ONE PAGE SUMMARY

IT & Software › Ethical Hacking › Bug Bounty Basics

Introduction to Bug Bounty Basics

Unlocking Security: The Basics of Bug Bounty Programs

DEFINITION

> Bug bounty programs reward individuals for finding and reporting software vulnerabilities. They help improve security by leveraging the skills of ethical hackers.

KEY CONCEPTS

Bug Bounty Program

A program offered by organizations to incentivize ethical hackers to find security flaws.

Vulnerability Disclosure

The process of reporting identified security weaknesses to the organization responsible for the software.

Ethical Hacking

Legally probing systems to discover vulnerabilities, with permission from the owner.

Rewards and Incentives

Financial or non-financial compensation given to hackers for successfully reporting bugs.

Responsible Disclosure

The practice of reporting vulnerabilities privately to the organization before making them public.

EXAMPLES

→ Finding a SQL injection flaw in a web application.

→ Identifying a cross-site scripting (XSS) vulnerability in a mobile app.

→ Reporting a security misconfiguration in a cloud service.

MEMORY TIPS

★ Remember 'Bugs = Bounty' to connect vulnerabilities with rewards.

★ Use the acronym 'V.E.R.' for Vulnerability, Ethical hacking, and Reporting.

★ Visualize a treasure map where bugs are marked as 'X' for rewards.

COMMON MISTAKES

✗ Not reading the program's rules and scope before testing.

✗ Failing to report vulnerabilities responsibly and publicly disclosing them.

✗ Assuming all bugs will be rewarded without understanding the criteria.

QUICK RECAP

Bug bounty programs are essential for enhancing software security through ethical hacking. Participants find and report vulnerabilities for rewards, following responsible disclosure practices.