Advanced Web Application Hacking and Exploitation Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Advanced Web Application Hacking and Exploitation Training Course is designed to elevate security professionals from intermediate penetration testing skills to the mastery of Advanced Web Exploitation techniques. The contemporary digital landscape is dominated by complex, feature-rich web applications, often built on modern frameworks, serverless architectures, and extensive API Security layers. Traditional vulnerability scanning falls short, making in-depth, manual Offensive Security tradecraft an essential skill. This course transcends the OWASP Top 10, focusing on deeply rooted, non-obvious flaws like advanced logic bypasses, complex deserialization, and chaining vulnerabilities for Remote Code Execution (RCE). Participants will adopt a Red Teaming mindset, learning to think like a persistent, sophisticated threat actor to uncover critical weaknesses in heavily fortified applications.

The curriculum is built around practical, Real-World Scenarios and custom-developed vulnerable applications, ensuring every participant can immediately apply learned techniques to complex, high-stakes engagements such as bug bounty hunting and professional penetration tests. Key areas of focus include bypassing modern security controls, exploiting Server-Side Request Forgery (SSRF) to compromise internal networks, and mastering Cryptographic Attacks against authentication mechanisms like JSON Web Tokens (JWT). Graduates will possess the expertise to conduct comprehensive, in-depth Web Application Penetration Testing, moving beyond surface-level flaws to discover and exploit the most impactful vulnerabilities that scanners miss, thereby becoming a critical asset in the domain of Cybersecurity and application defense.

Programme Curriculum

Advanced Web Application Hacking and Exploitation Training Course

Introduction

Advanced Web Application Hacking and Exploitation Training Course is designed to elevate security professionals from intermediate penetration testing skills to the mastery of Advanced Web Exploitation techniques. The contemporary digital landscape is dominated by complex, feature-rich web applications, often built on modern frameworks, serverless architectures, and extensive API Security layers. Traditional vulnerability scanning falls short, making in-depth, manual Offensive Security tradecraft an essential skill. This course transcends the OWASP Top 10, focusing on deeply rooted, non-obvious flaws like advanced logic bypasses, complex deserialization, and chaining vulnerabilities for Remote Code Execution (RCE). Participants will adopt a Red Teaming mindset, learning to think like a persistent, sophisticated threat actor to uncover critical weaknesses in heavily fortified applications.

The curriculum is built around practical, Real-World Scenarios and custom-developed vulnerable applications, ensuring every participant can immediately apply learned techniques to complex, high-stakes engagements such as bug bounty hunting and professional penetration tests. Key areas of focus include bypassing modern security controls, exploiting Server-Side Request Forgery (SSRF) to compromise internal networks, and mastering Cryptographic Attacks against authentication mechanisms like JSON Web Tokens (JWT). Graduates will possess the expertise to conduct comprehensive, in-depth Web Application Penetration Testing, moving beyond surface-level flaws to discover and exploit the most impactful vulnerabilities that scanners miss, thereby becoming a critical asset in the domain of Cybersecurity and application defense.

Course Duration

10 days

Course Objectives

Upon completion, participants will be able to:

1. Master advanced Web Exploitation techniques for complex, multi-layered applications.
2. Identify and bypass modern Web Application Firewall and security controls.
3. Perform in-depth API Penetration Testing on REST and GraphQL endpoints.
4. Discover and exploit critical Server-Side Request Forgery vulnerabilities for internal network pivoting.
5. Analyze and exploit common Deserialization Flaws leading to Remote Code Execution
6. Execute advanced attacks against Authentication and Authorization systems, including JWT Attacks and SSO Bypass.
7. Uncover and leverage subtle Business Logic Flaws and Race Conditions.
8. Conduct effective Source Code Review to identify non-obvious vulnerabilities.
9. Develop and customize powerful exploitation scripts and Burp Suite Extensions for automation.
10. Exploit modern browser security features and Client-Side Vulnerabilities like advanced XSS and Clickjacking.
11. Securely configure and audit applications to prevent the latest OWASP Top 10 risks.
12. Perform attacks against Cloud-Hosted Applications and serverless functions.
13. Apply a Red Teaming methodology to consistently deliver high-impact security findings.

Target Audience

1. Intermediate to Senior Penetration Testers
2. Security Architects and Consultants
3. Application Security Engineers
4. Bug Bounty Hunters seeking advanced skills
5. Red Team Operators
6. Security-focused DevOps Engineers

7. Incident Responders looking to understand attacker tradecraft
8. Software Developers aiming to master Secure Coding principles

Course Modules

1. Advanced Proxy and Fuzzing Techniques

- Mastering advanced Burp Suite Professional features.
- Customizing attack payloads and developing Burp Extensions
- Automating payload generation and using advanced fuzzing tools
- Bypassing common input filters and URL normalization defenses.
- Case Study: The use of custom Burp extensions to find an overlooked parameter that led to a mass assignment vulnerability in a major cloud service provider.

2. Deep Dive into Deserialization Attacks

- Understanding different serialization formats and their insecure implementations.
- Identifying and exploiting insecure YAML and JSON deserialization.
- Crafting custom gadget chains to achieve Remote Code Execution
- Mitigation strategies.
- Case Study: The widespread exploitation of a deserialization vulnerability in the Apache Struts framework and its advanced variants.

3. Server-Side Request Forgery Masterclass

- Exploiting basic SSRF to scan and query the internal network.
- Advanced SSRF Filter Bypass techniques
- Using SSRF to interact with Cloud Metadata APIs
- Exploiting SSRF for Serverless Function compromise and information disclosure.
- Case Study: The Capital One breach, where a misconfigured WAF and SSRF/SSRF-like attack led to the compromise of customer data via a metadata service.

4. Advanced Authentication and Authorization Bypass

- Attacks against JSON Web Tokens
- Exploiting Single Sign-On issues in SAML and OAuth 2.0 implementations.
- Bypassing Multi-Factor Authentication and rate-limiting controls.
- Second-Order and complex Insecure Direct Object Reference attacks.
- Case Study: The exploitation of JWT signature bypass vulnerabilities found in numerous applications allowing for privilege escalation to an admin account.

5. Cryptographic Attacks in Web Applications

- Exploiting weak cryptography.
- Applying attacks like Padding Oracle and Hash Length Extension against custom crypto schemes.
- Recovering plaintext from encrypted data using known-plaintext attacks.
- Understanding and attacking modern key exchange protocols
- Case Study: Real-world examples of Padding Oracle attacks against ASP.NET applications to achieve authentication bypass and decrypt sensitive data.

6. Complex Injection Attacks

- Manual and advanced automated Blind SQL Injection using time-based and OOB techniques.
- Exploiting NoSQL Injection for data exfiltration and RCE.
- Leveraging injection to achieve OS Command Execution and file system interaction.
- Bypassing WAFs and defensive coding using various encoding and obfuscation techniques.
- Case Study: The discovery of a complex, time-based blind NoSQL injection vulnerability in a major payment processing service that allowed full database enumeration.

7. Advanced Client-Side and Browser Attacks

- Advanced Cross-Site Scripting.
- Crafting payloads for DOM XSS using complex event handlers and JavaScript sandbox escapes.
- Exploiting WebSockets for Man-in-the-Middle and message injection.
- Deep analysis of Clickjacking and UI Redressing vulnerabilities.
- Case Study: Successful exploitation of a XSS vulnerability to perform a sophisticated Content Security Policy bypass and exfiltrate user session cookies.

8. Web Cache Deception and Poisoning

- Understanding how web caches and CDNs work.
- Performing Web Cache Deception attacks to steal sensitive, non-cached content.
- Executing Web Cache Poisoning to serve malicious content to other users.
- Exploiting misconfigured caching headers and key normalization.
- Case Study: A demonstration of a cache poisoning attack on a popular blog platform that resulted in the persistent delivery of malicious JavaScript to thousands of visitors.

9. Business Logic and Race Condition Exploitation

- Identifying subtle flaws in multi-step application workflows
- Exploiting Mass Assignment vulnerabilities via request parameters.
- Discovering and exploiting Race Conditions to trigger double-spending or unauthorized actions.
- Bypassing payment and financial controls through logic manipulation.
- Case Study: An analysis of a Bug Bounty finding where a successful race condition attack was used to claim multiple promo codes with a single-use token.

10. Attacking Modern API Gateways and Microservices

- API Gateway security testing and exploiting common configuration errors.
- Advanced GraphQL attack vectors.
- Testing for Authorization Flaws in microservice communication
- Exploiting insecure deployment pipelines and environment variables.
- Case Study: Compromising a microservice architecture by exploiting a trust relationship and a lack of proper authorization checks between internal APIs.

11. Exploiting Host Header and HTTP Request Smuggling

- Attacking applications that trust the HTTP Host Header for logic.
- Leveraging Subdomain Takeover techniques
- Performing classic and advanced HTTP Request Smuggling attacks
- Chaining smuggling attacks with other vulnerabilities
- Case Study: The use of an HTTP Request Smuggling attack to completely bypass an upstream WAF and compromise a user's session token.

12. Server-Side Template Injection

- Identifying and testing for SSTI in various templating engines
- Escalating SSTI to Remote Code Execution using sandbox escapes.
- Understanding the differences between client-side and server-side template injection.
- Developing payloads specific to different template environments.
- Case Study: Exploiting a Server-Side Template Injection flaw in a marketing platform that allowed an attacker to execute OS commands on the underlying server.

13. Advanced File Interaction Vulnerabilities

- Exploiting secure/hardened File Upload mechanisms with double extensions and content type bypasses.
- Advanced Local File Inclusion and Remote File Inclusion techniques.
- Exploiting file path traversal in application logic.
- Attacking XML and related processing using XML External Entity attacks.
- Case Study: A two-part attack where a secure file upload was bypassed to plant a webshell, followed by an LFI exploit to execute it.

14. Advanced Source Code Analysis

- Applying static and dynamic analysis tools for vulnerability discovery.
- Mastering the methodology of manual Code Review for security flaws.
- Identifying insecure patterns in popular languages
- Finding entry points and data flow issues leading to sinks.
- Case Study: Reviewing the vulnerable source code of a real-world application to manually find a flaw that an automated scanner missed, such as a subtle IDOR.

15. Real-World Vulnerability Chaining and Red Teaming

- Developing multi-stage attack scenarios to bypass layered defenses.
- Practicing Post-Exploitation techniques, including privilege escalation and pivoting.
- Simulating a full-scope Red Team operation on a web application.
- Effective vulnerability reporting and recommending robust mitigation strategies.
- Case Study: A comprehensive end-to-end hack of a simulated production environment involving chaining an SSRF, a deserialization flaw, and an IDOR to achieve full system compromise.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

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
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

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

Register Online Now

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