Bug Bounty Hunting Methodology and Tooling 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

The Bug Bounty Hunting Methodology and Tooling course is your definitive gateway into the lucrative and ethical world of vulnerability disclosure. Bug Bounty Hunting Methodology and Tooling Training Course is meticulously designed to break down the end-to-end process of a successful bug bounty hunt, from sophisticated asset discovery and vulnerability enumeration to professional proof-of-concept (PoC) creation and expert vulnerability reporting. You'll master industry-standard offensive security tools like Burp Suite Professional, Nmap, and specialized reconnaissance tools, enabling you to systematically uncover critical flaws like Server-Side Request Forgery (SSRF), Insecure Direct Object Reference (IDOR), and complex vulnerability chains in modern web applications and APIs. This course focuses on building a repeatable, efficient, and highly-rewarding hacking mindset, moving beyond basic scans to creative and deep-seated bug identification.

The curriculum is designed to transform enthusiastic beginners and intermediate security professionals into top-tier ethical hackers. It emphasizes a hands-on, lab-intensive learning experience, grounded in real-world case studies and practical bug bounty scenarios. By focusing on both cutting-edge tooling and a foundational understanding of web application security architecture, you will gain the competence to navigate the ethical and legal landscape of major bug bounty platforms like HackerOne and Bugcrowd. Graduates will be prepared to immediately apply a professional, process-driven methodology to identify high-impact, zero-day-potential vulnerabilities, significantly boosting their earnings and reputation in the cybersecurity community.

Programme Curriculum

Bug Bounty Hunting Methodology and Tooling Training Course

Introduction

The Bug Bounty Hunting Methodology and Tooling course is your definitive gateway into the lucrative and ethical world of vulnerability disclosure. Bug Bounty Hunting Methodology and Tooling Training Course is meticulously designed to break down the end-to-end process of a successful bug bounty hunt, from sophisticated asset discovery and vulnerability enumeration to professional proof-of-concept (PoC) creation and expert vulnerability reporting. You'll master industry-standard offensive security tools like Burp Suite Professional, Nmap, and specialized reconnaissance tools, enabling you to systematically uncover critical flaws like Server-Side Request Forgery (SSRF), Insecure Direct Object Reference (IDOR), and complex vulnerability chains in modern web applications and APIs. This course focuses on building a repeatable, efficient, and highly-rewarding hacking mindset, moving beyond basic scans to creative and deep-seated bug identification.

The curriculum is designed to transform enthusiastic beginners and intermediate security professionals into top-tier ethical hackers. It emphasizes a hands-on, lab-intensive learning experience, grounded in real-world case studies and practical bug bounty scenarios. By focusing on both cutting-edge tooling and a foundational understanding of web application security architecture, you will gain the competence to navigate the ethical and legal landscape of major bug bounty platforms like HackerOne and Bugcrowd. Graduates will be prepared to immediately apply a professional, process-driven methodology to identify high-impact, zero-day-potential vulnerabilities, significantly boosting their earnings and reputation in the cybersecurity community.

Course Duration

10 days

Course Objectives

The participant will be able to:

1. Master the Core Bug Bounty Methodology from scouting to submission.
2. Perform advanced Automated Reconnaissance and Asset Discovery.
3. Utilize Burp Suite Professional for effective Web Proxying and analysis.
4. Identify and exploit sophisticated Server-Side Request Forgery (SSRF) flaws.
5. Locate and bypass controls for Insecure Direct Object Reference (IDOR) vulnerabilities.
6. Discover and weaponize different types of Cross-Site Scripting (XSS) vulnerabilities.
7. Exploit common and blind SQL Injection (SQLi) and NoSQL Injection techniques.
8. Find and demonstrate Remote Code Execution (RCE) through various attack vectors.
9. Develop custom, complex Vulnerability Chains for maximum impact.
10. Systematically hunt for API Vulnerabilities and exploit GraphQL Endpoints.
11. Craft high-quality, professional Vulnerability Reports with clear Proof-of-Concept (PoC) steps.
12. Adhere to Responsible Disclosure standards and platform rules of engagement.
13. Integrate modern Open-Source Intelligence (OSINT) and Fuzzing Tools into a workflow.

Target Audience

1. Aspiring Bug Bounty Hunters
2. Junior Web Application Penetration Testers
3. Security Analysts and Consultants
4. Web Developers and Software Engineers
5. Ethical Hacking enthusiasts with basic web knowledge
6. Cybersecurity Students seeking practical skills
7. DevSecOps Professionals
8. IT Professionals aiming to transition into Offensive Security

Course Modules

Module 1: Bug Bounty Foundations and Methodology

- Introduction to the Bug Bounty Ecosystem
- Understanding Scope and Rules of Engagement
- Setting up the Optimal Hacking Environment
- Responsible Disclosure principles and legal considerations.
- Case Study: Analysis of a high-severity bug submission that was initially deemed Out-of-Scope but successfully argued for reward due to exceptional impact.

Module 2: Advanced Reconnaissance and Asset Discovery

- Passive Reconnaissance
- Active Reconnaissance
- Content Discovery and Hidden Directory Fuzzing
- JavaScript Analysis for forgotten endpoints and API keys
- Case Study: A successful takeover of a forgotten, low-hanging subdomain using Subdomain Takeover techniques discovered during advanced recon.

Module 3: Mastering Web Traffic and Proxying

- Deep dive into HTTP/S Protocols and web architecture.
- Setup and advanced usage of Burp Suite Proxy and Repeater.
- Effective use of Burp Suite extensions for workflow automation.
- Interception and modification of encrypted traffic.
- Case Study: How a simple response manipulation in Burp Repeater led to a Session Fixation vulnerability and an Account Takeover.

Module 4: Injection Vulnerabilities: SQL and NoSQL

- Fundamental concepts and detection of SQL Injection
- Exploiting different types.
- Introduction to NoSQL Injection in modern data stores.
- Automating exploitation with tools like SQLMap and manual bypass techniques.
- Case Study: A highly-rated Blind SQLi vulnerability chained with an un-restricted query to achieve full database exfiltration.

Module 5: Cross-Site Scripting

- Identification and exploitation of Reflected XSS.
- Finding and exploiting high-impact Stored XSS.
- Deep dive into DOM XSS and source/sink analysis.
- Bypassing Content Security Policy (CSP) and modern filters.
- Case Study: An awarded Stored XSS found in a profile picture upload feature that bypassed image validation and a strict CSP, leading to a wormable attack.

Module 6: Broken Access Control (BAC) and IDOR

- Understanding and testing for Vertical and Horizontal Privilege Escalation.
- Systematic hunting for Insecure Direct Object Reference
- Bypassing access controls using mass assignment and parameter manipulation.

- Common IDOR protection mechanisms and how to bypass them.
- Case Study: A simple ID change in a URL parameter that allowed viewing and modifying private customer orders, earning a critical rating.

Module 7: Server-Side Request Forgery

- Detection and exploitation of Basic SSRF.
- Techniques for bypassing firewalls and blacklists
- Exploiting Blind SSRF and Out-of-Band techniques.
- Chaining SSRF with other vulnerabilities for RCE or internal network access.
- Case Study: An SSRF vulnerability found in an image-processing service that was chained to scan the internal network and retrieve cloud metadata.

Module 8: Authentication and Session Flaws

- Testing for Broken Authentication
- Exploiting weak Session Management
- Identifying and exploiting Cross-Site Request Forgery
- Attack vectors related to JSON Web Tokens and stateless authentication.
- Case Study: A critical JWT misconfiguration that allowed an attacker to forge a token with admin privileges without a valid signature.

Module 9: File Upload and Command Injection

- Bypassing file type, size, and content validation for malicious file uploads.
- Exploiting directory traversal and Local File Inclusion
- Finding and exploiting OS Command Injection via different shell environments.
- Achieving a reverse shell via a file upload or command injection.
- Case Study: An LFI vulnerability in a language selector that was escalated to RCE by leveraging a log file poisoning technique.

Module 10: API Hacking Methodology

- Understanding REST and GraphQL API structures.
- Applying the OWASP API Security Top 10 to testing.
- Broken Object Level Authorization and API Rate Limiting bypasses.
- Fuzzing API endpoints for unexpected behavior and data leakage.
- Case Study: Discovery of a BOLA vulnerability in a GraphQL mutation that allowed an attacker to delete any user's account by predicting the object ID structure.

Module 11: Advanced Fuzzing and Brute Force

- Using Burp Intruder and Turbo Intruder for powerful parallel attacks.
- Advanced dictionary and payload generation techniques.
- Customizing attack types
- Detecting and bypassing rate-limiting mechanisms.
- Case Study: A clever Rate Limit Bypass on a password reset function that was used to successfully brute force a six-digit One-Time Password

Module 12: Business Logic and Race Condition Flaws

- Identifying flaws in the application's core business process

- Exploiting integer overflows and parameter manipulation.
- Detecting and exploiting Race Condition vulnerabilities for financial gain.
- Testing for unexpected interactions between application features.
- Case Study: A Race Condition exploit during a checkout process that allowed a user to purchase a limited-edition item multiple times with a single authorized payment.

Module 13: Report Writing and Professional Disclosure

- Structure of a high-quality, reproducible vulnerability report.
- Creating compelling Proof-of-Concept steps and videos.
- Calculating the correct CVSS and estimating impact.
- Professional communication with program teams and triage analysts.
- Case Study: Comparison of two identical bug reports, demonstrating how a superior report structure and impact analysis secured a 3x higher bounty payout.

Module 14: Mobile Application Bug Hunting

- Setting up an Android/iOS testing environment.
- Proxying and analyzing traffic from mobile applications.
- Static and dynamic analysis for hardcoded secrets and logic flaws.
- Exploiting insecure data storage and deep linking vulnerabilities.
- Case Study: An Insecure Data Storage vulnerability in a mobile application that allowed a local attacker to extract session tokens for all users.

Module 15: Cloud and Infrastructure Flaws

- Basic understanding of common Cloud misconfigurations
- Hunting for exposed credentials in infrastructure-as-code files.
- Exploiting misconfigured security headers and CORS.
- Fundamentals of XML External Entity attacks.
- Case Study: A misconfigured CORS policy that was exploited to steal user data from an authentication domain by a malicious site.

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