**Bug Bounty Project \***

**Web Application Penetration Testing**

Fareeha Rani BSEF19M015

Aqsa Yaqoob BSEF19M009

Faiza Shahbaz BSEF19M015

**ABSTRACT**

Bug bounty is a set of activities, performing penetration tests on a system. Penetration Testing is an authorized simulated cyber-attack where ethical hackers implement attacks on an organization’s system to evaluate and assess the security of that system. This proposal provides brief overview about penetration testing. Important points under discussion will be objectives, benefits provided, background, and the methodology used. Steps involved in project methodology: Gathering the information, Pre-exploitation, Post exploitation and Report creation. It further discusses how to apply methodology provided to conduct penetration testing (Thomas Walshe).

1. **INTRODUCTION**

The increasing complexities and sizes of the systems have led to increase in security threats to software systems. Government agencies and business organizations today understand the constant need of ethical hacking to combat the growing threats to IT security.The more the sophisticated today’s technology has become and the ways ingenious hackers are discovering to create mischief in shared computing environments, especially the Internet. Furthermore, it is most prime responsibility for a business to protect its data from being stolen and the solution that the security experts and professional found was penetration testing and bug bounty hunting.

Penetration testing, or known as pen testing, is a simulation of cyber-attack against a particular functional, unified target system. It involves a number of activities to test various components of a system to check for vulnerabilities, bugs or misconfiguration of security (Aileen G. Bacudio).

* 1. **PURPOSE OF DOCUMENT**

The purpose of this document is to provide the purpose of the project, define its scope, overall description of the projects and the problems and the opportunities associated with the project and their solutions and finally the requirement and the resources required for the bug bounty project.

* 1. **PURPOSE**

To provide better security and to ensure the safety of the host systems from information being stolen Pen testing and bug bounty hunting is a methodology adopted which allows security tester finding vulnerabilities in a host system or web application from an attackers point of view and further exploiting the vulnerabilities providing the client, the organization or a person hiring pen testers to test their website, a glimpse of how many issues will be present in a full-fledged working Web App.

* 1. **SCOPE**

Web application penetration testing will be performed All the domain associated with the website will be tested. It will not be performed on the servers or the internal network of the organization. it will not be performed on internal network of the organization. Vulnerabilities associated with the website will be assessed and exploited.

1. **OVERALL PRODUCT DESCRIPTION**
   1. **STRATEGIES**

Pen testing used by us in this bug bounty projects are:

* Blackbox pen-tests:

Black box pen tests involve series of tests performed on a particular target and pen testers having no prior knowledge of it. Black box pen test has a resemblance to blind tests.

* External testing:

External testing is a series of cyber-attacks performed by the pen testers from an outside source and test how far they gain control of the target or the host system

* 1. **PHASES**
* Information gathering
* Pre-exploitation activities

1. Reconnaissance
2. Discovery And Scanning
3. Vulnerability Assessment

* Exploitation

1. Final Analysis and Review
2. Testing Results Utilization

* Post exploitation activities
  1. **TOOLS AND TECHNOLOGIES**

Some systems include tools for a range of security testing. One example among many is the Kali Linux (Bhalla, 2021), used in digital forensics and penetration testing. It contains eight standard security tools for penetration testing tools. The available options for penetration testing are highly specialized and numerous. Many systems include tools for a range of security testing of the operating system.

1. **THE PROBLEM OR OPPORTUNITY**

Uncover hidden vulnerabilities before attackers do. Many external breaches can be prevented by performing a penetration test. Pen testing will show exactly where an organization’s vulnerabilities are or where security defects can be compromised and will address those weaknesses – proactively – before attackers find them. Taking a 360-degree view of potential risk factors. Evaluating Monitoring and Response Effectiveness. Making the pen test reporting an invaluable tool to help the target organization improve their incident response skills and reinforce security practices with the entire company

1. **SOLUTION**

We can’t fix it if we don’t know where it’s broken! Pen testing team will go beyond finding security gaps and actively and try to exploit those vulnerabilities to see if a hacker could actually access data. It’s like an MRI for Target organization's infrastructure in that it looks for problems that may not have developed symptoms yet. It will be a true test of the effectiveness of existing protections and it will clearly reveal where organization is leaving doors open for cybercriminals to enter.A pre-testing consultation will be held to discuss the process and needed preparations. The Statement of Work (SOW) will be defined and timelines for completion will be established. The penetration test will be performed, penetration testing will then lead to making and presenting Network Penetration Test Assessment Report (Baloch).

1. **RESOURCES AND RISKS**

* **REQUIREMENT OF THE PROJECT**

This will include learning about common security mechanisms, security practices, their bypasses, common vulnerabilities in web applications, ways to find these vulnerabilities, and ways to patch and prevent the applications from these vulnerabilities. Pen testing team should be proficient at least with the fundamentals of inter-networking, IP addresses, MAC addresses, OSI stack (and TCP/IP stack), etc. Pen testing is a time-sensitive process and can take longer than expected if issues arise. It’s best to run this test during a time of low business activity. Depending on the organization's infrastructure

* **POTENTIAL DELAYS AND HURDLES**

One of the common hurdles proves to be scope related. "In scope" and "out of scope" bugs are common feature of disclosure processes. for example, Organization may want to know about Remote Code Execution (RCE) vulnerabilities but will not consider issues that might be less severe despite their exploitability or real-world impact such as server-side Request Forgery CSRF, unsecured servers or IDOR vulnerabilities.The tools and technology used sometimes unusually produces false positive and often false negative results for example, while using kali Linux running certain commands on the pre-built tools generated no response when there was no error on testing team side proving an error to be on serve side that is an off the shelf potential delay of penetration testing

1. **REFERENCES**

# Aileen G. Bacudio, Xiaohong Yuan, Bei-Tseng Bill Chu, Monique Jones. "An Overview of Penetration Testing." *International Journal of Network Security & Its Applications (IJNSA)* (November 2011): 19-20. Document.

Thomas Walshe, Andrew Simpson. "An Empirical Study of Bug Bounty Programs." *Walshe and Simpson An Empirical Study of Bug Bounty Programs* (2020): 1-4. Document.