Bug Bounty Programs: Hunters' vs Organizations' Perspectives

Noura Alomar[1] Primal Wijesekera[1,2] Serge Egelman[1,2] Edward Qiu[1]
Amit Elazari[1]
[1]*University of California (Berkeley),* [2]*International Computer Science Institute*

Abstract

Software vulnerabilities continue to exist despite tremendous advances in static and dynamic vulnerability detection techniques. Many organizations have resorted to creating bug bounty programs to encourage security researchers to responsibly disclose software vulnerabilities. However, there are two questions that are yet to be answered by the research community: (1) when should an organization consider creating a bug bounty program? and (2) what are the factors that impact hackers' decisions of whether to participate in a bug bounty program or not? To answer these questions, we conducted semi-structured interviews with security managers at a diverse set of organizations and bug bounty hunters in a number of countries. Our hope is to spur further discussion in this domain and provide organizations with a framework that can be utilized in their vulnerability detection and remediation plans.

1 Introduction

Bug bounty programs allow organizations to utilize the capabilities of the crowdsourcing in searching for security vulnerabilities in their production systems. This approach is believed to attract security researchers to find new vulnerabilities in exchange for monetary or reputational rewards. Organizations, on the other hand, are getting beyond in-house security testing to identify vulnerabilities that were not identified by their internal security teams or other security testing such as pentesting and red teaming. In this project, we sought to gain an improved understanding of the challenges and concerns surrounding the bug bounty ecosystem by combining the perspectives of bug bounty hunters and security managers at organizations. We conducted semi-structured interviews with bug bounty hunters and security managers working for a diverse set of organizations to understand the reasons that drive organizations to create bug bounty programs, identify the factors that affect how bug bounty hunters select what program to participate in, and highlight potential areas for improvement.

2 Preliminary Results

Our results suggest that security researchers are attracted to bounty programs that have wider scopes and offer reasonable bounty amounts. Having good reputation in the hackers' community and being responsive to hackers when triaging vulnerability reports are also considered critical factors. Additionally, security researchers might be attracted to participate in a program if they wanted to apply for a full-time position at the organization sponsoring the program. Our results also suggest that recently released programs are likely to attract more attention by security researchers, as the systems included in such programs are perceived to have more vulnerabilities compared to mature bug bounty programs. Providing documentation describing how software features are supposed to work is also a factor that could motivate bug bounty hunters to spend some time looking for vulnerabilities in target systems.

From organizations' perspectives, we noted that they have concerns regarding not having visibility into who is researching their systems, and this motivated some organizations to have private bug bounty programs, where they invite a set of highly ranked researchers to search for vulnerabilities in their systems. For public bug bounty programs, some participants highlighted the fact that it is sometimes difficult to follow up with researchers and get more information about the vulnerabilities they reported.

Participants with prior experience managing bug bounty programs mentioned that running a program should never replace internal security testing, and starting such a program needs a certain maturity level for internal vulnerability management processes. Without a proper vulnerability patching mechanism, and clear communication lines between internal security teams and bug hunters, it could easily overwhelm the internal security teams. Thus, a matured internal security apparatus is a mandatory prerequisite for having a successful bug bounty program.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2019.
August 11–13, 2019, Santa Clara, CA, USA.