Justin Lassalle

November 13, 2024

CYSE 201S

Journal

Bug Bounty Programs and Their Impact on Cybersecurity

From the bug bounty article, I learned about the economic viability of these programs, the impact of company characteristics, industry disparities, and the importance of longevity and engagement. Bug bounties are crucial for economic viability because they offer companies a cost-effective way to enhance their cybersecurity posture. Many ethical hackers are motivated by factors beyond just financial compensation; they often seek reputation and personal growth. As a result, smaller companies can attract skilled hackers without needing to offer the highest bounties. Regarding company characteristics, it appears that factors such as company revenue and brand recognition do not significantly influence the number of vulnerability reports received. This means that larger companies may draw more attention from ethical hackers simply because of their size. The article also highlights industry disparities, revealing that companies in finance, retail, and healthcare tend to receive fewer valid vulnerability reports compared to other industries. This may be because hackers perceive greater risks in these sectors, which raises questions about how ethical hackers can be encouraged to engage in reporting. The longevity and engagement of bug bounty programs are vital. Older programs often experience a decline in the number of reports over time. This decline can occur because as programs age, they may need to adapt their scopes to maintain hacker engagement. After reading this article, I have a better understanding of bug bounty policies related to cybersecurity.