Bug Bounty Assessment

Amit Kumar
Department of MCA
RV College of Engineering
Bengaluru, India
amitk.mca21@rvce.edu.in

Dr.S.S.Nagamuthu.Krishnan
RV College Of Engineering
Bengaluru,India
ssnk@rvce.edu.in

Abstract - Bug bounty program is a initiative that invites security researchers to find vulnerabilities and report them to the organization running the program. This concept emerged as a way to harness the collective intelligence and skills of the security community to identify and address software vulnerabilities before they can be exploited by malicious actors .The bug bounty assessment refers overview of a bug bounty program. It typically includes key details about the program, its objectives.it encourage participants to focus on identifying critical vulnerabilities that could compromise user data, system integrity, or overall security. The program encompasses both web and mobile applications, APIs, and selected infrastructure components.

Keywords: Bug Bounty, Security, Vulnerability Assessment.

Introduction

Bug bounty programs have emerged as a powerful approach for organizations to enhance their cyber security posture by leveraging the collective intelligence and skills of a global community of security researchers. These programs provide a platform for security researchers, often referred to as white-hat hackers or ethical hackers, to identify and report vulnerabilities in exchange for monetary rewards or recognition.

The concept of bug bounty represents a shift from traditional security testing methods, where organizations rely solely on internal resources or third-party penetration testing firms. Bug bounty programs offer a more dynamic and proactive e approach, enabling organizations to tap into a diverse pool of talented individuals who possess specialized knowledge and expertise in finding security flaws.

The primary goal of bug bounty programs is to identify and address vulnerabilities before malicious actors can exploit them. By actively encouraging independent security researchers to search for weaknesses, organizations can uncover and resolve potential security risks, thereby reducing the likelihood of breaches, data leaks, and other malicious activities. Bug bounties also provide organizations with an opportunity to gain valuable insights into the effectiveness of their security controls, architecture, and incident response capabilities.

Literature Survey

We studied papers from various journals, conferences, and acquired data. The following is how the various papers are organized:

David Wheeler this paper proposes compares different vulnerability severity rating systems, analyzing their strengths, weaknesses, and inconsistencies. It provides insights into the challenges of assessing vulnerability severity and offers recommendations for improving the accuracy and consistency of severity ratings [1]

Thao Dang and Laurent This survey paper provides an overview of various vulnerability assessment techniques used in cyber security. It covers network vulnerability assessment, application security testing, penetration testing, and other assessment methods. The paper discusses the strengths and limitations of each technique and provides guidance for selecting appropriate approaches network anomalies, such as DoS and DDoS attacks.[2]

Christian Dietrich, et al in This paper presents a comprehensive survey of automated vulnerability assessment techniques. It covers vulnerability scanners, static analysis tools, and hybrid approaches. The survey discusses the capabilities, limitations, and challenges of automated vulnerability assessment and highlights future research directions in the field.[3]

James Newsome and Dawn Song This paper focuses on evaluating the effectiveness of network vulnerability scanners. It proposes a framework for assessing the accuracy and completeness of

vulnerability scanning tools. The paper presents empirical results comparing different commercial scanners and provides insights into their strengths and weaknesses. [4]

Richard A. Kemmerer, et al. This research paper introduces a framework for quantifying the impact of vulnerability announcements on the security of software systems. It proposes metrics to measure the severity, exploitability, and discoverability of vulnerabilities. The framework aims to provide a standardized approach for assessing the impact of vulnerabilities and prioritizing remediation efforts.[5]

Jingyu Hua et al This survey paper focuses on vulnerability assessment techniques specific to web services. It covers various types of vulnerabilities in web services, such as XML-based attacks and injection vulnerabilities. The paper reviews existing vulnerability assessment approaches for web services and discusses their effectiveness and limitations.[6]

Mekkattu et al, This survey study offers overview of various deep-learning methods used for vulnerability detection, including CNNs. It covers several facets of deep learning-based detection, including feature extraction, and network traffic analysis. The authors also go through the difficulties and potential directions for further research in this area.[7]

Proposed Methodology

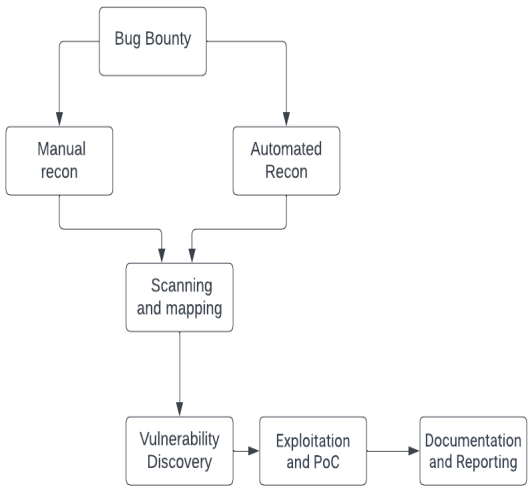

Fig 1. Architecture Diagram

The following are the main characteristics and elements :

Bug bounty programs offer organizations a proactive and crowd-sourced approach to identify and address software vulnerabilities. to discover and responsibly disclose vulnerabilities in exchange for financial rewards, bug bounty programs provide a valuable layer of defense against potential cyber threats. These programs promote continuous testing, responsible disclosure, and collaboration between organizations and bug hunters, ultimately leading to improved security for software applications, systems, and digital assets.

a)Bug Bounty

Program Familiarization: Read and understand the bug bounty program's guidelines, rules, scope, and rewards structure.

b)Reconnaissance:

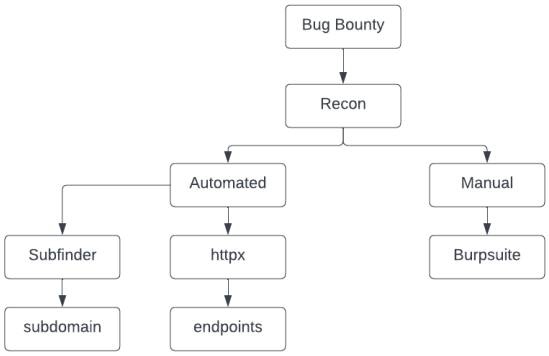

Fig 2. Recon Diagram

Reconnaissance is a critical phase in bug bounty programs that involves gathering information about the target assets before conducting vulnerability assessments.[11] It is the initial step where bug hunters gather intelligence to understand the target's attack surface and identify potential entry points.[12] Reconnaissance techniques include passive information gathering, such as searching for public information, analyzing DNS records, inspecting web archives, or exploring social media profiles.

c) Scanning and Mapping:

[13]Scanning and mapping are crucial steps in bug bounty programs that follow the reconnaissance phase. Scanning involves using automated tools or techniques to systematically probe the target's infrastructure, applications, and network for potential vulnerabilities.[14] These tools scan for common security issues, misconfigurations, or weaknesses that could be exploited.

[15] Mapping refers to the process of creating a comprehensive understanding of the target's attack surface. It involves identifying all accessible entry

points, such as web applications, APIs, network services, or endpoints, and mapping out their interconnections and dependencies.

d) Vulnerability Discovery

Vulnerability discovery is a core objective of bug bounty programs. It refers to the process of actively identifying security vulnerabilities within the target applications, systems, or infrastructure.[8]This includes well-known vulnerabilities like Cross-Site Scripting (XSS), SQL Injection, Cross-Site Request Forgery (CSRF), or Server-Side Request Forgery (SSRF) Bug hunters various techniques and methodologies to uncover vulnerabilities that could potentially be exploited by malicious actors.

e) Exploitation and PoC

Exploitation and Proof-of-Concept (PoC) are important stages in bug bounty programs that follow the discovery of a vulnerability. These stages involve validating the vulnerability's impact and demonstrating its exploitability.Proof-of-Concept (PoC) as evidence of the vulnerability's exploitability. [9]The PoC is a clear and concise demonstration of the steps needed to reproduce the vulnerability, showcasing the potential consequences or risks associated with it. It provides a practical illustration that helps program organizers understand the severity and urgency of the vulnerability

f) Documentation and Reporting

Documentation and reporting are essential components of bug bounty programs that enable bug hunters to communicate their findings effectively to program organizers. After discovering and validating a vulnerability, bug hunters meticulously document their findings and prepare a comprehensive report.[10]The documentation includes detailed information about the vulnerability, its impact, steps to reproduce, and any supporting evidence like screenshots, code snippets, or network captures

Conclusion

[16] Bug bounty assessments provide a proactive and crowd-sourced approach to identifying and addressing vulnerabilities in software applications, systems, and infrastructure.[17] They harness the collective intelligence and expertise of security researchers, often referred to as bug hunters, to uncover security weaknesses before they can be exploited by malicious actors Bug bounty programs allow for ongoing security testing, enabling organizations to benefit from the continuous efforts of bug hunters to identify and report vulnerabilities.

References

[1] David Wheeler and Emily Ratliff, "A Comparative Analysis of Vulnerability Severity Ratings" in IEEE Access, vol. 6, pp. 32280-32289, 2018.

[2] Thao Dang and Laurent Mounier., "A Survey of Vulnerability Assessment Techniques in Cybersecurity" in IEEE Internet of Things Journal, vol. 7, no. 6, pp. 5245-5256, June 2020.

[3] Christian Dietrich, et al., " Automated Vulnerability Assessment," in IEEE Transactions on Network and Service Management, vol. 15, no. 3, pp. 1241-1254, Sept. 2018.

[4] James Newsome and Dawn Song., " Measuring the Effectiveness of Network Vulnerability Scanners," in IEEE Transactions on Industrial Informatics, vol. 15, no. 8, pp. 4518-4527, Aug. 2019.

[5] Richard A. Kemmerer, et al., " A Framework for Measuring the Impact of Vulnerability Announcements," in IEEE Communications Magazine, vol. 55, no. 2, pp. 126-133, Feb. 2017.

[6] Jingyu Hua, et al.,"Vulnerability Assessment for Web Services" in IEEE Access, vol. 7, pp. 31288-31297, 2019.

[7] A. Azzouni et al., "Deep Learning for Bug bounty Assessment," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 2025-2067, third quarter 2020.

[8] H. Nguyen et al., "A SQl Intrusion Detection System for Identifying Malicious Executables," in Proceedings of the 2019 Neural Networks (IJCNN), Budapest, Hungary, 2019, pp. 1-8.

[9] H. Fryer and E. Simperl, "Web science challenges in researching bugbounties," in Proceedings of the 2017 ACM on Web Science Conference. ACM, 2017, pp. 273–277.

[10]. Allodi, "Economic factors of vulnerability trade and exploitation," in Proceedings of the 2017 ACM SIGSAC

Conference on Computer and Communications Security. ACM, 2017, pp. 1483–1499

[11] D. Votipka, R. Stevens, E. Redmiles, J. Hu, and M. Mazurek,"Hackers vs. testers: A comparison of software vulnerability discoveryprocesses," in 2018 IEEE Symposium on Security and Privacy (SP).

IEEE, 2018, pp. 374–391.

[12] T. D. LaToza and A. van der Hoek, "Crowdsourcing in software engineering: Models, motivations, and challenges," IEEE software, vol. 33, no. 1, pp. 74–80, 2016.

[13] M. Zhao, J. Grossklags, and P. Liu, "An empirical study of webvulnerability discovery ecosystems," in Proceedings of the 22nd ACMSIGSAC Conference on Computer and Communications Security.ACM, 2015, pp. 1105–1117.

[14] J. L. Christian, "Bug bounty programs: Analyzing the future of vulnerability research," Ph.D. dissertation, Utica College, 2018. J. Ruohonen and L. Allodi, "A bug bounty perspective on the disclosure of web vulnerabilities," arXiv preprint arXiv:1805.09850, 2018

[15] H. Homaei and H. R. Shahriari, "Seven years of software vulnerabilities: The ebb and flow," IEEE Security & Privacy, vol. 15, no. 1, pp. 58–65, 2017

[16] M. Zhao, J. Grossklags, and K. Chen, "An exploratory study of white hat behaviors in a web vulnerability disclosure program," inProceedings of the 2014 ACM workshop on security information workers. ACM, 2014, pp. 51–58.

[17] A. Kuehn and M. Mueller, "Analyzing bug bounty programs: An institutional perspective on the economics of software vulnerabilities," in TPRC, the 42nd Research Conference on Communication, Information and Internet Policy, 2014.