ART001: What you need to know about bug bounties

Introduction

Bug bounties have gained significant attention in the cybersecurity community as a means to enhance security by crowdsourcing vulnerability discovery. However, there are several misconceptions surrounding bug bounties that need to be addressed. In this article, we will delve into the truth behind bug bounties, dispelling myths and providing a comprehensive understanding of their nature and purpose.

Bug bounties ≠ Hunting Bugs

Contrary to the name, bug bounties are not solely focused on hunting bugs. Instead, they are about securing applications and helping companies improve their security measures. Bug bounty hunters aim to identify vulnerabilities within target systems, but their role extends beyond bug hunting. They provide a unique perspective by adding their spin to the existing security coverage, ensuring comprehensive protection.

Bug bounties ≠ Pentesting

Bug bounty hunters should not be confused with pentesters. While pentesters are typically the first to assess a target, bug bounty hunters often come into the picture much later. They cannot approach the task in the same manner as a pentester, as they must think creatively and adapt to the specific circumstances. Bug bounty hunters have a distinct role in complementing pentests and vulnerability scans, contributing their expertise to uncover potential vulnerabilities that may have been missed.

Bug bounties ≠ A Reliable Way of Earning Money

Bug bounties may appear lucrative, but they are not a guaranteed or consistent source of income. Even the most skilled hunters may face delays in receiving payouts, irrespective of their ability to consistently discover bugs and expedite triage processes. Therefore, it is crucial for aspiring bug bounty hunters to test their skills while maintaining a stable job before considering a full-time bug hunting career. The financial aspect requires a long-term perspective, as monthly earnings may fluctuate, and earnings may be lower compared to a traditional full-time job.

Bug bounties ≠ Exploiting Researchers

Bug bounty programs are a privilege, not a right. Hunters must recognize that they are hacking live targets with the company's consent and trust. It is an opportunity to test and showcase their skills against real-world applications while getting rewarded for securing them. Companies do not owe hunters anything beyond the agreed-upon bounties. Understanding the collaborative nature of bug bounties is crucial to maintain a positive relationship between researchers and organizations.

Conclusion

Bug bounties play a significant role in the cybersecurity landscape, fostering collaboration between organizations and independent researchers to bolster system security. It is essential to dispel common misconceptions surrounding bug bounties to promote a better understanding of their purpose and expectations. By recognizing that bug bounties are not solely about hunting bugs, not equivalent to traditional pentesting, not a reliable source of income, and not an exploitative practice, aspiring bug bounty hunters can approach their endeavors with a realistic mindset.