Bug Bounty Hunter, Red Teamer, or Pen tester? A Closer Look at the Roles of Security Teams in Vulnerability Discovery

Noura Alomar
University of California, Berkeley
nnalomar@berkeley.edu

Edward Qiu
University of California, Berkeley
edwardqiu@berkeley.edu

Primal Wijesekera
University of California, Berkeley
International Computer Science Institute
primal@berkeley.edu

Amit Elazari
University of California, Berkeley
amit.elazari@berkeley.edu

Serge Egelman
University of California, Berkeley
International Computer Science Institute
egelman@cs.berkeley.edu

Abstract

Detecting the presence of security vulnerabilities has been a challenge for organizations over the years. Some development mistakes (e.g., misconfigured system) and other security lapses have caused breaches ranging from leaking sensitive data to national security threats. These incidents have caused significant financial and reputational damages to these companies. These security breaches are prevalent despite the array of different vulnerability discovery processes deployed in these companies. We believe the ecosystem surrounding vulnerability discovery and its processes need to be adequately studied to understand current pitfalls, strengths, and more importantly, avenues where it can be improved to avoid future security breaches. To this end, we have conducted a series of semi-structured interviews with 53 security professionals to understand these processes, how different roles contribute to the common goal of securing the environment, the expectations surrounding different vulnerability discovery processes and, more importantly, the hurdles security professionals face in the course of vulnerability discovery. The paper reports the findings from these interviews, and our findings include challenges in organizations culture, constraints in trust between security professionals and companies, funding, and how to streamline different security vulnerability strategies and processes.

Author Keywords
Software Vulnerability, Vulnerability Discovery Process; Red teaming; Blue teaming; Purple teaming; Bug Bounty Program; Penetration Testing.

Introduction
Vulnerability discovery has become a diverse process and an ecosystem by itself. There are a lot of different teams and strategies involved in finding security vulnerabilities, such as red teams, pen testers, and bug hunters. The tools being used in these processes have advanced in automatic detection of software vulnerabilities. Yet, software security vulnerabilities remain vastly prevalent. We believe, as a research community, we need to study this ecosystem in order to identify the areas that could be further improved. In recent years, the research community has seen several research efforts that explored the factors that lead software developers to write insecure code [7, 1], studied the usability of security APIs and frameworks [5], and researched how security can be incorporated in organizations' cultures. Other lines of work focused on studying the economics of penetration testing teams, bug bounty programs, and the differences between white-hats' and penetration testers' strategies towards vulnerability discovery [8, 6, 3]. However, the security industry has also witnessed the development of offensive and defensive security testing strategies that are yet to be examined in the academic literature. Red teaming, blue teaming, purple teaming, pen testing, and bug bounty hunting are only a few examples of security roles and strategies being deployed by companies. In this research project, we take the first step towards bridging the gap that currently exists between academia and industry on the holistic understanding of the ecosystem of vulnerability discovery by interviewing 53 security professionals from across the spectrum of the ecosystem. We focused our investigation on the cultural, managerial, and technical factors that could contribute to making vulnerability discovery or remediation processes more effective. We found that factors like trust, staffing, and budget are leading organizational cultural factors that might hinder how security professionals act. Having multiple different security strategies have led to the issue of expectational conflict due to a lack of understanding of the pros and cons of different strategies. This in turn has led organizations that lack sufficient expertise to implement suboptimal strategies that could have adverse effects on the overall security of organizations' technical infrastructures.

Methodology
In April, May and June 2019, we recruited security professionals from across the spectrum using social media. We conducted interviews with 53 security professionals, holding managerial or technical security testing positions in the industry. Our sample included blue teamers, red teamers, purple teamers, bug bounty hunters, penetration testers, and CISOs. Our semi-structured interviews included questions about participants' testing processes, tools they find useful for vulnerability discovery, vulnerability remediation processes, challenges they face in their day-to-day work and lessons they learned from their experiences holding technical or managerial security positions. As a token of appreciation for the participants, we offered a lottery drawing for five $100 Amazon gift cards. The project has been approved by the Institutional Review Board (IRB) at the University of California, Berkeley. After collecting the required dataset, three research scientists independently coded the interviews and analyzed the collected data by looking at common themes that emerged in our interviews.

Results
The analysis uncovered a few themes across different roles in the vulnerability discovery process. In this section, we

summarize the main themes that emerged in our discussions with the study participants.

Bug Bounty Hunters

One of the most publicized strategies in vulnerability discovery is bug bounty programs. Organizations ranging from small e-commerce websites to federal agencies like the Pentagon are using bug bounty programs to uncover security flaws in their systems. Literature has looked into bug bounty programs from a process perspective and an economic perspective [2, 3, 4], but we wanted to understand how bug bounty programs fit into the whole ecosystem, as well as the hurdles and opportunities for improvement identified by participants.

Trust is a significant concern among bug hunters. Many participants mentioned the concerns that they have to report specific bugs in fear of reprisal from companies in the form of legal battles. With organizations moving towards defining scope based on various factors like data sensitivity and threat modeling, bug hunters are likely to find bugs out-of-scope while searching for vulnerabilities in target systems. Yet, bug hunters do not often feel safe reporting discovered vulnerabilities to corresponding organizations for fear of reprisal. Safe harbor programs are specifically addressing this problem, but it seems that they have a long way to go.

> *"And in terms of testing I learned that anonymity is important for me because in Germany we have few, I would say, anti-hacker laws so you are not allowed to use certain hacker tools. Yeah, you have to hide in the beginning."* (P14)

Trust is also eroding from a managerial perspective as well, more and more companies are moving towards using private bug bounty programs where companies can hand-pick who will be part of the process rather than open to the public. This trend makes the difference between bug bounty programs and external pen-testing fragile and pushes it into a grey area.

> *"You know, some companies have even come up with a hybrid approach where they have like invitation only bug bounties. I think that is a great idea to at least have some visibility into who is testing your applications and what they might be capable of, without exposing it to the general public."* (P25)

From an economic perspective, bug bounty programs are biased towards companies offering the largest financial rewards. Bug hunters who are likely to work on less financially lucrative bounty programs are ones who are learning the trade. Hence, such programs might not get the best eyes working on their systems. Highly ranked bug hunters have fewer incentives to work on less financially rewarding programs. This leaves the question of whether every company listed on a bug bounty platform gets the same benefit. Also, what is the solution?

> *"Really low pay outs. Crappy pay out tables, I do not want to spend my time on such programs. I think like a small scope with a good pay out table still interests me but if you have a really small scope and also really bad like reward tables, like low bounty amounts then I would not really be interested in looking."* (P27)

While there is literature on bug hunting processes, one of the questions we wanted to analyze was what is the right

time to start a bug bounty program? When should an organization consider creating a bug bounty program? Participants who had worked with bug bounty programs were in agreement that before going to a bug bounty program, a company should possess a mature vulnerability management process, and an effective channel of communication between bug hunters and the company. Participants with prior experience said bug bounty programs can easily overwhelm internal teams with many reports. Therefore, unless the company is prepared to deal with vulnerability reports promptly, it would not be in a position to make use of the benefits of bug bounty programs.

> *"I have seen organizations that have made the mistake of thinking that a bug bounty program would solve their security issues. And it is really easy to get overwhelmed and not be able to address those vulnerabilities in a timely fashion as they come in."* (P13)

Too many cooks spoil the soup?
When we look at vulnerability discovery holistically, a few different strategies and roles are working for the common goal of securing the production environment. Few of the stable patterns we observed are that many strategies and roles have led to an identity crisis among different roles as to be uncertain about how each role is different and how each role should be contributing to having effective vulnerability discovery processes. Moreover, importantly, there is also not a clearly defined way to utilize the multiple vulnerability discovery strategies. When we asked one of the participants who had more than 10 years of experience in the industry how he would define red teaming and penetration testing, he mentioned:

> *"..so just from my experience from the communities that I have been involved in, and the people that I have worked with I would make no distinction between those two terms."* (P12)

One of the main observations we had is that there is a common confusion on how red teaming is different from penetration testing. In some instances, participants considered themselves red teamers; however, when we asked them to describe their role more specifically and talk about their objectives, tools, and approaches to vulnerability discovery, we realized that the type of work they do is essentially penetration testing.

Having multiple teams working towards the same goal means, they have to collaborate and work together, but that appears to be another problematic situation. The communication seems to be a bottleneck in such a situation. Communication issues come in two broad categories: (1) communication between different teams in security such as between red teams and blue teams; (2) communication between testers (hackers) and management when they communicate found bugs to the higher ups to get their attention.

Most of the participants who had experience working with red and blue teams admitted that there is a disconnect between blue and red teamers. From the perspective of red teamers, they noted that blue teams sometimes see red teams as a threat to them, which defies the objective of having these teams work collaboratively to defend themselves against the adversary and might contribute to introducing knowledge gaps between these teams. When we asked blue teamers about their perspectives on this common problem, one commented:

> *“..that is sometimes down to the attitude of the*

red team. There are so many stereotypes for red teams that they are a bit cavalier, a bit cowboy-esque. Maybe bigger egos and more to prove than the blue teams, which doesn't help...both thinking of it as a competition between the red team and the blue team, when really it shouldn't be. It should be a learning experience for both sides." (P6)

Conclusion

In this project, we conducted an empirical investigation of the factors that could influence vulnerability discovery processes in organizational settings. Our ultimate goal is to establish a framework that could help organizations make informed decisions on what teams to hire while taking into consideration their resources, technical capabilities, and attack surfaces. To the best of our knowledge, we are taking the first step to investigate this problem holistically. We present our preliminary results and hope that our findings will spur further research efforts on how to develop effective techniques that could help identify and fix software vulnerabilities promptly.

REFERENCES

1. Hala Assal and Sonia Chiasson. 2018. Motivations and Amotivations for Software Security. In *SOUPS Workshop on Security Information Workers (WSIW)*.
2. Lorenz Breindenbach, Phil Daian, Florian Tramèr, and Ari Juels. 2018. Enter the hydra: Towards principled bug bounties and exploit-resistant smart contracts. In *27th USENIX Security Symposium USENIX Security*. 1335–1352.
3. Matthew Finifter, Devdatta Akhawe, and David Wagner. 2013. An empirical study of vulnerability rewards programs. In *the 22nd USENIX Security Symposium*. 273–288.
4. Hideaki Hata, Mingyu Guo, and M Ali Babar. 2017. Understanding the heterogeneity of contributors in bug bounty programs. In *Proceedings of the 11th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement*. 223–228.
5. Daniela Seabra Oliveira, Tian Lin, Muhammad Sajidur Rahman, Rad Akefirad, Donovan Ellis, Eliany Perez, Rahul Bobhate, Lois A DeLong, Justin Cappos, and Yuriy Brun. 2018. API Blindspots: Why Experienced Developers Write Vulnerable Code. In *Fourteenth Symposium on Usable Privacy and Security*. 315–328.
6. Daniel Votipka, Rock Stevens, Elissa Redmiles, Jeremy Hu, and Michelle Mazurek. 2018. Hackers vs. testers: A comparison of software vulnerability discovery processes. In *IEEE Symposium on Security and Privacy (SP)*. 374–391.
7. Chamila Wijayarathna and Nalin Asanka Gamagedara Arachchilage. 2018. Am I Responsible for End-User's Security? A Programmer's Perspective. (2018).
8. Mingyi Zhao, Jens Grossklags, and Peng Liu. 2015. An empirical study of web vulnerability discovery ecosystems. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 1105–1117.