By compensating ethical hackers for identifying and reporting vulnerabilities, bug bounty programs are a clever method for businesses to improve their cybersecurity. According to the literature assessment in the article, these initiatives are founded on the straightforward economic principle that rewarding a hacker is less expensive than dealing with the consequences of a significant breach. However, money isn't the only factor. Since businesses are essentially encouraging outsiders to tinker with their systems, trust is also crucial. The authors emphasize both the advantages and the difficulties in their findings. These initiatives have the potential to be very effective, but there are obstacles to overcome, such as ensuring that hackers receive appropriate compensation, navigating legal ambiguities, and determining what truly encourages participation. It can be challenging since some hackers sincerely want to assist, while others are more interested in the payoff. Overall, the paper demonstrates that, with good planning and management, bug bounty programs may be quite successful. Although they are not a one-size-fits-all solution, they may be very helpful in maintaining the security of systems when rules, trust, and communication are properly balanced.