

Bug Bounty

Duration: 2 Days

Description

Did you know that big companies like Facebook, Google, Microsoft have paid millions of dollars' worth of prize so far to bug bounty hunters who discover security vulnerabilities in their systems? As one of the most popular jobs of the new age, bug bounty hunting allows you to do your profession as the boss of your own business at anytime and anywhere you want. In this course, mainly you will learn how to identify critical security vulnerabilities that are commonly found in the web and mobile applications.

Target Audience

- Penetration testers
- Bounty hunters at beginner level
- Cyber security professionals

Outline

What is Bug Bounty? Bug Bounty concepts Bug Bounty rules Key to Success Finding the right system Easy targets Collecting information over the Internet Common vulnerabilities in the systems Application analysis and methodology Advanced Burp Suite usage Essential security elements Authentication and session management Authorization Brute force attacks Content injection (content spoofing) Cross site request forgery Cross site scripting Encryption - SSL / TLS weaknesses Business and logic errors Information disclosures Running command Incorrect server and application configurations SQL injection Denial of service Bypass security checks Reporting and Monitoring Continuity and Up-to-dateness

Prerequisites

Essential knowledge of TCP/IP, networking and penetration test