Bug Hunt 101 — Recon to Report

Student Name: BHAVNATH KUMAR **College:** CGC University, Mohali **Country:** India

Abstract

This project provides a hands-on introduction to the bug bounty and ethical hacking process by simulating a real-world security assessment in a controlled laboratory environment. The goal of the project is to understand how vulnerabilities are discovered, validated, and reported responsibly while maintaining ethical standards and respecting defined scope.

Objectives

The main objectives of this project include understanding reconnaissance techniques, identifying common web application vulnerabilities, gaining practical experience with industry-standard security tools, and developing the ability to write clear and professional vulnerability reports suitable for real bug bounty platforms.

Environment, Scope and Tools

The testing environment consisted of a deliberately vulnerable web application such as Damn Vulnerable Web Application (DVWA) or OWASP Juice Shop hosted locally. All testing was conducted strictly within the defined lab scope. Tools used during the assessment included Nmap for network and service discovery, Amass/Sublist3r for reconnaissance, Burp Suite for intercepting and analyzing HTTP requests, and SQLMap for automated SQL injection testing.

Methodology

The project followed a structured methodology starting with reconnaissance to identify open ports, services, and potential input vectors. This was followed by manual and tool-assisted testing to detect vulnerabilities such as Cross-Site Scripting (XSS), SQL Injection (SQLi), and Insecure Direct Object References (IDOR). Each identified vulnerability was validated, documented, and analyzed to understand its security impact.

Findings, Impact and Learning Outcomes

The assessment revealed multiple security weaknesses related to insufficient input validation and improper access control mechanisms. In real-world applications, such issues could lead to data leakage, account compromise, or unauthorized system access. Through this project, valuable learning outcomes were achieved, including improved understanding of web security concepts, hands-on tool usage, and professional security documentation skills.

Conclusion

This project successfully demonstrates the complete bug bounty workflow from reconnaissance to professional vulnerability reporting. It emphasizes the importance of ethical hacking, responsible disclosure, and continuous security testing as essential components of modern software development and cyber security practices.