Developing a gamified peer-reviewed bug bounty programme

Jamie O'Hare
Lynsay A. Shepherd

O'Hare, J. & Shepherd, L.A. (2022) 'Developing a gamified peer-reviewed bug bounty programme'. In: C. Stephanidis, M. Antona & S. Ntoa (eds.) *HCI International 2022 Posters: 24th International Conference on Human-Computer Interaction, HCII 2022, Virtual Event, June 26 – July 1, 2022, Proceedings. vol. part IV*. Springer, Cham, pp. 514-522, 24th International Conference on Human-Computer Interaction, 26 June-1 July 2022.

Developing a Gamified Peer-Reviewed Bug Bounty Programme

Jamie O'Hare[0000−0002−5847−6488] and Lynsay A. Shepherd[0000−0002−1082−1174]

Division of Cyber Security, School of Design and Informatics, Abertay University, Dundee, United Kingdom
{j.o'hare, lynsay.shepherd}@abertay.ac.uk

Abstract. Bug bounty processes have remained broadly unchanged since their inception. Existing literature recognises that current methods generate intensive resource demands, impacting upon programme effectiveness. This paper proposes a novel implementation which aims to alleviate resource demands and mitigate inherent issues through gamification. This incorporates the use of additional crowdsourcing of vulnerability verification and reproduction by peers, allowing the client organisation to reduce overheads at the cost of rewarding participants. The system has the potential to be used in Higher Education Institutions which typically face resource and budget constraints.

Keywords: Bug Bounty · Ethical Hacking · Human-Computer Interaction · Gamification · Higher Education

1 INTRODUCTION AND BACKGROUND

Traditionally, in-house teams, consulting penetration testers, or external good-natured researchers would identify and report security weaknesses to an accountable organisation. However, with large estates operating a diverse array of technologies, organisations struggle to identify all vulnerabilities. As a result, organisations are increasingly harnessing the power of crowdsourcing through the implementation of bug bounty programmes to combat this problem [21].

The past decade has seen the rapid adoption and development of bug bounty programmes [21, 5], however innovation remains scarce. Crowdsourcing mechanisms which underpin bug bounty programmes have been given minimal attention. One area of potential innovation is the introduction of gamification. Thus, this paper seeks to provide an overview of issues present in bug bounty programmes and presents a novel gamified bug bounty implementation based on the micro-tasking solution discussed by Su and Pan [17].

1.1 Bug Bounty Programmes

Figure 1 illustrates the most popular variants of the bug bounty process [4]. In process A the external hacker corresponds directly with the vendor, however process B introduces an intermediate platform. This intermediary can provide

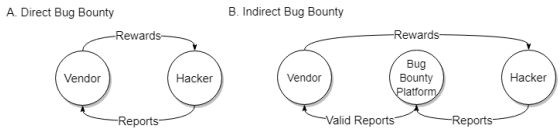

Fig. 1. Variants of the bug bounty process. Adapted from [14].

verification and triage on behalf of the vendor, mitigating the vendor's concomitant administrative impact for a fee. Google [5] follows the direct bug bounty process, whereas many organisations use platforms such as HackerOne [6] to facilitate the indirect process.

Typically, hackers receive a monetary reward for a successful submission; however, for less critical vulnerabilities or in a conservative programme, branded vendor merchandise or kudos may be awarded [11, 14]. A hacker can also receive a further bonus for a well-written report, or a novel discovery [12].

There are systemic issues with existing bug bounty crowdsourcing techniques. A prevailing issue is the high volume of low-quality submissions [1]. Insufficient report quality is a casualty of the first-come-first-served response to submissions, with hackers racing to submit a vulnerability. Many hackers concentrate on capitalising from their skills, by maximising submissions [7].

To address the signal-to-noise ratio, larger ecosystems attempt to educate their users to produce greater quality reports, while some programmes require specific information items. The 2018 update of ISO 29147 outlines various items to request in the vulnerability reporting process [9]. Others have introduced signal requirements and rate limiter mechanisms [10].

The first-come-first-served basis also gives rise to the issues surrounding duplicate submissions [23, 11], while essential details may be lacking. A vendor or platform requires communication with the hacker to gain further information in this scenario. Concurrently, another hacker may submit a more detailed report for the same vulnerability. Although possibly more beneficial to the vendor, the second report, under the first-come, first-served attitude, is a duplicate. The stance on duplicates varies across platforms and programmes, with some awarding the second hacker with non-monetary rewards, while most receive nothing. The latter actively discourages detailed submissions.

To facilitate an improved bug bounty process, we propose an implementation featuring gamification, addressing the issues found in traditional programmes.

1.2 Gamification

Gamification mechanics should be considered in the context of the environment in which they are placed and can include social networks, encouraging exploration, challenges, and the sharing of knowledge. User types have also been considered and help link which gamification elements might be better suited to individuals, e.g., free spirits who are motivated by autonomy may enjoy exploration elements [13][19].

Gamification has been used in a number of domains, including Higher Education [18]. It has also been used to help non-experts learn about the potential consequences of cybersecurity issues. Additionally, the development of a gamified environment has been proposed which would include elements such as leaderboards and onboarding tutorials to help senior executives at critical national infrastructure facilities decide how to invest in cyber defenses [2]. Furthermore, preliminary work has been conducted to improve security awareness in non-cybersecurity experts via the use of gamification in a mobile quiz application [16].

The implementation of gamification in bug bounty programmes is limited, though some programmes incorporate a leaderboard or a Hall of Fame, but go no further than this [20, 14, 12]. The solution proposed makes extensive use of gamification to address systemic issues within bug bounty programmes.

2 METHODOLOGY

2.1 Direct Crowd-vetted Bug Bounty

The proposed bug bounty process follows a four-step procedure, as presented in Figure 2. In Step 1, a hacker discovers a vulnerability and reports this finding to the vendor through appropriate channels. In Step 2, after optionally validating the report and checking for duplicates, the vendor redistributes this submission to a field of vetted hackers. In Step 3, these hackers, if possible, verify the original submission, and report back to the vendor on the verification and reproducibility of the report. Finally in Step 4, the vendor will receive an actionable vulnerability report or sound reasoning to dismiss the submission. If successful, the original hacker will receive a reward, while the verifiers will receive a reward regardless.

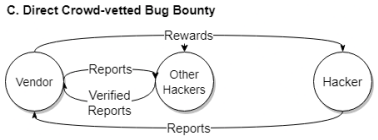

Fig. 2. Proposed bug bounty process using two phases of crowdsourcing.

The proposed methodology borrows from existing work [17], which suggested crowdsourcing of vulnerability discovery and verification. The novel solution this paper proposes differs by limiting the number of roles in the bug bounty process, allowing individuals to verify vulnerabilities as they see fit. Furthermore, a direct process is suggested with an intermediate in the form of a vetted hacker verification. This peer-review process is the methodology's unique aspect, introducing further crowdsourcing into the process. The reproduction process by multiple intermediary verifiers reduces the likelihood of false positives, while simultaneously, the reproduction and cooperation in refining the submission result

in a high-quality report. Greater report quality ensures minimal vendor interaction is required, thus reducing overhead. However, this proposed process is not without fault. Without vendor intervention, the verification process may dismiss more esoteric vulnerabilities, such as those valid yet out of scope and existing programmes address these on a case-by-case basis.

Nevertheless, this process presents significant opportunities for further development. Whereas current bug bounty processes concentrate on the reporter, this process allows the vendor organisation to build relationships with verifiers. Through these relationships, a community focused on the programme can be built [20]. As there are more moving parts in this process, there are more opportunities to implement gamification elements towards participation, verification and rewards. One such element may incentivise the process' innate potential as an educational resource. Through the verification process, participants will become exposed to new methods, similar to the existing disclosed reports process; however, verifiers will go further by performing the required actions to exploit a vulnerability successfully [22, 20].

However, this process introduces unique threats, arising from the introduction of other individuals upstream [7]. One particular issue is the possibility verifiers may collude with the reporter to receive rewards without proper scrutiny. Similarly, a verifier may seek a report's dismissal only to submit the same issue. Another issue is the difficulty in maintaining a consistent barometer for verified vulnerabilities with a rotating cast of verifiers of differing expertise [15]. Also, the gamification components may introduce an element of competitiveness, from which significant privacy and trust issues can arise.

2.2 Aspects of Gamification

When developing a gamified bug bounty programme, it is vital to consider challenges typically found in traditional programmes; gamification should mitigate the following issues. **A1:** Inclusion of all aspects of the bug bounty process for each user, and consideration of the individuals' expertise in each of these areas. **A2:** Implementation of gamification elements should enhance and support the experience. **A3:** Incentivise participation in the programme. **A4:** Encourage prolonged activity across the programme.

Existing bug bounty programmes give minimal consideration to such features. Gamification elements should encompass all steps of the bug bounty process to satisfy the criteria outlined in A1, and should ensure symmetry in gamification elements between vulnerability discovery and verification. This would value both processes equally, potentially mitigating the possible neglect for one system over another. Programmes should be dynamic and tailored to one's strengths and weaknesses to provide an engaging experience.

Some bug bounty programmes currently incentivise higher quality submissions, thus enhancing the bug bounty experience and effectiveness, through additional monetary rewards [23]. Gamification elements could substitute or reinforce such a process. Encouraging well-mannered correspondence, promoting diverse vulnerability discovery methods, and alignment to pressing business objectives

are all goals further gamification implementations can pursue in the name of programme effectiveness.

Bug bounty participants are heterogeneous, with the majority never achieving a successful submission [7]. However, in the proposed method, less successful participants can still contribute to the programme through the verification process. They can learn from peers and apply this new knowledge in their pursuit of vulnerabilities. In this scenario, a prolific verifier encounters significant incentivisation to attempt vulnerability discovery and vice-versa. Other methods to encourage participation could include initial higher incentives and rewards.

While scope increases and significant codebase updates can sustain participation in the bug bounty process, A4 strives to achieve this through gamification aspects. With a significant decrease in activity typical after the initial launch window of a bug bounty, programme managers will attempt to repeat the success through attracting participants to return with limited-time events with greater rewards. Such events often coincide with scope increases. Providing solely monetary incentivisation during this event can lead to a significant signal-to-noise ratio impacting the effectiveness of this strategy [4] and may lead participants to ignore difficult vulnerabilities, in favour of superficial bugs. This strategy could partly or completely replace monetary incentivisation for gamification elements.

To address potential issues, the proposed solution includes gamification concepts that may appeal to all users of the system (general and rewards elements), and more specific elements which link to user types. Gamification Inspiration Cards were used [13] to determine elements for inclusion.

General and Reward Elements These concepts can work for a variety of user types. An example is *Investment* where rewards such as badges and points, leaderboards, and increasingly complex challenges to foster investment and support engagement. Another concept is *Progress and feedback* as users need to receive feedback to remain engaged, and to highlight their advancement through the system - badges and achievements can be used to support this. Finally, *Onboarding & tutorials* should be considered - teaching users how to use the system will help them become accustomed and will support engagement. Rewards can also support a number of user types. One method of implementing these is via a *Fixed reward schedule* - where rewards can be awarded based on specific events within the system, e.g., a user's first submission could earn double points. Badges could be used for every 10 verified submissions to the programme. Providing fixed objectives may address issues concerning sustaining participants and their attention.

User Types These can include *Players* motivated by rewards implemented via badges, achievements, leaderboards, and points (A1-A4). *Achievers* are motivated by mastering skills, which can be achieved by the use of certificates and challenges (A1-A4). *Socialisers* are motivated by relatedness to others. This can be generated via a social status, competitions, guilds, and teams A1-A3). Fi-

nally, *Philanthropists* are motivated by purpose. This can be implemented via a clear meaning as to what the programme is trying to achieve (A2-A3).

2.3 Suitable Implementation Environment

One area that harmonises well with the proposed process's strengths and weakness is a tertiary educational institution environment. Currently, bug bounty programmes at education institutions seem limited to select American universities, yet, some British counterparts operate vulnerability disclosure policies. The reduced overhead removes a considerable upfront burden from an often less-resourced information services department. Gamification's compatibility provides an alternative to an economic incentivisation measure. Additionally, the use of students and staff as participants in the process mitigates severe trust-related issues through their existing relationship. Lastly, the process provides an additional educational resource where students can swap isolated labs or virtual machines for an authentic infrastructure with real-world impact.

3 DISCUSSION

3.1 Strengths and Limitations of the Proposed Solution

There is ample room for further implementation of gamification in the bug bounty domain. One example is a bug hunter submitting a singular bug, which unknowingly impacts more systems across the programme's scope. Those who become aware of this vulnerability through the verification process may report the other instances. While unfair to the original reporter, the issue is multi-faceted. Failing to identify multiple instances of the same vulnerability shows immaturity in the bug hunter's methodology. Thus during the verification process, verifiers should remind the hunter to seek other vulnerability instances. Similarly, upon remediation, if the organisation does not identify other instances, it highlights problems in the remediation process. Gamification could reward original reporters and those who cite their work in subsequent related reports.

3.2 The Role of Gamification

Commonly used gamification elements found in Higher Education computing courses include points, badges, and leaderboards. Gamification must fit within the context used, and emotions, engagement, and motivation must factor into the design [3]. Through the gamified peer review process, participants will learn effective report writing and technical skills through bug hunting or validation reports, augmenting what cybersecurity students learn through their curriculum.

Although gamification is widely used in Higher Education, it has limitations [18]. Previous work implemented a gamification strategy in a course teaching introductory C programming at undergraduate level [8], aiming to improve knowledge acquisition. However it presented issues for students: some became disengaged when reaching the round number of one hundred points.

Prior studies that have noted the importance of reward evolution as the programme and organisation security matures [22, 1]. One study suggests front-loading the launch of a programme with high payouts, before adjusting payout structure to decrease payout towards a market average to allow for greater rewards for complex vulnerabilities [20]. By doing so, a programme can incentivise participation during the initial release and continue to encourage dedicated participation when the number of successful reports tapers. However, such a strategy may be less effective when a bug bounty operates on a significantly limited budget or relies on non-monetary rewards. Therefore, those in this scenario may require alternative solutions to keep encouraging participation.

4 CONCLUSION AND FUTURE WORK

By leveraging gamification techniques against common bug bounty issues, this paper proposes a new implementation intending to provide a crowdsourcing cybersecurity solution and an educational resource. Using a higher education institution as a potential use case allows for the consideration of gamification elements to improve programme effectiveness. Without a trial implementation and concomitant study, the reality of the process remains uncertain. However, this proposal highlights the limited use of gamification in bug bounties thus far and contributes approaches to implement aspects which may increase programme effectiveness. Future work seeks to establish the viability of this novel process in practice, with prototyping and user testing.

References

1. Al-Banna, M., Benatallah, B., Schlagwein, D., Bertino, E., Chai, B.M.: Friendly hackers to the rescue: How organizations perceive crowdsourced vulnerability discovery. In: PACIS. p. 230 (2018)
2. Cook, A., Smith, R., Maglaras, L., Janicke, H.: Using gamification to raise awareness of cyber threats to critical national infrastructure. In: 4th International Symposium for ICS & SCADA Cyber Security Research 2016 (ICS-CSR). pp. 1–11. BCS (2016). https://doi.org/https://doi.org/10.14236/ewic/ICS2016.10
3. Fischer, H., Heinz, M., Schlenker, L., Follert, F.: Gamifying higher education. beyond badges, points and leaderboards. Knowledge Communities in Online Education and (Visual) Knowledge Management pp. 93–104 (2016)
4. Fryer, H., Simperl, E.: Web science challenges in researching bug bounties. In: Proceedings of the 2017 ACM on Web Science Conference. p. 273–277. WebSci '17, Association for Computing Machinery, New York, NY, USA (2017). https://doi.org/10.1145/3091478.3091517
5. Google: Program rules - application security (2020), https://www.google.com/about/appsecurity/reward-program/. Last accessed 18 Feb 2021
6. HackerOne: Hacker powered security testing (2020), https://www.hackerone.com/
7. Hata, H., Guo, M., Babar, M.A.: Understanding the heterogeneity of contributors in bug bounty programs. In: Proceedings of the 11th ACM/IEEE International

Symposium on Empirical Software Engineering and Measurement. p. 223–228. ESEM '17, IEEE Press (2017)
8. Ibanez, M.B., Di-Serio, A., Delgado-Kloos, C.: Gamification for engaging computer science students in learning activities: A case study. IEEE Transactions on learning technologies **7**(3), 291–301 (2014)
9. ISO/IEC: International standard: Information technology—security techniques—vulnerability disclosure (29147:2018(e)) (2018), https://www.iso.org/standard/45170.html. Last accessed 18 Feb 2021
10. Laszka, A., Zhao, M., Grossklags, J.: Banishing misaligned incentives for validating reports in bug-bounty platforms. In: European Symposium on Research in Computer Security. pp. 161–178. Springer (2016)
11. Laszka, A., Zhao, M., Malbari, A., Grossklags, J.: The rules of engagement for bug bounty programs. In: International Conference on Financial Cryptography and Data Security. pp. 138–159. Springer (2018)
12. Malladi, S.S., Subramanian, H.C.: Bug bounty programs for cybersecurity: Practices, issues, and recommendations. IEEE Software **37**(1), 31–39 (2019)
13. Marczewski, A.: 52 Gamification Mechanics and Elements (2020), https://www.gamified.uk/user-types/gamification-mechanics-elements/. Last accessed 15 Jul 2020
14. Ruohonen, J., Allodi, L.: A bug bounty perspective on the disclosure of web vulnerabilities. In: "17th Annual Workshop on the Economics of Information Security (WEIS 2018), WEIS 2018 (2018)
15. Sanagavarapu, L.M., Reddy, Y.R.: Crowdsourcing security - opportunities and challenges. In: 2018 IEEE/ACM 11th International Workshop on Cooperative and Human Aspects of Software Engineering (CHASE). pp. 37–40 (2018)
16. Scholefield, S., Shepherd, L.A.: Gamification techniques for raising cyber security awareness. In: International Conference on Human-Computer Interaction. pp. 191–203. Springer (2019)
17. Su, H.J., Pan, J.Y.: Crowdsourcing platform for collaboration management in vulnerability verification. In: 2016 18th Asia-Pacific Network Operations and Management Symposium (APNOMS). pp. 1–4. The Institute of Electronics, Information and Communication Engineers (2016). https://doi.org/10.34385/proc.25.P1-7
18. Subhash, S., Cudney, E.A.: Gamified learning in higher education: A systematic review of the literature. Computers in Human Behavior **87**, 192–206 (2018)
19. Tondello, G.F., Mora, A., Marczewski, A., Nacke, L.E.: Empirical validation of the gamification user types hexad scale in english and spanish. International Journal of Human-Computer Studies **127**, 95–111 (2019)
20. Votipka, D., Stevens, R., Redmiles, E., Hu, J., Mazurek, M.: Hackers vs. testers: A comparison of software vulnerability discovery processes. In: 2018 IEEE Symposium on Security and Privacy (SP). pp. 374–391. IEEE (2018)
21. Walshe, T., Simpson, A.: An empirical study of bug bounty programs. In: 2020 IEEE 2nd International Workshop on Intelligent Bug Fixing (IBF). pp. 35–44 (2020)
22. Zhao, M., Grossklags, J., Liu, P.: An empirical study of web vulnerability discovery ecosystems. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. p. 1105–1117. CCS '15, Association for Computing Machinery, New York, NY, USA (2015). https://doi.org/10.1145/2810103.2813704
23. Zhao, M., Laszka, A., Grossklags, J.: Devising effective policies for bug-bounty platforms and security vulnerability discovery. Journal of Information Policy **7**, 372–418 (2017)