Security Testing with Burp Suite Professional Training Course

Professional Development Training Course Outline

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

Course Introduction

This intensive, hands-on masterclass delivers the advanced web application security testing skills required to become an elite Penetration Tester and Bug Bounty Hunter. We focus on mastering Burp Suite Professional, the industry-standard toolkit, to conduct thorough vulnerability assessment and exploitation. The modern web landscape demands security professionals who can go beyond automated scanning. This training is your gateway to achieving a DevSecOps mindset, employing sophisticated manual and automated techniques to find critical, non-obvious flaws like HTTP Request Smuggling, Insecure Deserialization, and advanced API vulnerabilities that automated scanners often miss. Security Testing with Burp Suite Professional Training Course emphasizes practical application and real-world attack scenarios to ensure graduates are immediately effective in securing modern, complex web applications.

Our course is built on a "learn-by-doing" philosophy, utilizing interactive labs and Capture the Flag challenges to solidify your skills. By the end of this course, you will not only be proficient in all core and advanced Burp Suite tools but also be able to custom-tailor attacks using Burp Extensions and seamlessly integrate security testing into the CI/CD pipeline. This course prepares you to tackle the most complex security challenges, elevate your Application Security career, and maximize your earnings in the competitive Bug Bounty space.

Programme Curriculum

Security Testing with Burp Suite Professional Training Course

Introduction

This intensive, hands-on masterclass delivers the advanced web application security testing skills required to become an elite Penetration Tester and Bug Bounty Hunter. We focus on mastering Burp Suite Professional, the industry-standard toolkit, to conduct thorough vulnerability assessment and exploitation. The modern web

landscape demands security professionals who can go beyond automated scanning. This training is your gateway to achieving a DevSecOps mindset, employing sophisticated manual and automated techniques to find critical, non-obvious flaws like HTTP Request Smuggling, Insecure Deserialization, and advanced API vulnerabilities that automated scanners often miss. Security Testing with Burp Suite Professional Training Course emphasizes practical application and real-world attack scenarios to ensure graduates are immediately effective in securing modern, complex web applications.

Our course is built on a "learn-by-doing" philosophy, utilizing interactive labs and Capture the Flag challenges to solidify your skills. By the end of this course, you will not only be proficient in all core and advanced Burp Suite tools but also be able to custom-tailor attacks using Burp Extensions and seamlessly integrate security testing into the CI/CD pipeline. This course prepares you to tackle the most complex security challenges, elevate your Application Security career, and maximize your earnings in the competitive Bug Bounty space.

Course Duration

5 days

Course Objectives

1. Web Application Penetration Testing
2. Master Burp Suite Professional
3. Advanced Vulnerability Exploitation
4. Hands-on Bug Bounty Hunting
5. API Security Testing (REST/GraphQL)
6. CI/CD Security Integration
7. Server-Side Request Forgery (SSRF)
8. Insecure Deserialization Attack Vectors
9. HTTP Request Smuggling & Web Cache Poisoning
10. Custom Burp Extension Development
11. Session Management and Authentication Bypass
12. DOM-based and Advanced XSS Exploitation
13. DevSecOps Toolchain Proficiency

Target Audience

1. Penetration Testers.
2. Security Analysts.
3. Ethical Hackers and dedicated Bug Bounty Hunters.
4. Application Security Engineers.
5. Software Developers.
6. Red Team Operators.
7. Security Consultants.
8. Security Architects.

Course Modules

Module 1: Burp Suite Foundation and Advanced Proxying

- Project options, target scope, and invisible proxying.
- Advanced traffic interception and modification with the Burp Proxy.
- SSL/TLS configuration, client-side certificate handling, and session handling rules.

- Utilizing Logger++ for efficient request review and filtering.
- Case Study: Analyzing a blind, stored Cross-Site Scripting (XSS) vulnerability on a high-profile e-commerce site using advanced proxy history filtering to trace the data flow from client-side input to server-side storage.

Module 2: Automated & Manual Discovery with Target and Scanner

- Mastering the Burp Scanner.
- Deep content discovery using the Target Site Map, custom directory wordlists, and the Content Discovery tool.
- Effective result interpretation, false positive reduction, and vulnerability prioritization.
- Leveraging Burp Infiltrator for enhanced code-level visibility during dynamic testing.
- Case Study: Using Burp's passive scan to identify exposed Git or sensitive configuration files on a live, publicly accessible website, leading to an Information Disclosure and a bypass of the application?ÇÖs intended access control.

Module 3: Fuzzing and Brute-Forcing with Intruder

- Mastering Intruder attack types.
- Optimizing Intruder payloads, position markers, and custom extractors for complex attacks.
- Brute-forcing authentication mechanisms and performing complex Parameter Tampering.
- Using Intruder for dictionary attacks and fuzzing for Blind SSRF and injection flaws.
- Case Study: Demonstrating a Broken Access Control exploit by setting up a Cluster Bomb attack in Intruder to rapidly iterate through sequential user IDs, enabling the theft of private user data across thousands of accounts.

Module 4: Manipulating Requests with Repeater and Comparer

- High-efficiency request manipulation, chaining attacks, and macro recording with Repeater.
- Manual confirmation and exploitation of automated Scanner findings.
- Using Repeater to craft malicious payloads for non-standard ports and protocols.
- Leveraging Comparer for effective diffing of responses to identify subtle vulnerabilities
- Case Study: Exploiting an HTTP Request Smuggling vulnerability by meticulously crafting two separate requests in Repeater and observing the server's response differential to confirm the smuggled request was processed.

Module 5: Advanced Web Application Attacks

- In-depth testing for Insecure Deserialization using the Java Deserialization Scanner extension.
- Exploiting Web Cache Poisoning and HTTP Host Header attacks using the Burp Scanner and manual techniques.
- Testing and exploiting various forms of Server-Side Template Injection
- Leveraging the Burp Collaborator for out-of-band application security testing and Blind XXE/SSRF exploitation.
- Case Study: Using the Collaborator to confirm a blind SSRF vulnerability that resulted in internal network port scanning and access to an AWS metadata endpoint, proving a critical server-side vulnerability.

Module 6: API and Mobile Application Security Testing

- Testing REST and GraphQL APIs.
- Utilizing Burp for testing mobile application traffic via proxy configuration and SSL Pinning bypass.

- Exploiting API-specific vulnerabilities
- Parsing and testing non-standard data formats in Repeater and Intruder.
- Case Study: A BOLA (Broken Object Level Authorization) case where a malicious user modified an API request parameter in Repeater to retrieve another user's financial transaction data, demonstrating a critical authorization bypass.

Module 7: Extensibility, Automation, and CI/CD Integration

- Developing custom Burp extensions using Python/Jython.
- Utilizing useful community extensions like ActiveScan++, Autorize, and Param Miner.
- Automating recurring tasks using Burp Macros and Session Handling Rules.
- Introduction to integrating Burp Scanner and reporting into a DevSecOps/CI/CD pipeline using the command line interface.
- Case Study: Developing a custom extension in Python to automate the detection of a proprietary, custom-encoded parameter often used by the target application, significantly reducing manual testing time.

Module 8: Reporting and Professional Ethics

- Generating professional, high-impact security reports from Burp's data.
- Categorizing and rating vulnerabilities based on industry standards
- Effective remediation guidance and communicating risks to developers and management.
- Adherence to legal and ethical guidelines during penetration testing.
- Case Study: Reviewing a full end-to-end report on a chain of vulnerabilities, focusing on clear exploit narration, risk scoring, and practical mitigation steps for the development team.

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.com 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
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

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

Register Online Now

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