Bug Bounty Expert (BBE)

Bug Bounty Expert is a tailored course that helps you recognize the security bugs or vulnerability in the web application. A bug-bounty program is a contract offered by various websites, such as **Twitter, Yahoo, Uber, Coinbase**, who are inviting researchers to assist and mitigate zero-day attacks or other possible security flaws, along with rewarding $100, $1,000, and even $10,000 per bug.

This kind of bounty program addresses questions **like How do you turn into a good bug hunter?** This will help to make you go from zero to thousands of dollars on Hacker One or other bug hunting sites. This course will assist you in learning how to find bugs step by step (LIVE) in the process.

❖ Prerequisites

- Basic Cybersecurity Fundamentals
- knowledge of computer networks, firewall, security architecture
- Basic knowledge of web technology

NOTE:

Basic videos will be provided before sessions for better understanding of prerequisites.

❖ Who can Attend?

- Information Security Professional
- Forensics Investigators
- Incident Responders
- Software Developers
- Programmers
- Students
- Who wish to be a Professional Bug Hunter

❖ System Requirement

- CPU: 64-bit Intel i5/i7 with 4th generation + (2.0 GHz)
- 8 GB of RAM or higher
- 300 GB free space
- Administrator Access
- Wi-Fi 802.11 capability
- Windows 10 Pro, Linux or macOS (Latest updated)

NOTE:

All other software and configuration requirement will be provided and guided.

❖ Duration

- 40 hours

❖ Pricing

- 47,200 INR | 630 USD

❖ BBE Syllabus

Module 1- Brief Introduction to BBE

Module 2- Offensive Approach to Hunt Bugs

Module 3- Penetration Testing Methodologies

Module 4- SAST & DAST

Module 5- Black Hat Tools Overview

Module 6- Bug Hunting Penetration Testing Lab Setup

Module 7- Hacker Associate Customize Virtual Machine for Bug Hunting

Module 8- OWASP Top-10

Module 9- XSS Bug Hunting on any Application

Module 10- SQL Injection on any Application

Module 11- Payload Creation and Technique (Design your own Payload for attack)

Module 12- Industry best practices to hunt any Web Application

Module 13- Header Injection Attack

Module 14- CORS Exploitation

Module 15- URL Redirection Attack

Module 16- XXE Injection Attacking Technique

Module 17- LFI & RFI Vulnerability Identification and Exploitation

Module 18- File Upload Vulnerability Identification and Exploitation

Module 19- Command Injection Vulnerability Identification and Exploitation

Module 20- Subdomain Takeover Vulnerability Identification and Exploitation

Module 21- Broken Authentication and Access Control

Module 22- Insecure Deserialization Vulnerability Identification and Exploitation

Module 23- HTML Injection Vulnerability Identification and Exploitation

Module 24- Session Handling and Management

Module 25- WAF (Web Application Firewall) bypassing

Module 26- Captcha Bypassing

Module 27- Payment Gateway Analysis

Module 28- Parameter Tempering

Module 29- Create backdoor and hunt any Web Application

Module 30- RCE Vulnerability Identification and Exploitation

Visit www.hackerassociate.com for more details.