An Extensive Research on Bug Bounties

Rahul Kumar
21BCS1723@cuchd.in
CSE Department
Chandigarh University
Mohali,India

Kushagr Jain
21BCS1877@cuchd.in
CSE Department
Chandigarh University
Mohali,India

Supervisor :
Er. Gurleen Kaur
Gurleen.e14988@cumail.in

ABSTRACT—**Bug bounty programs have become a pivotal component in modern cybersecurity strategies, offering organizations an innovative approach to discover and remediate vulnerabilities in their software systems. This research paper delves into the landscape of**

bug bounty programs, examining their evolution, impact on cybersecurity, challenges, and future prospects. Through an extensive analysis of existing literature, empirical data, and case studies, this paper seeks to shed light on the dynamics, benefits, and limitations of bug bounty programs.

The research investigates the underlying motivations for hackers and security researchers participating in bug bounty programs, exploring the incentives, rewards, and ethical considerations shaping their engagement. Additionally, it evaluates the effectiveness of bug bounty initiatives in identifying and mitigating security vulnerabilities compared to traditional security assessment methods.

Furthermore, the paper outlines the operational aspects of bug bounty programs, discussing best practices in program design, management, and coordination between organizations and security researchers. It examines the role of automation, AI-driven tools, and platforms in streamlining bug bounty processes while ensuring the integrity and credibility of reported vulnerabilities.

This research paper also addresses the challenges faced by bug bounty programs, including issues related to vulnerability disclosure, scalability, legal complexities, and the growing sophistication of cyber threats. It analyzes the implications of these challenges on the sustainability and effectiveness of bug bounty initiatives.

INTRODUCTION : a ‘bug bounty’ or ‘vulnerability reward program’ (vrp) is the process for rewarding the discovery of a flaw or vulnerability in a piece of software. The concept has been around for a long time, notably donald knuth offering rewards for omissions in his the art of programming books, or flaws in his latexsoftware, and in the 1990s netscape offered a reward for flaws in its browser. Despite this history, examples of its application have been sparse up until the last few years where its popularity has increased, as this decade high profile programs from companies such as mozilla and google[26], and even the us department of defense in 2016 have started. There now exist services which act as middlemen in connecting companies with people who are prepared to search their systems for weaknesses. This paper will provide a brief review of some of the key research into bug bounties. For the most part, this has been tangential, merely acknowledging their existence, as a part of overall web or application securityease of use

Technology : it is vital to giving individuals and organizations the system security tools wanted to protect themselves as of cyber attacks. Three chief objects essential be threatened: endpoint strategies like pcs, handheld devices, and routers; systems; and the cloud. Shared technology cast-off to defend these objects contain next-generation firewalls, dns pass through a filter, malware defence, antivirus tools, and email safety results. Cyber might be distinct as somewhat connected to the collection of workstations or the network. At the same time, security means the mechanism of protecting anything. Consequently the terms cyber and safety took organized define the way of defensive user informations on or after the spiteful attacks that might clue to the security break. It is the time that has been cast-off for a period back afterward the internet happening developing like whatever. By asset of cybersecurity, any society or any user can protected their critical data from hackers. However it is apprehensive with hacking at around point, it in fact used ethical hacking to contrivance cybersecurity in any structuremaintaining the integrity of the specifications.

Proccess :

i)Choose a Bug Bounty program
ii)Understand Program Scope and Rules
iii)Reconnaissance and Research
iv)Scanning and Enumeration
v)Vulnerability Identification
vi)Exploitation and Proof of Concept (POC)
vii)Reporting
viii)Collaboration and Communication
ix)Validate and Retest
x)
Reward and Recognition

A. *Types of CyberSecurity*

I. Phishing: Phishing is the rehearsal of distribution fake communications that look like emails from dependable sources. The goal is to bargain thoughtful data comparable to credit card details and login data. It’s the greatest kind of cyber attack. You can help defend manually over learning or an expertise solution that sieves malicious electronic mail.

II. Ransomware: It is a type of malicious software. It is considered to extract currency by blocking contact to records or the PC system until the deal is paid. Paying the ransom does not assurance that the records will be recuperated or the system returned. Malware It is a type of software intended to gain illegal right to use or to cause impairment to a system. Social engineering It is a tactic that opponents use to pretend you into illuminating delicate information. They can importune a monetarist payment or improvement access to your reserved information.

III. Social engineering: It can be collective with some of the pressures registered above to style you additional probable to connect on links, transfer malware, or belief a malicious cause. Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity that you use in an equation.

IV. Definition Cyber Security and Bug Bounties

A bug bounty program is a crowdsourced initiative offered by companies, organizations, or software developers to incentivize independent security researchers, often referred to as "white-hat hackers" or "ethical hackers," to find and report security vulnerabilities or bugs in their software, applications, websites, or system. It could be defined as the procedure to ease the security fears in order to protect repute damage, commercial loss or financial loss of all group. The term Cybersecurity obviously required that it’s a gentle of security that we proposal to the organisation that frequent users can contact using the internet or over a network. There are numerous tackles and techniques that are castoff to deploy it. The greatest significant fact around safeguarding information is that it’s not a one interval procedure but a non-stop process. The organisation proprietor has to keep stuffs modernised in mandate to keep the hazard low

V. Goals :

A. Bug bounty programs have several overarching goals aimed at improving cybersecurity and fostering collaboration between organizations and independent security researchers. Some key goals include:

B. Identifying Vulnerabilities: Bug bounties aim to discover and report security vulnerabilities that might otherwise remain unidentified. This proactive approach helps organizations identify and fix weaknesses before they can be exploited by malicious actors.

C. roving Security Posture: By incentivizing ethical hackers to find and report vulnerabilities, bug bounty programs contribute to enhancing the overall security posture of software, websites, or systems. This allows organizations to fortify their defenses against potential cyber threats.

D. Encouraging Responsible Disclosure: Bug bounty programs encourage ethical disclosure of vulnerabilities by providing a structured channel for security researchers to report their findings. This helps prevent the exploitation of vulnerabilities for malicious purposes and fosters a culture of responsible disclosure.

E. Engaging with the Security Community: Bug bounty programs facilitate collaboration and engagement with the wider security community. They enable organizations to tap into the diverse skill sets and expertise of independent researchers worldwide, creating a collaborative ecosystem focused on cybersecurity.

F. Rewarding Security Researchers: These programs provide monetary rewards, recognition, or other incentives to ethical hackers who responsibly disclose vulnerabilities. This motivates researchers to actively search for and report security issues, incentivizing their ongoing involvement in improving security.

G. Enhancing Customer Trust: Organizations that run bug bounty programs demonstrate a commitment to security and transparency. Engaging in such initiatives can boost customer confidence and trust in the security measures implemented by the organization.

VI. Methodology :

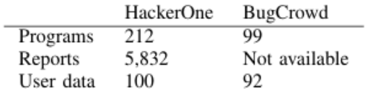
Despite the increasing popularity of bug bounties [6], and their seeming relationship with crowdsourcing, we were unaware of any work which considered bug bounties within the context of crowdsourcing. The one exception to this was Su &Pan, who proposed a system to introduce micro tasking to the process, where additional actors would test and verify the vulnerability submitted by another researcher [36]. As a result, we conducted a literature review, based on the methodology of Maoetal’s review of the related area of crowdsourced software engineering . The search was for the phrases “bug bounties", “vulnerability reward program", “vulnerability disclosure", in any available eld in seven online search engines: ACM Digital Library, IEEE Digital Library, Springer link Online Library, Wiley Online Library, Elsevier ScienceDirect, ProQuest, and Google Scholar. As a fallback, we additionally used snowballing of references where further titles were identified. To identify relevant literature, the title, abstract and introduction sections of each paper were read, which was usually enough to identify it as being outside the criteria for inclusion. Where this was not the case, the whole paper was read. As an exploratory study, our research question was: what are the gaps in the existing literature related to bug bounties, which can be addressed by crowdsourcing? As a result, the inclusion criteria for the literature review was that the paper in question was about bug bounties specifically, or contained analysis of a bug bounty program, platform, or behaviour of the workers in a program. Literature was excluded where it merely mentioned the existence of bug bounties, or it focused on vulnerability management more generally. In future work, it is intended that this inclusion criteria be widened, because these are all relevant with regards to policy implications, as well as assessing cost-e effectiveness for starting a bug bounty.

A. *Data Points for latest bug bounties :*

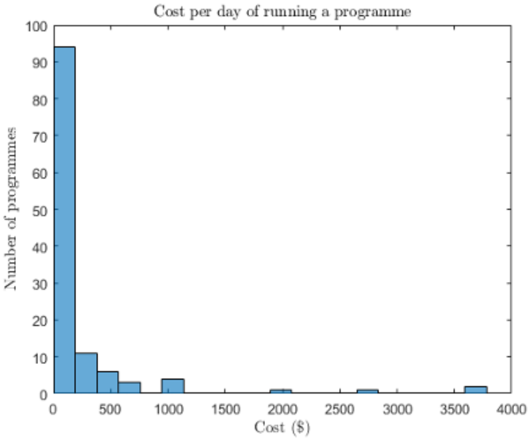
An increasingly popular approach to identifying vulnerabilities in software is to offer rewards to security researchers that are external to an organisation ('hackers') to find and disclose vulnerabilities [1]. This approach is now seeing adoption in areas such as e-voting systems, government systems and self driving cars [2]–[4]. As an example. the Swiss government launched a program offering e132,000 for hackers to find vulnerabilities in an e voting system. Rewards of up to e 44,000 were made available to hackers who discovered undetectable ways of manipulating votes [2]. As another example, the US Department of Defense (DoD) launched the 'Hack the Pentagon' pilot program in April 2016, with the aim of assessing the benefit of opening up vulnerability discovery to hackers. Within six hours 138 vulnerabilities were found and reported [5]. The success of the program has led to the DoD introducing a new vulnerability disclosure policy, opening up new domains to hackers [3], [6]. There have also been suggestions for US government departments to participate in searches for vulnerabilities in open-source projects [7].

GRAPHS RELATED TO THE DATA POINTS FOR THE LATEST BUG BOUNITIES :

TABLE II
SUMMARY OF INFORMATION COLLECTED FROM HACKERONE AND BUGCROWD



	HackerOne	BugCrowd
Programs	212	99
Reports	5,832	Not available
User data	100	92



THE ABOVE GRAPH REPRESENTS THE NUMBER OF PRORGRAMMES TO THE TOTAL COST OF RUNNING THESE PROGRAMS AS BUG BOUNTIES. IT PROVIDES A VIEW FROM 2 DIFFERENT SITES LIKE HACKERONE AND BUGCROWD

Acknowledgement

I would like to express my sincere gratitude to all those who contributed to the completion of this research paper on "An Extensive Research on Bug Bounties."

First and foremost, I extend my deepest appreciation to , my supervisor/advisor, for their invaluable guidance, continuous support, and insightful feedback throughout the research process. Their expertise and encouragement have been instrumental in shaping this study.

I am profoundly grateful to the participants and contributors within the bug bounty community who generously shared their insights, experiences, and expertise. Their willingness to share knowledge has been invaluable in understanding the nuances and intricacies of bug bounty programs.

I would also like to extend my thanks to the researchers, authors, and professionals whose published work and contributions formed the foundation for this research. Their pioneering efforts have been an inspiration and a valuable resource.

Special thanks to my family and friends for their unwavering encouragement, understanding, and patience during this research journey. Their support provided the strength needed to persevere through challenges.

Finally, I would like to acknowledge [Institution/Organization Name] for providing the necessary resources, facilities, and environment conducive to research endeavors.

This research would not have been possible without the support, guidance, and contributions of all those mentioned above. Any errors or omissions are solely my responsibility.

REFERENCES :

coordinated vulnerability disclosure," Crime Science, vol. 7, no. 1, pp. 16–17, 2018. [1] H. Fryer and E. Simperl, "Web science challenges in researching bug bounties," in Proceedings of the 2017 ACM on Web Science Conference. ACM, 2017, pp. 273–277. [2] Euro News. (2019, Feb) Euro News: Switzerland paying e-voting hackers. [Online]. Available: https://www.euronews.com/2019/02/13/ switzerland-offers-cash-to-hackers-who-can-crack-its-e-voting-system [3] Department of Defense. (2018, Oct) United States Department of Defense: Expanding hack the Pentagon. [Online]. Available: https://dod.defense.gov/News/News-Releases/News-Release-View/ Article/1671231/department-of-defense-expands-hack-the-pentagon crowdsourced-digital-defense-pr/ [4] AI Trends. (2019, Feb) AI trends: Bug bounties and AI systems: The case of AI self-driving cars. [Online]. Available: https://www.aitrends.com/ai-insider/bug-bounties-and-ai-systems-the case-of-ai-self-driving-cars/ [5] HackerOne. (2016, Jul) HackerOne: Hacking the pentagon. [Online]. Available: https://www.hackerone.com/blog/hack-the-pentagon-results [6] A. T. Chatfield and C. G. Reddick, "Cybersecurity innovation in government: A case study of US Pentagon's vulnerability reward program," in Proceedings of the 18th Annual International Conference on Digital Government Research. ACM, 2017, pp. 64–73. [7] A. Schwartz, R. Knake, and Belfer Center for Science and International Affairs, Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process. Harvard Kennedy School, Belfer Center for Science and International Affairs, 2016. [8] HackerOne. (2019, Jan) HackerOne: Bug bounty program directory. [Online]. Available: https://hackerone.com/directory [9] M. Finifter, D. Akhawe, and D. Wagner, "An empirical study of vulnerability rewards programs," in USENIX Security Symposium, 2013, pp. 273–288. [10] Glassdoor. (2019, Jan) Glassdoor: Software engineer salaries in london. [Online]. Available: https: //www.glassdoor.co.uk/Salaries/london-software-engineer-salary.htm [11] M. Blatter, S. Muehlemann, and S. Schenker, "The costs of hiring skilled workers," European Economic Review, vol. 56, no. 1, pp. 20–35, 2012. [12] P. Foreman, Vulnerability management. 9. [Online]. Available: https://www.bsimm.com/download/ [14] BugCrowd. (2018, Aug) BugCrowd: Integrating crowdsourced security with the SDLC. [Online]. Available: https://www.bugcrowd.com/blog/integrating-crowdsourced-security with-the-software-development-lifecycle/ [15] Google. (2019, Jan) Google: Vulnerability reward program. [Online]. Available: https://www.google.com/about/appsecurity/reward-program/index.html [16] Facebook. (2018, Sep) Facebook: Whitehat program. [Online]. Available: https://www.facebook.com/whitehat [17] Microsoft. (2018, Jul) Microsoft: Bug bounty programs. [Online]. Available: https://www.microsoft.com/en-us/msrc/bounty [18] HackerOne. (2019, Jan) HackerOne: HackerOne bug bounty platform. [Online]. Available: https://www.hackerone.com/ [19] BugCrowd. (2019, Jan) BugCrowd: BugCrowd bug bounty platform. [Online]. Available: https://www.bugcrowd.com [20] Cobalt. (2019, Jan) Cobalt: Bug bounty platform. [Online]. Available: https://cobalt.io/ [21] 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. [22] E. Raymond, "The cathedral and the bazaar," Knowledge, Technology & Policy, vol. 12, no. 3, pp. 23–49, 1999. [23] M. Rouse. (2007, Jun) Search Security: Whitehat hacker definition. [Online]. Available: https://searchsecurity.techtarget.com/definition/white-hat [24] A. Laszka, M. Zhao, A. Malbari, and J. Grossklags, "The rules of engagement for bug bounty programs," in International Conference on Financial Cryptography and Data Security, 2018. [25] M. W. Kranenbarg, T. J. Holt, and J. van der Ham, "Don't shoot the messenger! a criminological and computer science perspective on [26] E. Kovacs. (2018, Jul) SecurityWeek: Intel's record bounty. [Online]. Available: https://www.securityweek.com/intel-pays-100000-bounty new-spectre-variants [27] L. 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. [28] D. Votipka, R. Stevens, E. Redmiles, J. Hu, and M. Mazurek, "Hackers vs. testers: A comparison of software vulnerability discovery processes," in 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018, pp. 374–391. [29] 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. [30] M. Zhao, J. Grossklags, and P. Liu, “An empirical study of web vulnerability discovery ecosystems,” in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015, pp. 1105–1117. [31] Wooyun. (2016, Jun) Wooyun: Vulnerability disclosure platform. [Online]. Available: https://www.wooyun.org [32] P. Paganini. (2016, Aug) Security Affairs: Wooyun group arrested. [Online]. Available: https://securityaffairs.co/wordpress/49916/hacking/ wooyun-group-arrested.html [33] Google. (2019, Jan) Google: Chromium bug tracker. [Online]. Available: https://www.chromium.org [34] Google. (2019, Mar) Google Trends: Search popularity of bug bounty platforms. [Online]. Available: https://trends.google.com/trends/ explore?q=HackerOne,bugcrowd,safehats,Intigriti,Synack [35] Synack. (2019, Mar) Synack: Bug bounty platform. [Online]. Available: https://www.synack.com/solution/ [36] R. B¨ ohme, “A comparison of market approaches to software vulnerability disclosure,” in M¨uller G. (eds) Emerging Trends in Information and Communication Security. ETRICS 2006. Lecture Notes in Computer Science, vol 3995. Springer, Berlin, Heidelberg, 2006, pp. 298–311. [37] J. L. Christian, “Bug bounty programs: Analyzing the future of vulnerability research,” Ph.D. dissertation, Utica College, 2018. [38] J. Ruohonen and L. Allodi, “A bug bounty perspective on the disclosure of web vulnerabilities,” arXiv preprint arXiv:1805.09850, 2018. [39] First. (2019, Mar) First: User guide to CVSS 3.0. [Online]. Available: https://www.first.org/cvss/user-guide [40] HackerOne. (2019, Mar) HackerOne: Paypal program page. [Online]. Available: https://hackerone.com/paypal [41] N. Munaiah and A. Meneely, “Vulnerability severity scoring and bounties: Why the disconnect?” in Proceedings of the 2nd International Workshop on Software Analytics. ACM, 2016, pp. 8–14. [42] 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. [43] A. M. Algarni and Y. K. Malaiya, “Most successful vulnerability discoverers: Motivation and methods,” in Proceedings of the International Conference on Security and Management (SAM). The Steering Committee of The World Congress in Computer Science, Computer , 2013, p. 1. [44] HackerOne. (2019, Feb) HackerOne: Response target metrics. [Online]. Available: https://docs.hackerone.com/programs/response-target-metrics.html [45] European Commission. (2015, Sep) Publications office of the European Union: User guide to the SME definition. [Online]. Available: http://www.innovation.public.lu/en/brochures-rapports/s/ sme-definition/sme-definition-user-guide-2015.pdf [46] HackerOne. (2019, Feb) HackerOne: 188 fascinating facts. [Online]. Available: https://www.hackerone.com/blog/118-Fascinating-Facts HackerOnes-Hacker-Powered-Security-Report-2018 [47] M. Al-Banna, B. Benatallah, D. Schlagwein, M. C. Barukh, and E. Bertino, “Friendly hackers to the rescue: How organizations perceive crowdsourced vulnerability discovery,” in Pacific Asia Conference on Information Systems (PACIS), 2018. [48] D. Mu, A. Cuevas, L. Yang, H. Hu, X. Xing, B. Mao, and G. Wang, “Understanding the reproducibility of crowd-reported security vulnerabilities,” in 27th USENIX Security Symposium, USENIX Security 18), 2018, pp. 919–936. [49] HackerOne. (2018, Nov) HackerOne: 2018 hacker report. [Online]. Available: https: //www.hackerone.com/sites/default/files/2018-01/2018-Hacker-Report [50] A. Laszka, M. Zhao, and J. Grossklags, “Banishing misaligned incentives for validating reports in bug-bounty platforms,” in European Symposium on Research in Computer Security. Springer, 2016, pp. 161–178. [51] BIS. (2018, Oct) Department for Business Innovation and Skills: Business population estimates for the uk and regions 2018. [Online]. Available: https://assets.publishing.service.gov.uk/government/ uploads/ system/uploads/attachment data/file/746599/OFFICIAL SENSITIVE BPE 2018-statistical release FINAL FINAL.pdf [52] DIGIT. (2019, Jan) Directorate-general for informatics: Commission launches open source bug bounties. [Online]. Available: https://ec.europa.eu/newsroom/informatics/item-detail.cfm [53] A. Pentland, D. L. Shrier, and H. E. Shrobe, New Solutions for Cybersecurity. MIT Connection Science and Engineering, 2018. [54] K. Huang, M. Siegel, S. Madnick, X. Li, and Z. Feng, “Diversity or concentration? hackers’ strategy for working across multiple bug bounty programs,” in 37th IEEE Symposium on Security and Privacy (S&P), 2016. [55] M. Zhao, J. Grossklags, and K. Chen, “An exploratory study of white hat behaviors in a web vulnerability disclosure program,” in Proceedings of the 2014 ACM workshop on security information workers. ACM, 2014, pp. 51–58. [56] M. Zhao, A. Laszka, T. Maillart, and J. Grossklags, “Crowdsourced security vulnerability discovery: Modeling and organizing bug-bounty programs," in The HCOMP Workshop on Mathematical Foundations of Human Computation, Austin, TX, USA, 2016. [57] K. Afifi-Sabet. (2019, Feb) IT Pro: Meltdown and spectre. [Online]. Available: https://www.itpro.co.uk/exploits/30478/what-are-meltdown and-spectre-and-are-you-affecte

Summary:

I. Introduction

Bug Bounty Definition: A bug bounty program rewards ethical hackers for discovering and reporting vulnerabilities in software.

Historical Context: Bug bounty concepts have existed for a while, with examples like Donald Knuth and Netscape offering rewards.

Recent Popularity: Bug bounty programs gained popularity in recent years, with high-profile initiatives from companies like Mozilla and Google, as well as government involvement.

II. Technology and Cybersecurity

Essential Targets: Cybersecurity focuses on protecting endpoints (e.g., PCs, handheld devices), networks, and the cloud.

Shared Technologies: Next-generation firewalls, DNS filters, malware defense, antivirus tools, and email safety contribute to cybersecurity.

Cybersecurity Importance: Protects critical data from hackers, using ethical hacking to maintain system integrity.

III. Bug Bounty Process

Steps:

Choose a bug bounty program.

Understand program scope and rules.

Reconnaissance and research.

Scanning and enumeration.

Vulnerability identification.

Exploitation and Proof of Concept (POC).

Reporting.

Collaboration and communication.

Validate and retest.

Reward and recognition.

IV. Types of Cybersecurity Threats

Phishing: Distribution of fake communications to obtain sensitive data.

Ransomware: Malicious software designed to extract payment by blocking access to files or systems.

Social Engineering: Manipulating individuals to disclose sensitive information.

V. Definition of Cybersecurity and Bug Bounties

Bug Bounty Program Definition: Crowdsourced initiative rewarding ethical hackers for finding and reporting vulnerabilities.

Cybersecurity Definition: Security measures for internet-connected systems, requiring continuous updating.

VI. Goals of Bug Bounty Programs

Identifying Vulnerabilities: Proactively discover and fix vulnerabilities.

Improving Security Posture: Enhance overall security of software, websites, or systems.

Responsible Disclosure: Encourage ethical disclosure of vulnerabilities.

Engaging Security Community: Collaborate with the wider security community.

Rewarding Security Researchers: Incentivize ethical hackers with rewards and recognition.

Enhancing Customer Trust: Demonstrate commitment to security, building customer confidence.

VII. Methodology

Literature Review: Explored bug bounties within the context of crowdsourcing.

Research Question: Explored gaps in existing bug bounty literature that can be addressed by crowdsourcing.

VIII. Data Points for Latest Bug Bounties

External Identification of Vulnerabilities: Organizations offer rewards to external security researchers for finding and disclosing vulnerabilities.

Examples: Swiss government's e-voting system, the US Department of Defense's "Hack the Pentagon" program.

IX. Acknowledgment

Gratitude: Expresses gratitude to supervisors, bug bounty community, contributors, family, friends, and the institution/organization.

X. References

Literature Review: Lists references related to bug bounties, vulnerability disclosure, and cybersecurity.