Proceedings Series on Social Sciences & Humanities, Volume 21
Proceedings of the 4th 2024 UMP Progressive Youth Conference (UPYC)
Universitas Muhammadiyah Purwokerto
ISSN: 2808-103X

The Effectiveness of Bug Bounty Program for Technology Company Ecosystem

Miftahul Munir
Informatics Engineering, Faculty of Engineering and Science,
Universitas Muhammadiyah Purwokerto

ARTICLE INFO

Article history:

DOI:
10.30595/pssh.v21i.1517

Submitted:
Jan 25, 2025

Accepted:
Apr 16, 2025

Published:
Apr 25, 2025

Keywords:

Cyber Security; Bug Bounty; Technology Company Ecosystem; Benefits

ABSTRACT

Bug bounty is one of the programs in the field of Cyber Security with the purpose to finding and uncovering vulnerabilities in technology company ecosystem. Researcher focusing on the security field will play a critical role to the success of bug bounty program with their expertise in security system and deep understanding of the technology. The purpose of this study is to examine the effectiveness of bug bounty and its benefits in improving company security system. Qualitative methods were used for collecting and analyzing the data. The results show the importance of bug bounties as the right solution for developing and maintaining security company ecosystem. It is hoped that this paper can serve as a reference for companies to consider the adoption of this program. In the future, this research can develop further by involving effective communication between researchers and the companies to obtain more up-to-date data.

Corresponding Author:
Miftahul Munir
Informatics Engineering, Faculty of Engineering and Science
Universitas Muhammadiyah Purwokerto
Email: munirmiftahul07@gmail.com

1. INTRODUCTION

In the digital era that continues growing, security device software become one critical aspect in ensuring integrity, confidentiality, and availability system. Attacks to this device software can consequently affect loss significant financial, sensitive data leaks, and reputation damage of a organization. To overcome these challenges, companies and organizations must adopt various strategies for strengthening their security device software (Isma Elan Maulani, 2023). Safeguarding systems is imperative for companies to ensure the security of their data. Therefore, several measures can be taken, such as conducting penetration testing.

Penetration testing is a security exercise where a cyber-security expert attempts to find and exploit vulnerabilities in a computer system. The purpose of this activity is to identify any weak spots in a system's defences which attackers could take advantage of (Cloudflare, 2024). However, there is a weakness of using penetration testing that is limited testing timeframe. Then, one of the Cyber security programss that can be adopted is Bug Bounty which offers a program that can run at any time within an undetermined timeframe and encompasses a broader range of assets under examination.

The Bug Bounty Program is a reward-based program designed to test a system developed by a software developer with the aim of identifying security vulnerabilities. Referring to (Yaworski, 2019) , he stated that "A Bug Bounty is a reward a website or a company gives to anyone who ethically discover a vulnerability and report it to that website or company". Based on two statements above, it can be inferred that this program is an initiative program that offers reward, typically in the form of monetary sum, to ethical hackers who successfully identify vulnerabilities in a developed system.

By using this program's ability of figuring out all the vulnerability of the system, its corelates with the requirement of current company. In this current era, companies will continue to grow, and an increasing number of system will be developed to meet the specific needs of the company ecosystem. Consequently, the likelihood of errors in system arises, whether due to mistake in the development process or the lack of robust defence mechanisms system. On the other hand, leveraging the expertise of security-focused hackers can prove beneficial in analyzing the security robustness of a company's system.

Therefore, Bug Bounty can serve as an appropriate platform to facilitate the collaboration of proficient hacker with a company that require assistance in enhancing the security of their system. Based on the aforementioned above, this paper aims to examine the effectiveness of bug bounty program in improving company security system. This paper also discusses about the significant of this program to the company security system.

2. METHODOLOGY

This study used a qualitative method as the research instrument for collecting and analyzing data. By utilizing the qualitative method, the study gained a deep understanding of the various impacts of bug bounty programs on a technology company ecosystem. Several step were undertaken by the researcher in collecting data. The researcher read several, books, articles, and journals related to bug bounty programs to collect data related to the understanding of bug bounty, the objectives of bug bounty, and its significance to technology company ecosystem. The data were in the form of sentences reflecting the concept of bug bounty were taken using the note-taking method. Then, from all of data that collected, the researcher analyzed the benefits that company can gain through the implementation of bug bounty program.

3. RESULTS AND DISCUSSIONS

New Data-Driven businesses are increasingly, organization across industries are embracing technological advancements, but cybercriminals are getting more sophisticated. Cybercrime rates are growing, and with further growth of such crimes expected. Unlike traditional penetration services that generate a culture of fear and meeting compliance requirement, bug bounty are about creating a culture of opennes, transparency, and responsibility. (Broshevan, 2024)

The statements below show about why bug bounty can be a good platform for maintaining security system according into (WEERABANGSA, 2023).

a. Bug bounty programs assist in proactive security measures.

Penetration testing is often carried out by businesses that want to take a proactive approach to security. One excellent technique to discover what you are unwittingly disclosing to hackers is via a typical penetration exam. The result of penetration testing, however, are only as good as the hired team's security expertise. This indicates that there is a significant likelihood that crucial vulnerabilities may be missed throughout the procedure.

b. Collaboration with hackers.

Since businesses only get paid when vulnerabilites are reported and verified, using bug bounty program is a cost-effective strategy to increase cybersecurity. Bug bounty schemes draw hackers from various backgrounds and level of expertise, rather than depending just on one security expert, to enhance security. Having access to the world's hackers means that all the assets in the scope are adequately examined.

c. Teams for internal security improve their abilities and knowledge.

A skills gap in cybersecurity has been extensively publicized, but bug bounty schemes work in two ways of lessing its affect. The first is that businesses may quickly access a considerably greater variety of skill, information, and background by relying on a community of thousands of researchers. The second method is for development teams to gain cyber security expertise by studying the vulnerabilities that are disclosed via the program. Here are several advantages that companies can gain from this program according to (vaadata, 2021)

d. Enhancement security

Successful bug bounty hunting program possible company for identify and fix vulnerability the previous one no known, this in a manner significant increase level security device software of system used by the company

e. Efficiency Cost

Within period long, bug bounty program can become more efficient in a manner financial compared to with recruit team internal security or depend on service company security external, this program utilise expertise and skills from numnber of participating security researcher without must give wages full or contract period long.

f. Enhancement Reputation

A capable successful bug bounty program find and overcome vulnerability with fast and precise can increase repution company in matter safety and reliability. This can get up trust customers and users to product or service company.

Ideally Bug bounty program should be launched only after four fundamental components are in place. First, developers need secure coding training on identifying and fixing common vulnerabilities and ensure that code gets written in a way that minimizes vulnerabilities. Second, Establish a baseline of vulnerabilities. The developers should be an effort to both find and remove basic vulnerabilities before starting bug bounty. Third, Companies use automated scanning vulnerabilities on their software to find additional vulnerabilities. Fourth, developers need to take responsibility for security vulnerabilities in their code should be as invested in secure code as the security team or outside security researcher . (Journey, 2019)

From all data above we can conclude that using this program is an effective way to find vulnerabilities in a very large company environment. By embracing expert at different levels, this will enable vulnerabilities to be tested thoroughly in a system. Moreover, this program will also save company costs, because they only reward bug hunters who succeed in finding vulnerabilities, so the reporting results they receive will be more selected. This study shows that bug bounty programs are reliable initiatives in maintaining the ecosystem within technology companies. Through bug bounty programs, companies no longer need to worry about potential threats that could attack them at any time, as vulnerability in their system can be addressed promptly.

4. CONCLUSIONS

This journal is highly relevant for technology companies aiming to enhance or develop their operations. It provides detailed explanation of the theory behind bug bounty programs and their correlation with companies, offering significant benefit. However, on the flip side, this journal may be less suitable for individuals who seeking in-depth insight into the process of conducting bug bounty activities. Through this journal, it is hoped that bug bounty will gain greater recognition among companies and serve as an accurate reference.

REFERENCES

Broshevan, E. (2024). *Why every organization needs a bug bounty program*. Retrieved from TechBeacon: https://techbeacon.com/security/why-every-organization-needs-bug-bounty-program

Cloudflare. (2024). *What is penetration testing | what is pen testing*. Retrieved from cloudflare.com: https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/

Evgeniia Rudenko, A. G. (2021). Leveraging Ethical Hacking in Russia : Exploring the Design and Potential of Bug Bounty Programs. *Stanford University*, 15.

Hernawan, Y. K. (2019). *BUG HUNTING 101 (Web Application Security).* AL-FURSAN CYBERSECURITY LEARNING RESOURCES.

Isma Elan Maulani, R. A. (2023). BUG BOUNTY HUNTING, A CASE STUDY OF SUCCESSFUL VULNERABILITY DISCOVER AND DISCLOSURE . *Devotion-Journal of Research and Community Service*, 6.

Journey, S. (2019, December 26). *When Should I Launch a Bug Bounty Program?* Retrieved from securityjourney.com: https://www.securityjourney.com/post/when-should-i-launch-a-bug-bounty-program

Masarik, J. (2019). Automating Bug Bounty. 80.

Simpson, T. W. (2020). An Empirical Study of Bug Bounty Programs. *Oxford University Research Archive*, 10.

WEERABANGSA, N. (2023, March 4). *The Advantages Of starting A Successful Bug Bounty Program*. Retrieved from blog.bugzero.io: https://blog.bugzero.io/the-advantages-of-starting-a-successful-bug-bounty-program-aab3184cd3a6

Yaworski, P. (2019). *Real-World Bug Hunting A Field Guide to Web Hacking.* San Francisco: William Pollock.