Conceiving Effective Rules for Bug-Bounty Platforms and Security Vulnerability Detection

MARIAM FEYISAYO YUSSUF
Faculty of Engineering and Informatics, University of Bradford, United Kingdom.

Abstract- ***In a world of rising security risks, legislation and standards for protecting existing IT information and data preservation are major concerns and costs. Security and data vulnerability concern every company. Ethical and unethical hackers find and report vulnerabilities to bug bounty sites for modern security. Organizations rely on white hats, but they must constantly assess risks and rewards. Concerned institutions adopt special regulations to control white hat activity wherever they are, imposing responsibility on the participating organization like bounty levies. The quantitative study established bug bounty platform standards for system security vulnerability detection. The research explored and suggested basic security vulnerability detection criteria to detect typical system flaws. The study proposed relevant security vulnerability detection rules.***

Indexed Terms – White Hat; Ethical Hacker; Bug Bounty Platform.

I. INTRODUCTION

Though there has been significant improvement in the development of software and programs aimed at ensuring the security of computers and institution's hard investment in Information Technology, the role of hackers still affects the sustainability of core IT facilities which makes for large insecurity of systems used by organizations. The fact that there is increasing fortune and return on investment for those saddled with ensuring the safety of client information and other assets of the organization has opened the window for external threats which has given rise to vulnerability of data and security concerns.

The efforts and programs around bug bounty were initially limited to the security services offered organization by Netscape as far back as 1995, but recently many organizations both private such as Google, Apple and many others and even states like the United States of America have in place bug bounty programs to ensure system security and quick detection of security vulnerability.

The activities of hacks whether ethical or unethical calls for major concerns in the operations of information communication technology and ensuring the safety of business interest. The strategic security functions and roles of providing opposition to the efforts of malicious hackers on organization systems and database by white hats which finds and reports security exposure and vulnerability have been studied across IT institutions and organizations. A good number of factors have been adduced to be serving as motivation to enormous roles played by the ethical or white hat hackers which include, monetary consideration, the desire to build reputation and profile or opening for job placement, while for some others, it is the need to further their knowledge when they can detect the presence and operation of the bug in a system.

Through the comprehensive structure of remunerated or unremunerated schemes, the works of white hats or ethical hackers are provided to a targeted organization to help detect system or security vulnerabilities that might affect their operations [1, 2, and 3]. The works of these hackers are currently delivered to the organizations through the platforms provided by bug bounties such as Cobalt, Bug Crowd and Hacker One to mention a few. As a major part of the programs under Bug Bounties, big organizations or corporations give access to ethical hackers to their systems and security structures to point them to observed shortcomings which might not be detected by their organization’s security teams and which might cause unethical hackers to cause major security breach and expose their systems to external attacks by black hats. Platforms are used to facilitate the process for the operation of ethical hackers through the management

of their payments, meditating in times of disagreement between parties such as ethical hackers against holders of bug bounty programs or between law enforcement agents and in some rare cases serving as the most important point of call for the ethical hackers and the organization concerned.

This study which serves as further research to other studies is making a valuable contribution to the existing subject of security vulnerability through the conduct of studies on effective and workable strategies for undertaking the all-important task of bug bounty programs. These rules guiding the operations and services rendered are in themselves primary for the operations and intersections in the role and interest of ethical hackers and the recipient or benefiting organizations. The imperative of this action, therefore, is to bring to the fore two outstanding facts which are, they set in place for each program the expected outcome of an ethical hacker which helps to detect any exposure or security vulnerability in the organization's programmed site and when they go ahead to present the report of the vulnerability discovered to the organization and secondly, they make organizations agree to some standard rules of engagement and corresponding actions, such as the bounty reward for a given vulnerability or security breach found and the time required for solving the issues discovered.

Beyond the interaction between ethical hackers and the supporting programme, the agreed parameters of operation also inject competition among the platform's programmes. The agreed terms of operations often drive ethical hackers to do more research or force them to stop serving the organization's security interests, which can hurt the organization's security programme against system vulnerability because ethical hackers bring a different perspective to security breaches.

This paper proposes guidelines based on current literature to help bug bounty platforms find security vulnerabilities across systems and networks. Thus, the report outlines effective bug bounty guidelines and organization system security weaknesses.

Organizations need to develop policies that protect varied interests due to the ubiquity of security breaches and unethical hackers exposing systems to data dangers.

II. LITERATURE REVIEW

The field of research covering the place of bug bounty and security vulnerability detection in the world of information technology has been extensively discussed in previous studies. Therefore, furthering the existing research in the field, the important literature is discussed below.

Studies [4, 5, 6] have concentrated on how bug bounty programmes function within the broader security framework of both public and private IT infrastructure with a strong emphasis on data gathered on the programme's contents and the associated incentive structures for ethical hackers. Other works [7, 8] have taken into consideration the processes involved in making decisions that guide the detection of security vulnerabilities.

The exposure of software to attack and the vulnerability of systems and data has been a source of concern amongst organizations [9, 10, 11, 12] and most importantly, the growing challenges of market vulnerability [8, 9 &10]. Very recently research has concentrated significant efforts towards understanding the activities of bug bounty programs and how they impact the security concerns of organizations across IT platforms. In their studies, Finifter et al. [1] undertook an examination of bug bounty programs put in place by Google Chrome and Mozilla search engines and documented that, it is more economically friendly to initiate these programs than getting an in-house security expert that will be engaged in searching for security breaches and system vulnerabilities.

In a related development, Edmundson et al [13] revealed in a study involving several participants who were asked to identify the number of security vulnerabilities that are contained in a sample of programmed code but none of the participants identify the security risks because they were too complex, and the mode of adoption was beyond their comprehension. Within the same breath, when the number of participants was reduced by half, the chances that the bug embedded was located increased by half of the allotted percentage.

Furthermore, studies have emphasized finding the operational dynamics in bounty platforms [15, 16].

Specifically, With the main goal of having an in-depth understanding of their built-in features, how they function, their trajectory, and their overall impact on the current programmes, Zhao et al concentrated on a thorough investigation of two significant bounty platforms, known as Wooyun and Hacker One. A major revelation of the study was that the effectiveness or success that will be recorded by bounty platforms is dependent on the importance of the contributor to the program and that different ethical hackers given their speciality have the tendency to make important and different contributions to the development of the platform.

The work by Maillart et al [15], which addressed the reward systems and the enrolment pattern of hackers and their involvement in bounty programs that are public related on Hacker One and found that the increase in reward system does not match the level of challenges of discovering system vulnerability, this gives ethical hackers the thought of switching to a new avenue of searching for bugs conveniently. Also, the work of Zhao et al [16] focused on the role program plays in attracting the best ethical hackers through the process of making available rules of engagement that are found to be attractive. The study also revealed the many challenges that undermine the proposed growth and development of programs and platforms initiated for the bug bounty. It was further reported [16] that the bug bounty platform is faced with the challenges of reports submitted which in most cases does not meet the required benchmark. It was discovered that the reports submitted percentage error ranges between 35-55 from platforms that are of different categories and methods of application.

Also, Zhao et al [16] advanced that, the decentralized nature of discovering system risks and vulnerabilities might cause ethical hackers to find similar issues and file outcomes which they often relay as duplicated discoveries.

Detailing the rules of incentives in the operation of a bug bounty for security vulnerability detection, [13] believed policy procedure can also be built on the increase in incentives which is meant to serve as motivation for the efforts of ethical hackers. It noted exclusively that, giving rewards measuring the nature of security vulnerability discovered drives the efforts of ethical hacks in their future searches. Zhao et al [16] considered engagement policy as a major driver for the activities of ethical hackers in security vulnerability detection. The work identified three fundamental rules or policy which is based on incentives for white hat such as bug bounty policies, policy on general incentives and policy based on allocation.

III. METHODOLOGY

The analytical method adopted for this paper is based on the contextual analysis and review of empirical literature in this area of study. It raised existing rules that have guided the operation of bug bounty platforms and the detection of security vulnerabilities in organizations' networks. These rules are grouped based on their appearance. When allotted specific groupings they further revealed an order of priority and importance of rules in use. The top rules deployed for bug bounty platforms and vulnerability detections were identified and were used to produce a set of rules that can serve the recent needs of parties and these rules formed the bases for analyses.

IV. DISCUSSION OF RULES FOR BUG BOUNTY AND SECURITY VULNERABILITY DETECTION

Bug bounty platforms are major structures that help organizations detect security vulnerabilities. In delivering this very important task, they are guided by rules which should aid their operations in engaging systems and security networks erected by institutions both private and public against unethical hacks. The following are rules conceived for Bug bounty platforms:

i) Setting specific nets for Bug Bounty Operation. This is a situation where an organization set out specific rules detailing the areas that can be investigated and what actions permissions are granted on [17] to avoid aimless search which might cost extra financing and time.
ii) Rules on Incentives and Invalid Reports [17]. This allows for remuneration or reward systems based on the nature of security vulnerabilities detected.
iii) Rules of Allocation and Duplicate Reports [16].

iv) Rules that ensure the protection of legitimate security reports [16]. This rule ensures the protection of white hats in the event of discovering and reporting any security vulnerability detected in an organization. This is the condition of the provision of explicit legal regulatory policy on the activities of white hats.
v) Rules on the guidance of vulnerability disclosure [16]. This is based on the operation of two fundamental rules for disclosing detected security vulnerabilities.

The full disclosure and coordinated disclosure of security vulnerability.

vi) Rules that make bug bounty platforms mandatory in every organization [16]
vii) Rules of Incentivizing validation [16]. This rule gives hackers the obligation of validating security vulnerabilities detected before incentives are provided by the organization.

SUMMARY

Currently, the operations of bug bounty platforms or search for security vulnerability is gaining global momentum given the rising security vulnerability that organization systems are been exposed to by black hats or unethical hacks and given the chances of limited prospects for unregulated by in-house hackers. Therefore, the adoption of the above-listed rules can drive the optimal adoption and engagement of white hats in the prompt discovery of security vulnerabilities by global entities or major powers and ensure the speedy disclosure of threats discovered to achieve quick response by the organization's IT team.

REFERENCES

[1] Finifter, M., Akhawe, D., Wagner, D. (2013). An empirical study of vulnerability rewards programs. In: USENIX Security Symposium.

[2] Kuehn, A., Mueller, M. (2014). Analyzing bug bounty programs: An institutional perspective on the economics of software vulnerabilities. TPRC Conference Paper

[3] Zhao, M., Grossklags, J., Liu, P. (2015). An empirical study of web vulnerability discovery ecosystems. In: 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS)

[4] Amit Elazari (2019). Private ordering shaping cybersecurity policy: The case of bug bounties. In R. Ellis & V. Mohan (Eds.), Rewired: Cybersecurity Governance (pp. 102). Wiley.

[5] Matthew Finifter, Devdatta Akhawe, and David Wagner (2013). An empirical study of vulnerability rewards program. In 22nd USENIX Security Symposium (USENIXSecurity). USENIX Association.

[6] Aron Laszka, Mingyi Zhao, Akash Malbari, and Jens Grossklags (2018). The rules of engagement for bug bounty programs. In 22nd International Conference on Financial Cryptography and Data Security (FC). Springer.

[7] Kelsey R. Fulton, Samantha Katcher, Kevin Song, Marshini Chetty, Michelle L. Mazurek, Chloé Messdaghi, and Daniel Votipka (2023). Vulnerability discovery for all: Experiences of marginalization in vulnerability discovery. In To Appear in 32nd USENIX Security Symposium (USENIX Security). USENIX Association.

[8] Daniel Votipka, Seth Rabin, Kristopher Micinski, Jeffrey S. Foster, and Michelle L. Mazurek (2020). An observational investigation of reverse engineers' processes. In 29th USENIX Security Symposium (USENIX Security). USENIX Association.

[9] Bozorgi, M., Saul, L., Savage, S., & Voelker, G. (2010). Beyond heuristics: Learning to classify vulnerabilities and predict exploits. In Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD).

[10] Clark, S., Frei, S., Blaze, M., Smith, J. (2010). Familiarity breeds contempt: The honeymoon effect and the role of legacy code in zero-day vulnerabilities. In: Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC). pp. 251–260

[11] Ozment, A. (2005). The likelihood of vulnerability rediscovery and the social utility of vulnerability hunting. In: Workshop on the Economics of Information Security (WEIS)

[12] Ozment, A., Schechter, S. (2006) Milk or wine: Does software security improve with age? In: USENIX Security Symposium

[13] Edmundson, A., Holtkamp, B., Rivera, E., Finifter, M., Mettler, A., Wagner, D. (2013). An empirical study on the effectiveness of security code review, In Engineering Secure Software and Systems

[14] Huang, K., Siegel, M., Madnick, S., Li, X., Feng, Z. (2016). Poster: Diversity or concentration? Hackers' strategy for working across multiple bug bounty programs. In 37th IEEE Symposium on Security and Privacy (S&P)

[15] Maillart, T., Zhao, M., Grossklags, J., Chuang, J. (2017). Given enough eyeballs, all bugs are shallow? Revisiting Eric Raymond with bug bounty markets. Journal of Cyber security.

[16] Zhao, Grossklags, and Liu, (2016) "An empirical study of web vulnerability discovery ecosystems." Hacker One, Improving Public Bug Bounty Programs with Signal Requirements, HackerOne Blog. https://hackerone.com/blog/signalrequirements

[17] The bug-bounty rules for Twitter on the Hacker One platform