and simulations for web security audits

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