Bug Beginners Course

Bug Bounty for Beginners: A Quick Information Guide

Topics Covered:

1. What is Bug Bounty?
2. Getting Started for Bug Hunt
3. Types of Responsible Disclosure
4. Burp Suite Introduction
5. Topics Covered:

6. Recon: Active/Passive
7. How to Choose a Target
8. Scope Analysis
9. System Configuration
10. Topics Covered:

11. Vulnerabilities
12. Cross-Site Request Forgery (CSRF)
13. Cross-Site Scripting (XSS): Reflected/Stored
14. Session Vulnerabilities (5 Counts)
15. Rate Limit Attack (5 Counts)
16. Topics Covered:

17. Vulnerabilities
18. Information Disclosure Bugs
19. Payment Gateway Bypasses
20. URL Redirection Issue
21. Insecure Protocol Attack
22. Topics Covered:

23. Unauthorized Access (3 Counts)
24. SQL Injection (GET/POST)
25. Server-Side Request Forgery (SSRF)
26. Password Reset Vulnerabilities
27. Denial-of-Service (DoS) Attack Methods
28. Topics Covered:

29. Account Takeover Vulnerabilities
30. Exif Metadata Issues
31. Weak/Lack of Authentication
32. Broken Link Hijacking
33. Sensitive Data Gathering
34. Topics Covered:

35. Weak Password Policy
36. Directory Listing
37. API-based Vulnerabilities
38. 5 More Surprise Bugs

Join our Bug Bounty for Beginners course and gain valuable insights into the world of bug hunting. Learn about various vulnerability types, responsible disclosure practices, and tools like Burp Suite. Dive into recon techniques, vulnerability analysis, and exploitation methods. Enhance your skills in identifying and reporting security issues. Enroll now and kickstart your bug bounty journey with confidence!

Please note that the content provided is a brief overview, and the course will provide comprehensive coverage of each topic.