**PROJECT SUMMARY**

**PROJECT TITLE:**

Bug Bounty

**GROUP MEMBERS:**

* BSEF19M009 AQSA YAQOOB
* BSEF19M012 FAIZA SHAHBAZ
* BSEF19M015 FAREEHA RANI

**PROJECT SUPERVISOR:**

Mr Farooq Javed

**TABLE OF CONTENTS**

1. Introduction..………………………………………………………….3

2.Description…...………………………………………………………..3

3.Objectives...……………………………………………………………3

4.Phases..…………………………………………………………………4

**INTRODUCTION**

A multi phased testing process will be implemented, the test is designed to find vulnerabilities in the system. while performing the tests, tester will act as a hacker to locate vulnerabilities more thoroughly.

Basically it will be a method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might.

**BUG BOUNTY**

A bug bounty program is a deal offered by many websites, organizations and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities.

**PENETRATION TESTING:**

A penetration test, colloquially known as a pen test or ethical hacking, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system. The test is performed to identify weaknesses also referred to as vulnerabilities, including the potential for unauthorized parties to gain access to the system's features and data, as well as strengths, enabling a full risk assessment to be completed.

**OBJECTIVES**

1) To identify and eliminate security vulnerabilities of your organisation/system/website/network

2) Evaluate the effectiveness of the security strategy to see if its specified measures create an effective defence when followed.

3) Evaluate your complete attack surface and find any vulnerabilities in equipment that face the outside.

4) Determine if your external controls adequately mitigate risk and keep out bad actors.

**TYPE OF TEST**:

external Network testing

web Application testing

**TECHNOLOGY TO BE USED**

Kali Linux Toolkit

Burp Suite

**PHASES INVOLVED**

**INFORMATION GATHERING**

The organization being tested will provide the penetration tester with general information about in-scope targets.

**PRE EXPLOITATION**

**a. Reconnaissance**

Before launching an attack, the attacker collects all the necessary information about the target. The data is likely to contain passwords, essential details of employees, etc. It helps identify which attacks can be launched and how likely the organization’s systems fall vulnerable to those attacks.

**b. Discovery and Scanning**

Port scanning

The information gathered is used to perform discovery activities to determine things like ports and services that were available for targeted hosts, or subdomains, available for web applications.

**C. Vulnerability Assessment**

Vulnerability scanning. vulnerability assessment is conducted in order to gain initial knowledge and identify any potential security weaknesses that could allow an outside attacker to gain access to the environment or technology being tested

**EXPLOITATION**

After interpreting the results from the vulnerability assessment, penetration testers will use manual techniques, human intuition, and their backgrounds to validate, attack, and exploit those vulnerabilities.

**POST EXPLOITATION**

**a. Final Analysis and Review**

This comprehensive report includes narratives of where we started the testing, how we found vulnerabilities, and how we exploited them. It also includes the scope of the security testing, testing methodologies, findings, and recommendations for corrections.

**b. Utilization of the Testing Results**

The organization being tested must actually use the findings from the security testing to risk rank vulnerabilities, analyze the potential impact of vulnerabilities found, determine remediation strategies, and inform decision-making moving forward