SYLLABUS

CYBER SECURITY · COURSE HANDOUT 2026

BUG BOUNTY HUNTING

CON . AUTOMATION . DISCOV
WEB . API . LOGIC FLAWS . B
EPORTS . TRIAGE . PAYOUTS

DURATION	LEVEL	MODULES	MODE
45 Hours	**Intermediate to Advanced**	**8**	**Classroom · Online · Hybrid**

01 COURSE OVERVIEW

A bug bounty course on finding, proving and reporting real vulnerabilities within programme rules. The course covers reconnaissance at scale, vulnerability classes that pay, duplicate avoidance, proof-of-concept quality and report writing, along with the etiquette and legal boundaries of public programmes.

Learners work on authorised public programmes and submit at least one complete report during the course.

WHO IT IS FOR

- Security enthusiasts and students
- Web developers with security interest
- Penetration testers building a portfolio
- Freelance researchers

PREREQUISITES

Web application security fundamentals and comfort with the Linux command line.

02 LEARNING OUTCOMES

01 Read programme scope and stay within it.

02 Automate subdomain and asset discovery.

03 Prioritise targets by likely reward.

04 Find injection, access control and logic flaws.

05 Chain low-severity issues into higher impact.

06 Write reproducible proof-of-concept reports.

07 Handle triage responses and duplicates professionally.

03 MODULE STRUCTURE

8 MODULES

01 PROGRAMMES AND RULES

- Platforms
- Safe harbour
- Reputation systems
- Scope and out-of-scope
- Disclosure policies

02 RECONNAISSANCE

- Subdomain enumeration
- Content discovery
- Historical data
- Asset discovery
- JS analysis

TOOLS

SUBFINDER · HTTPX · FFUF · GAU

03 AUTOMATION

- Recon pipelines
- Rate limiting and courtesy
- Notification workflows
- False positive filtering

LAB

PERSONAL RECON PIPELINE

04 HIGH-VALUE WEB BUGS

- Access control flaws
- XSS chains
- File upload
- SSRF
- Injection
- Cache deception

LAB

LIVE TARGET HUNTING

05 API AND MOBILE SURFACES

- Undocumented endpoints
- Token scope abuse
- GraphQL introspection
- Mobile app endpoints

06 BUSINESS LOGIC

- Payment flows
- Race conditions
- Account takeover chains
- Coupon and quota abuse
- Workflow bypass

07 PROOF OF CONCEPT

- Minimal reproduction
- Screenshots and video
- Severity rating
- Impact demonstration
- Redaction

08 REPORTING AND FOLLOW-UP

- Report structure
- Duplicates and disputes
- Building a track record
- Triage communication
- Retesting

PROJECT

ONE COMPLETE SUBMITTED REPORT

04 ASSESSMENT & CERTIFICATION

Module assignments and labs	**25%**
Mini projects	**20%**
Internal assessments	**15%**
Final project and review	**40%**

CERTIFICATION

Learners who complete all modules, submit the final project and clear the review receive a course completion certificate from Kaizen Infinities Private Limited. Project work is documented for the learner's portfolio, and interview preparation is included in the closing sessions.

05 CAREER OUTCOMES

ROLES THIS PROGRAMME PREPARES FOR

BUG BOUNTY HUNTER **FREELANCE SECURITY RESEARCHER** **APPLICATION SECURITY ANALYST** **PENETRATION TESTER** **SECURITY CONSULTANT**

CALL US
+91 73051 33996

EMAIL US
apply@kaizeninfinities.com

VISIT OUR WEBSITE
www.kaizeninfinities.com