BUG BOUNTY ADVANCED COURSE

By Aditya Shende

WE HUNT • WE EARN

Powered by KONGSEC

Course Details

Duration: 1 Month (Weekend Batch)
Price: ₹9,999 INR *(Installments Available)*
Payment Options: UPI • Bank Transfer • UK Transfer • Wise

About the Course

The **Bug Bounty Advanced Course** is a premium-level, real-world focused training designed for learners who already understand the basics of bug hunting and now want to step into **high-severity, real-money vulnerabilities**.

This course is crafted around **actual bug bounty methodologies**, deep exploitation techniques, business logic abuse, automation workflows, and professional report writing — exactly how elite hunters operate.

Core Course Content

Module 1 – Targeting & Code Intelligence

1. Target Approaching Strategies

2. Advanced Code Analysis
3. Information Disclosure & PII Exposure
4. Professional Dork Creation Techniques
5. Server-Side Request Forgery (SSRF)
6. Broken Access Control
7. Professional Report Writing
8. MFA Bypass Techniques
9. P1 Severity Surprise Bugs
10. API Key Exploitation

Deep-Dive Curriculum

Phase 1 – Recon & Data Discovery

1.1 Target Approach
1.2 Code Analysis
1.3 Information Disclosure
1.4 Sensitive Data Discovery Techniques

Phase 2 – High-Impact Exploitation

2.1 Unauthenticated Remote Code Execution (RCE)
2.2 Database Exploitation
2.3 Hardcoded Credentials Discovery
2.4 Advanced Data Enumeration

Phase 3 – Authentication & Token Attacks

3.1 MFA Bypass
3.2 Token Validation Bypass
3.3 Request Analysis
3.4 Response Analysis
3.5 Desktop & Session Manipulation Techniques

Phase 4 – Business Logic Exploitation

4.1 Business Logic Abuse
4.2 Organization-Level Impact Assessment
4.3 Functional Exploits
4.4 Blind Attacks
4.5 Mitigation Strategy Design

Phase 5 – Memory & Injection Attacks

5.1 Function Glimpse
5.2 Web Application Memory Attacks
5.3 Blind Comment Injection

Phase 6 – SSRF Mastery

6.1 SSRF Attacks
6.2 Beginner to Expert-Level Exploitation
6.3 Blacklist & Whitelist Bypass
6.4 Localhost & Internal Network Attacks

Phase 7 – Platform Misconfigurations

7.3 Platform-Level Misconfigurations
7.4 Localhost Attacking Techniques

Phase 8 – Google Recon & Reporting

8.1 Google Dorking Methodology
8.2 Subdomain Enumeration
8.3 Reconnaissance Automation
8.4 Effective Report Writing

Phase 9 – Automation & Workflow Optimization

9.1 Automation Frameworks
9.2 Tool Installation & Configuration
9.3 Key Bindings & Productivity Hacks
9.4 Simplified Automation Pipelines

Phase 10 – Surprise P1 Hunting

10.1 Exclusive Surprise Vulnerabilities
10.2 Discover 5 Live P1 Bugs
10.3 Comprehensive Professional Reporting

Why Choose This Course?

✔ High-severity vulnerability hunting
✔ Real bug bounty workflows
✔ Automation-based recon & exploitation
✔ Business logic abuse training
✔ Professional report writing mastery
✔ Designed for serious bug bounty earners

Outcome After Completion

You will be able to:

- Hunt P1 & critical vulnerabilities
- Bypass MFA and authentication controls
- Exploit logic flaws & internal services
- Automate recon and exploitation pipelines
- Submit professional reports to top companies
- Earn real bug bounty rewards

Enroll Now

Join the **Bug Bounty Advanced Course** and unlock elite-level vulnerability hunting skills under expert guidance.

Become a professional bug bounty hunter with KONGSEC.