Tutorial No. 4

Title: Bug Bounty Report

Roll No.: 16010420075 **Tutorial No.: 4**

Aim: To prepare a report on Bug Bounty program.

\

Resources: Internet (working)

IMPLEMENTATION AND RESULTS:

About Bug Bounty Program

Many websites, organizations, and software companies provide bug bounty programs in which individuals can be recognized and compensated for reporting bugs, particularly those related to security exploits and vulnerabilities.

These systems help developers to find and fix flaws before they are discovered by the broader public, preventing widespread exploitation. Mozilla, Facebook, Yahoo!, Google, Reddit, Square, Microsoft, and the Internet bug bounty are just a few of the companies that have introduced bug bounty programs.

Bug bounty programs are now being used by companies outside of the technology industry, including typically conservative entities like the US Department of Defense. Bug bounty programs are being used by the Pentagon as part of a shift in policy that has seen various US government agencies shift from threatening white hat hackers with legal action to inviting them to engage as part of a full vulnerability disclosure framework or policy.

Reporting bugs

You must file a report to publish your findings when you discover a bug or vulnerability.

In general, you must explain where the bug was discovered, who it affects, how to reproduce it, the parameters it affects, and offer Proof-of-Concept evidence. As supporting proof, you can upload any files or logs. This not only makes it easier to duplicate the problem, but it also speeds up the review process by eliminating delays caused by missing information.

At a minimum, the report must include the following information:

Section name	**Description**
Summary Title	This will be the title of your report. It must provide a brief overview of the type of bug found, where it was found, and the overall impact. For example, “Remote File Inclusion in Resume Upload Form allows remote

	code execution” is more descriptive and helpful than “RFI Injection found.”
Target	Identifies the specific target that is affected by the bug you have found.
Technical Severity	The Vulnerability Rating Taxonomy Classification identifies the kind of bug you have found based on our VRT, our baseline priority rating system for common bugs found on bug bounty programs. It is important that you choose the correct type so that the organization understands the risk from the bug. The severity rating suggested by VRT is not guaranteed to be the severity rating applied to your submission once impact is considered.
Vulnerability details	Include the following information: - **URL/Location of vulnerability**: Location in the application where you have discovered the bug. - **Description**: Provide detailed information about the vulnerability. Add clear and descriptive replication steps so that the organization can easily reproduce and validate your findings. Describe the risk and the impact. Provide illustrative evidence in the form of screenshots or videos that shows proof of the vulnerability. This is one of the most impactful things you can do to provide context around your submission. It is strongly recommended that you provide this every time you submit.
Attachments	Attach proof-of-concept scripts, screenshots, screen recordings, and so on.

How to Write a Good Bug Report

When drafting a bug report, it's critical to consider the audience that will be reading your report. For the exact vulnerability, Bugcrowd and Program Owner Analysts may not have the same level of understanding as you. As a result, when producing your report, make sure to include clear, concise, and descriptive information.

- **Gather and organize your data:** Explanations in plain language: In order to effectively replicate the vulnerability, order your report in the exact sequence of steps.

- **Explain clearly:** It is critical that you create your report with a specific aim in mind. To ensure that the submission is processed promptly and without the need for more information, let the reader understand the security implications, replication procedures, and actions that need to be taken to fix the issue.

- **Scenarios of assault that have been well documented:** The impact of the vulnerability is indicated by attack scenarios. "This vulnerability affects all users of your forum," for example. When a user signs up with XYZ@customer.com as their username and XYZ@customer.com as their password, their username is accepted. This vulnerability, together with a username enumeration flaw, can be used to brute-force forum usernames and passwords."

Vulnerability Disclosure Philosophy

Finder's rules:

- **Follow the rules.** Follow the guidelines given forth by the Security Team, or speak up if you are strongly opposed to the rules.

- **Privacy should be respected.** Make a good faith attempt to avoid accessing or destroying the data of another user.

- **Patience is required.** Upon asked, make a good faith effort to clarify and support their reports.

- **Don't cause any harm.** Act for the greater good by promptly reporting all discovered vulnerabilities. Never take advantage of others without their permission.

The security staff must follow the following rules:

- **Make security a top priority.** Make a good faith attempt to remedy security issues that have been disclosed in a timely and transparent way.

- **Finders are to be respected.** Give the finders public acclaim for their efforts.

- **Research should be rewarded.** When it's suitable, financially incentivize security research.

- **Don't cause any harm.** Not taking irrational retaliatory measures against finders, such as issuing legal threats or sending the situation to law enforcement.

Outcomes:

CO-1: Realize that premise of vulnerability analysis and penetration

testing (VAPT).

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

A report on Bug Bounty Program was prepared and assessed successfully.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

REFERENCES:

- www.wikipedia.com
- www.hackerone.com
- www.bugcrowd.com