EC-COUNCIL UNIVERSITY
ACCREDITED. FLEXIBLE. ONLINE.

BUG BOUNTIES VS. DARK WEB MARKETS: ARE COMPANIES FUELING THE HACKER ECONOMY?

AMMAR MOHAMED GHONAIM

EC-COUNCIL UNIVERSITY

ECCU 501-1: Ethical Hacking and Countermeasures

Dr. Warren Mack

September 5, 2025

TABLE OF CONTENTS

Abstract

This study analyzes the economic and ethical dimensions of vulnerability discovery through a comparative assessment of corporate bug bounty programs and underground exploit markets. This study examines whether companies, by offering bug bounty incentives, are unintentionally promoting the hacker economy or reducing it by directing hackers towards ethical disclosure practices. Utilizing secondary data and literature, such as industry reports and academic studies, the project demonstrates that bug bounty programs have experienced significant growth, disbursing millions in rewards and involving thousands of hackers (Bugcrowd, 2024; HackerOne, n.d.). Simultaneously, dark web markets and exploit brokers provide substantially greater financial rewards for exclusive zero-day exploits (Zetter, 2015; ZERODIUM, n.d.), thereby appealing to a distinct group of hackers. The analysis indicates a complex relationship: bug bounties enhance the professionalism of vulnerability discovery and diminish certain criminal incentives; however, substantial financial rewards in the black market persist in enticing individuals towards high-value exploits. The report examines the implications for policy and industry, concluding with recommendations aimed at enhancing ethical disclosure frameworks, aligning incentives, and ensuring that corporate practices support cybersecurity while avoiding unintended contributions to illicit exploit trade.

Keywords: bug bounty programs, zero-day exploits, vulnerability markets, ethical disclosure, cybercrime economy

Introduction & Background

Cybersecurity vulnerabilities are progressively regarded as commodities within a digital underground economy. The 2025 Verizon Data Breach Investigations Report indicates that approximately 20% of breaches were due to vulnerability exploitation, reflecting a 34% increase from the previous year (Verizon, 2025). This highlights the significant demand for exploits among threat actors and prompts inquiries regarding the acquisition and regulation of vulnerability supply.

Two distinct markets have emerged on the supply side: the legitimate bug bounty ecosystem and the illicit trade of exploits conducted on the dark web and through private brokers. This study examines whether corporate bug bounty programs, which incentivize hackers to report vulnerabilities, are unintentionally contributing to the expansion of the hacker economy or assisting in its regulation. Do these programs promote increased hacking activity through monetization, potentially leading to criminal markets, or do they redirect hackers from illegal actions by offering a legitimate alternative?

Bug bounty programs are initiatives wherein organizations solicit and compensate independent security researchers, commonly referred to as "ethical hackers," to identify and report vulnerabilities. Initially confined to a select number of technology firms, these programs have now expanded significantly across various industries and government entities (Segal, 2016). Platforms such as HackerOne and Bugcrowd enable these transactions, establishing a legitimate marketplace for vulnerabilities. As of 2024, companies collectively disbursed tens of millions of dollars in bounties and rectified thousands of security vulnerabilities through these programs (Bugcrowd, 2024; HackerOne, n.d.). The bounty model promotes disclosure rather than exploitation by offering financial rewards and recognition to hackers who enhance security.

Concurrently, a parallel underground exploit market continues to flourish. In the underground market, hackers trade zero-day exploits, previously unknown and unpatched vulnerabilities, to criminals or nation-state purchasers at elevated prices. Investigations and leaks indicate that exclusive exploits can command six- or seven-figure amounts, contingent upon their severity and target (Zetter, 2015; Segal, 2016). In contrast to bug bounty transactions that result in patches, these illicit sales necessitate the confidentiality of the vulnerability for offensive use. This underground market presents a significant risk, as the vulnerabilities traded are not communicated to vendors and consequently remain unaddressed.

The role of companies is crucial in these two markets. Funding bug bounties enables companies to financially support the hacker community, potentially incentivizing a greater number of individuals to engage in bug hunting activities. Conversely, they may be redirecting potential black-hat hackers towards legitimate employment, thus diminishing the availability of exploits for malicious purposes. This report examines the extent to which bug bounty programs impact the malicious hacker economy. This document outlines the research background and objectives, reviews current literature, conducts a comparative analysis of the two markets, and provides recommendations for optimizing incentive structures to improve cybersecurity.

Problem Statement

This analysis focuses on the potential interaction between corporate bug bounty programs and underground exploit markets. This inquiry examines whether bug bounty programs inadvertently encourage the hacker economy by normalizing and financially incentivizing vulnerability hunting, potentially leading some researchers to pursue greater rewards in dark web markets. Conversely, do they mitigate illicit activity by providing a legal alternative? The study investigates whether companies, by implementing bounty incentives, are inadvertently contributing to the hacker economy they aim to combat.

This issue is grounded in a conflict between economic and ethical considerations. Bug bounties assign a monetary value to vulnerabilities to promote responsible disclosure practices. Monetizing hacking skills may contribute to the normalization of a marketplace mentality, potentially leading to the illicit trading of exploits. A researcher who discovers a significant bug must decide between accepting a legal bug bounty reward or pursuing a potentially greater payment through illicit avenues. A bug valued at $10,000 in a corporate bug bounty may command a significantly higher price in the underground market, prompting researchers to consider the legal compensation against potential illegal gains. The issue is intensified in the context of high-stakes, high-skill exploits, such as zero-day vulnerabilities in widely utilized software, where the financial rewards in the underground market can be substantial. Some critics contend that companies prioritizing bug bounties may inadequately invest in secure development or timely patching, depending on external hackers to identify issues. This may unintentionally generate additional opportunities for hackers, effectively outsourcing security and potentially fostering an ongoing search for vulnerabilities (Zhou & Hui, 2020).

Thus, the problem statement can be articulated as follows: to examine whether bug bounty programs serve as a double-edged sword that both enhances software security and inadvertently perpetuates a marketplace that encourages the discovery and potential exploitation of vulnerabilities. This research seeks to clarify the circumstances in which bug bounties either support or hinder overarching security objectives. This entails an analysis of payout disparities, hacker motivations, and market dynamics distinguishing the “white” market (responsible disclosure) from the “black” market (illicit sales). This study aims to determine if modifications are necessary in the structuring of bug bounty programs by companies or in the regulation of vulnerability markets by policymakers.

Objectives of the Project

The project aims to achieve several specific objectives in response to the problem statement. This analysis aims to compare economic incentives by examining the financial rewards provided by bug bounty programs in relation to those available in dark web exploit markets. This involves analyzing standard payout ranges, the frequency of rewards, and the exclusivity of payments. For instance, a researcher may obtain several smaller rewards through legitimate programs, while a single substantial illegal transaction could yield a significantly higher yet more hazardous return.

The second objective is to evaluate the influence of bug bounty programs on hacker behavior by examining their decision-making processes. The primary inquiry concerns

whether ethical hackers adhere to legal channels due to bounty rewards or if the substantial prices in the black market still entice certain individuals to engage in the illegal sale of exploits. This study aims to analyze the trade-off decision from the perspective of a hacker (Zhou & Hui, 2020).

The third objective is to analyze vulnerability disclosure frameworks, focusing on the significance of ethical and policy standards, including responsible disclosure guidelines and international standards such as ISO/IEC 29147. The objective is to assess the extent to which these frameworks effectively mitigate the risks linked to exploit monetization (ISO/IEC, 2018).

The fourth objective involves analyzing trends and gaps in the literature through a thematic review. This entails the identification of patterns, including the growth rate of bug bounty findings, the evolution of exploit pricing in underground markets (Allodi, 2017; Dellago et al., 2022), and the gaps present in existing research. The study examines whether existing research indicates a correlation between increased bug bounty rewards and a reduction in black market activity, or if the relationship remains ambiguous.

The fifth and final objective is to offer recommendations derived from the findings. The recommendations are designed for various stakeholders. The objective for policymakers is to identify incentive structures or regulations that may promote responsible disclosure (Segal, 2016) and diminish the attractiveness of illicit exploit trading. The objective for industry is to propose optimal practices that enhance the security advantages of bug bounty programs, including reward structures and safe harbor provisions, while reducing any unintended adverse impacts on hacker motivation. The project aims to identify areas for further research and action within the cybersecurity community, including the enhancement of platforms for vulnerability exchange and the promotion of stronger ethical standards among hackers.

The outlined objectives offer a systematic framework for tackling the research question. The study develops a comprehensive view by comparing incentives and behaviors, examining governance structures, and reviewing current knowledge. The primary objective is to convert this understanding into practical insights that guarantee bug bounty programs and associated policies effectively improve cybersecurity without unintentionally compromising it.

Literature Review

Bug Bounty Growth and Benefits

Bug bounty programs have undergone significant expansion over the last ten years. Early adopters such as Netscape in 1995, followed by Mozilla and Google, illustrated the concept; however, it was during the 2010s and 2020s that bug bounties gained widespread acceptance. The emergence of hacker-powered security has established it as a distinct industry, exemplified by platforms like HackerOne, which has over one million registered hackers and supports programs for numerous organizations (HackerOne, n.d.). Reports indicate that by 2023-2024, companies are expanding the number of bounty programs and increasing reward sizes to attract top talent (Bugcrowd, 2024). Bugcrowd's Priority One report indicates that the government sector experienced a 151% increase in reported vulnerabilities and a 58% rise in critical (P1) findings following the expansion of bounty programs. Additionally, leading industries such as finance provided median payouts of $10,000 for critical bugs. This suggests a correlation between higher bounties and increased engagement, as well as the identification of high-severity discoveries, with researchers tending to focus on areas offering substantial rewards.

Research indicates that bug bounties can enhance security outcomes for vendors. Gal-Or et al. (2024) demonstrate through game-theoretic models that vendors engaged in bug bounty programs can expedite software updates and initially release products with a higher number of vulnerabilities, relying on the bounty community to identify these issues after release (Gal-Or et al., 2024). This finding, which may initially seem counterintuitive, suggests that a firm may choose to ship a product with "known unknown" bugs. This decision is justified by the presence of a bug bounty program, which serves as a safety net to identify and rectify these bugs prior to exploitation by malicious actors. The study indicates that the optimal number of hackers participating in a bug bounty is determined exclusively by the anticipated number of malicious attackers. The quantity of optimal ethical hackers consistently falls short of the anticipated number of malicious hackers, and this quantity increases in correlation with the rise in the expected number of malicious hackers. Furthermore, increased bounty awards have been demonstrated to enhance the effort exerted by hackers, consequently elevating the probability that ethical hackers will identify critical vulnerabilities prior to their exploitation by malicious actors.

Additional research investigates the motivations and behaviors of individuals involved in bug bounty programs. Wachs (2022) highlights the significance of platforms in shaping this market. Platforms decrease transaction costs through the standardization of vulnerability reporting and payment processes, thereby enhancing trust among participants. Reputational systems, such as hacker rankings and reward metrics, are implemented to promote good-faith interactions. This platform-mediated approach

mitigates information asymmetries that have historically impeded vulnerability markets; for instance, researchers are concerned about the reliability of vendors in honoring rewards, while vendors are apprehensive about the potential for duplicate reports or extortion. Platforms such as HackerOne function as reliable intermediaries, enabling smaller companies to implement bug bounty programs and allowing less-experienced researchers to engage in these initiatives (Wachs, 2022). Bug bounty platforms have formalized the practice of vulnerability hunting, establishing a labor market characterized by distinct norms and career trajectories. A significant number of elite hackers now engage in bounty hunting as either a full-time or substantial part-time occupation, achieving earnings comparable to those in software development positions. In 2020, HackerOne reported that certain individuals earned more than $300,000 annually through bounties, and the platform surpassed $100 million in total hacker payouts by that time (HackerOne, n.d.).

Zhou and Hui (2020) characterize bug bounty engagement as "sleeping with the enemy," offering a thought-provoking perspective. The economic analysis indicates that firms obtain two primary advantages from a bug bounty program: attack diversion, where hackers who might otherwise exploit a vulnerability are incentivized to report it for a reward, and protection delegation, wherein the firm outsources a portion of its security testing to the crowd (Zhou & Hui, 2020). They warn that a bug bounty program may result in a firm diminishing certain internal security measures, which could pose risks if not adequately managed (Zhou & Hui, 2020). They discuss the significance of legal safe harbor in bounty programs. Numerous bounty policies currently incorporate provisions that guarantee the non-pursuit of legal action against hackers who comply with the program regulations (ISO/IEC, 2018). Zhou and Hui (2020) demonstrate that a firm may not have the motivation to reduce the legal risks associated with third-party security testing by incorporating robust safe harbor provisions, even when it gains advantages from hackers' assistance, unless influenced by external pressures or policy modifications.

The literature highlights several advantages of bug bounties: They utilize a diverse pool of external talent, often uncovering more and varied bugs compared to traditional assessments; they offer economic efficiency by compensating only for results rather than full-time salaries; and they may decrease the exposure window by identifying vulnerabilities prior to exploitation by malicious actors. Successful programs are defined by equitable rewards, explicit legal terms, and an extensive scope that allows hackers to test any areas not specifically prohibited. According to Bugcrowd (2024), open-scope programs yield a greater number of serious vulnerabilities compared to restrictive programs. The growth trajectory of bug bounties indicates widespread acceptance; what was previously a novel experiment has now become a standard practice in cybersecurity management.

Economics of Underground Exploit Markets

In contrast to the collaborative nature of bug bounties, underground exploit markets function covertly, motivated by substantial incentives for malicious activities. These markets encompass dark web forums and private brokers where researchers may sell zero-day exploits to the highest bidder. The prices within this underground economy frequently exceed those of bug bounty rewards significantly. Empirical studies indicate that leading exploits command prices comparable to or exceeding those in the legitimate market. Allodi (2017) examined a prominent Russian cybercrime forum and discovered that numerous exploits were sold for prices that matched or exceeded the bounties offered by vendors. A critical vulnerability that may yield approximately $20,000 via a company's bug bounty could potentially command several times that amount on the black market if it is widely exploitable (Allodi, 2017). The author noted a distinct correlation between exploit sales and real-world attacks, suggesting that when a vulnerability is actively traded, it subsequently manifests in criminal campaigns (Allodi, 2017). This demonstrates that a dynamic exploit trade directly contributes to malicious hacking activities.

Dellago et al. (2022) enhance understanding by monitoring advertised prices from exploit brokers. Their analysis indicates that exceptionally rare exploits, such as a remote jailbreak for the latest iPhone iOS, can yield payouts in the seven-figure range (ZERODIUM, n.d.). Brokers frequently disclose substantial bounties to entice researchers, while actual agreements are negotiated privately (Dellago et al., 2022). The Hacking Team case exemplifies the challenges and costs associated with acquiring zero-day vulnerabilities, even with substantial financial incentives. Many hackers prefer to sell exclusively to governments or established brokers, resulting in Hacking Team securing only a limited number of exploits over several years, despite operating with six-figure budgets (Zetter, 2015).

Numerous reported statistics highlight the profitability of this market. Estimates indicate that mid-tier exploits, such as those targeting moderately popular software or enabling local privilege escalations, are valued between a few thousand and tens of thousands of dollars. In contrast, high-value zero-day vulnerabilities, which affect widely used and secure software, are priced from the low six figures to approximately $1 million or more (Segal, 2016; Zetter, 2015). Zerodium's announcements in 2017 indicated a reward of up to $1.5 million for specific smartphone exploits (ZERODIUM, n.d.). The numbers have increased as more sophisticated buyers, particularly state actors, elevate demand. Mandiant reported that in 2023, approximately 70% of vulnerabilities exploited in the wild were zero-days that were unknown to the vendor at that time (Mandiant, 2023). This underscores the significant dependence of advanced attackers on newly available exploits provided by the underground market.

Not all cybercriminals require zero-day exploits; numerous breaches arise from stolen credentials or existing vulnerabilities. Initial access broker (IAB) markets are available for the acquisition of compromised access to networks (European Union Agency for Law Enforcement Cooperation, 2023). As companies enhance fundamental security measures and address known vulnerabilities, the significance of genuine zero-day exploits increases. The Verizon (2025) report indicates a growing trend among attackers to utilize zero-day exploits targeting perimeter devices, such as VPNs and firewalls, in recent breaches. When straightforward options are unavailable, complex strategies emerge as the preferred method.

From both ethical and legal perspectives, the sale of exploits to criminals or hostile entities presents considerable risks. Researchers pursuing this approach may encounter legal repercussions and harm to their reputation if discovered. Certain exploit brokers function within a legal gray area by asserting that their sales are limited to governments or vetted clients; however, this practice results in vulnerabilities remaining undisclosed to the impacted software vendors (Segal, 2016). The presence of a robust gray market indicates that there will always be suppliers willing to meet the demand for advantages, provided there are individuals prepared to pay for them. This parallel economy of exploits encourages skilled hackers to retain critical vulnerabilities, thereby hindering public benefit. Despite legal and ethical concerns, a segment of individuals remains attracted to these lucrative sales.

The underground exploit market is characterized by its high profitability and offensive focus. A researcher possessing a novel vulnerability may achieve significantly greater financial gain through a clandestine sale compared to a public bug bounty, thereby encouraging a persistent inclination away from responsible disclosure. Organizations and defenders possess restricted insight into this domain owing to its clandestine nature. The subsequent section on ethical frameworks will examine the responses of the cybersecurity community and policymakers to this challenge, focusing on their efforts to reshape incentives and norms.

Ethical and Policy Frameworks

Policymakers and industry groups have acknowledged the necessity of adjusting incentives in favor of defense. Instead of prohibiting the sale of vulnerabilities, an approach that is difficult to enforce and may hinder research, experts advocate for the establishment of positive incentives for disclosure (Segal, 2016). Governments have initiated their own bug bounty programs and have expanded legal protections for researchers. The U.S. Department of Defense's "Hack the Pentagon" initiative, along with comparable efforts, indicates a governmental recognition of the importance of ethical hacking. Legal safe harbor provisions, including clarifications to anti-hacking

laws, are increasingly employed to safeguard good-faith security research (ISO/IEC, 2018; Segal, 2016). These measures facilitate a safer and more straightforward process for hackers to report vulnerabilities instead of exploiting them.

It has been proposed that if governments and companies decline to acquire exploits or commit to disclosing the majority of their findings, such as through a Vulnerability Equities Process, the black market could be diminished (Segal, 2016). International norms are addressed, including proposals for agreements that mandate the disclosure of identified vulnerabilities in critical infrastructure rather than their stockpiling. Although a global treaty is absent, these discussions indicate an increasing agreement that unregulated zero-day trading presents a shared risk.

In the hacker community, robust ethical norms contribute to self-regulation. Numerous researchers firmly oppose selling to cybercriminals, considering responsible disclosure to be the appropriate course of action. The sale of products to government entities remains a contentious issue, as some researchers express concerns regarding the potential offensive use of such exploits. The 2015 Hacking Team scandal, characterized by the exposure of internal emails from an Italian firm indicating the sale of exploits to authoritarian regimes, served as a significant alert. The incident elicited significant criticism from the security community and highlighted the potential reputational harm associated with participation in the clandestine exploit trade (Zetter, 2015). The combination of community pressure and professional recognition for ethical conduct effectively deters many hackers from violating moral boundaries.

In conclusion, current frameworks and policies are designed to incentivize responsible behavior while increasing the consequences of unethical actions. Coordinated Vulnerability Disclosure practices, as detailed in standards such as ISO/IEC 29147, along with well-defined bounty programs, enhance the incentive for ethical hacking. Additionally, clear safe harbor policies mitigate legal concerns for participants. Simultaneously, law enforcement agencies persist in their efforts to address criminal markets, while policy discussions focus on mitigating institutional demand for undisclosed exploits. The underground economy cannot be eradicated immediately; however, there is a trend towards increased transparency and collaboration, utilizing incentives and social norms to mitigate the appeal of the dark web market.

Methodology

This project utilized publicly accessible data and research. All analyses were performed using secondary sources, without direct involvement in underground forums or illicit activities. Primary data sources comprised established industry reports, including HackerOne Hacktivity statistics, Bugcrowd's Priority One report, ENISA's Threat Landscape 2023, Verizon's 2025 DBIR SMB snapshot, and Europol's IOCTA 2023, alongside scholarly publications and preprints such as Allodi (2017), Zhou and Hui (2020), Dellago et al. (2022), Wachs (2022), and Gal-Or et al. (2024). The sources offered quantitative metrics, including the number of reported vulnerabilities, payout ranges, and the prevalence of zero-day exploits in breaches, alongside qualitative insights, such as economic models and policy recommendations.

Thematic analysis was employed to synthesize information from these sources. Common themes, including the economics of bug bounties, pricing in exploit markets, hacker motivations, and policy responses, were identified and utilized to organize the literature review and results. Key points were validated through the cross-referencing of multiple sources. Claims regarding exploit prices from media reports were verified against academic findings, and statistics from industry reports, such as HackerOne's total payouts or Verizon's breach data, were corroborated with additional reports or public databases when accessible.

The methodology is constrained by the quality and transparency of publicly available data. The exploit economy of the dark web is characterized by its inherent opacity; thus, this research depended on case studies, leaks, and expert observations for insights. Companies frequently engage in selective reporting of bug bounty outcomes. To address bias, the study conducted a comparative analysis of information from various reports and utilized peer-reviewed findings to either support or contest industry narratives. Notwithstanding these limitations, reliance on legal and reputable sources guarantees that the analysis remains within ethical parameters and accurately represents the current state of knowledge. The findings represent a composite picture derived from the most reliable evidence available in the public domain.

Results

This study's findings reveal significant contrasts and nuanced relationships between bug bounty programs and dark web exploit markets. Results are organized into three sub-sections: (a) comparative findings on payouts and market dynamics, (b) analysis of hacker incentives and behavior, and (c) observed trends in vulnerability disclosure practices.

(a) Comparative Findings on Payouts and Market Dynamics: A key observation is the notable difference in potential rewards between the bug bounty market and the underground market for advanced exploits. Table 1 presents various examples:

Table 1

Comparison of Bug Bounty Rewards and Black Market Prices for Vulnerabilities

Vulnerability Category	Approx. Bug Bounty Reward (Legal)	Approx. Black Market Price (Illicit)
Minor web vulnerability (e.g., XSS)	$100-$500 (typical bounty)	Negligible (little to no black market demand)
Critical web/app bug (e.g., SQLi, RCE)	$1,000-$5,000 (high bounty range)	$10,000+ (if sold illicitly, varies)
Browser/OS zero-day (remote RCE)	Up to $50,000 - $100,000 (top programs)	$100,000-$500,000 (via exploit brokers)
Elite 0-day (e.g., iOS full chain)	Up to $1,000,000+ (rare vendor bounties)	$1,000,000+ (private gray-market buyers)

Note: Bug bounty figures are based on public program disclosures (Bugcrowd, 2024; HackerOne, n.d.), while black market prices are drawn from reported examples and broker announcements (Zetter, 2015; ZERODIUM, n.d.; Segal, 2016). Actual prices vary with exploit rarity, demand, and exclusivity.

The table indicates that for low-severity issues, such as a simple XSS, rewards are typically offered only by bug bounty programs, as criminals generally do not compensate for such minor vulnerabilities. For more critical vulnerabilities, bug bounties may provide compensation in the thousands of dollars; however, underground purchasers can offer significantly higher amounts. For example, a significant web

application vulnerability may yield a researcher $5,000 from a company, whereas a skilled cybercriminal could pay tens of thousands for an undisclosed exploit. A sophisticated full-chain exploit for a secure platform, such as an iOS remote jailbreak, could yield a bounty of up to seven figures from vendors like Apple. Additionally, brokers have proposed similar or higher amounts for exclusive rights (Zetter, 2015; ZERODIUM, n.d.).

(b) Analysis of Hacker Incentives and Behavior: The data indicates a complex understanding of hacker motivations.

Numerous hackers engage in bug bounties for motivations that extend beyond financial gain, including the enhancement of reputation, the pursuit of intellectual challenges, and a desire for altruism in securing systems. For these individuals, the availability of a legal pathway, along with the inherent benefits of recognition (such as being featured on a company's Hall of Fame or earning reputation points on a platform), is sufficient to maintain their adherence to ethical standards. Wachs (2022) observes that public disclosure and leaderboards serve as non-monetary incentives that promote positive behavior. Seeing one's name credited on HackerOne's Hacktivity page or receiving recognition from the community serves as a significant motivator (HackerOne, n.d.).

Evidence suggests that increased bug bounty rewards attract certain talent that may otherwise engage in the sale of exploits. Zhou and Hui (2020) characterize "coopetitive" hackers, who can act as either allies or adversaries, and contend that an effective bounty program effectively incentivizes these hackers to align with the cooperative side by rendering collaboration financially advantageous (Zhou & Hui, 2020). Verizon's 2025 report indirectly supports this assertion by emphasizing the importance of timely patching and noting the rapid exploitation of new vulnerabilities by attackers. This underscores the necessity for researchers to report bugs promptly. Bounties provide a crucial incentive; in their absence, numerous vulnerabilities may go unreported until they are exploited for malicious purposes.

However, some exploits possess such significant value that the temptation persists. An anecdote from the 2015 Wired article on Hacking Team referenced an iOS exploit valued at $500,000 in the zero-day market. It is challenging for any individual to overlook such an amount. Unconfirmed reports indicate that some researchers employ a dual strategy: they responsibly disclose numerous vulnerabilities through bounty programs, thereby establishing their reputation and securing a consistent income. However, in the case of discovering an exceptionally profitable vulnerability, they may opt to discreetly sell it to a broker. The justification is that a single substantial sale can provide financial stability for an extended period. Although evidence for this is limited, the market logic renders it plausible.

The risk factor serves as a substantial disincentive for the illegal sale of exploits. Engaging with a broker such as Zerodium exists within a legal gray area, as the sale of exploits is not explicitly prohibited in certain jurisdictions. In contrast, direct sales to criminal organizations on the dark web are unequivocally illegal. Europol's IOCTA 2023 reports successful dismantling of marketplaces, emphasizing that individuals attempting to engage in illicit profit are at risk of apprehension. This context encourages numerous hackers to adhere to legal boundaries.

Bug bounty hunting is characterized by its demanding nature and competitive landscape. Community discussions indicate that researchers do not consistently receive bounties; this process necessitates significant skill, persistence, and occasionally luck, with numerous reports ultimately being duplicates or rejected. The appeal of a guaranteed payout from a broker, contingent upon the delivery of a functioning exploit, may often outweigh the investment of time in identifying a bug that may have already been discovered by another individual. The structure of bounty programs is significant; those that are perceived as equitable, with transparent guidelines and timely payments, contribute to maintaining hacker engagement and reducing the likelihood of disillusionment or a shift towards unethical practices.

(c) Observed trends in vulnerability disclosure practices: Organizations and governmental entities are progressively modifying their practices to recognize the hacker economy and direct it towards beneficial outcomes.

An increasing number of organizations are implementing vulnerability disclosure policies, even in the absence of rewards, thereby providing hackers with formal avenues to report issues without apprehension. According to ENISA (2023), an increasing number of EU entities have established formal vulnerability disclosure processes (EUROPEAN UNION AGENCY FOR CYBERSECURITY et al., 2023). The presence of a Vulnerability Disclosure Policy (VDP) facilitates ethical engagement and indicates that the organization is receptive to contributions from security researchers.

Many companies are experiencing improvements in their time-to-patch; however, the time-to-exploit for attackers is advancing at a quicker pace (Mandiant, 2023). In 2023, the average interval between the disclosure of a vulnerability and its exploitation in attacks was merely 5 days (Mandiant, 2023). This creates an imperative for vendors to respond and implement patches without delay. Certain companies have begun to implement "quick fix" bonuses in their bug bounty programs for vulnerabilities that are addressed within a brief timeframe. This strategy aims to minimize the exploitation window once a vulnerability is identified.

Governments are increasingly assuming a leadership role in disclosure initiatives. The

United States employs a Vulnerability Equities Process (VEP) to ascertain which zero-day vulnerabilities its agencies will disclose to vendors and which will be retained for operational use; it is widely believed that many vulnerabilities are disclosed through this mechanism (Segal, 2016). Transferring additional vulnerabilities to vendors for patching diminishes the number of undisclosed flaws that may be traded on the black market.

Law enforcement is actively intervening in the cybercrime economy. Operations aimed at dark web forums and marketplaces introduce uncertainty for both exploit sellers and buyers (European Union Agency for Law Enforcement Cooperation, 2023). Over time, this increases the risk and diminishes the potential profit of illicit exploit trading, serving as an additional deterrent to participation in the black market.

In conclusion, the results indicate that bug bounty programs have established a strong and beneficial avenue for hacker talent, offering financial rewards that are becoming increasingly competitive, although they typically remain lower than the potential earnings available in the black market for the most valuable exploits. A substantial amount of vulnerability research has likely been appropriated, which, a decade or two prior, may have remained unutilized or ultimately been incorporated into exploit kits. However, for a limited number of vulnerabilities, particularly those impacting the most secure and high-value systems, the underground demand and associated pricing continue to pose a challenge. This discussion analyzes the implications of these findings for ethical hackers, the cybersecurity sector, and policymakers, specifically evaluating whether companies are contributing to or mitigating the hacker economy.

Discussion

The emergence of bug bounties has formalized hacking as a profession, offering consistent income and public acknowledgment for individuals who identify vulnerabilities. This constructive avenue allows numerous skilled hackers to direct their efforts towards defense instead of criminal activities. The ethos of the community, supported by bounty platforms such as public leaderboards and disclosed report credits, promotes ethical hacking and skill development (HackerOne, n.d.; Wachs, 2022). This indicates that bug bounty programs are typically directing hacker talent towards productive activities and away from illegal opportunities.

Organizations in the industry derive substantial advantages from bug bounty programs; however, careful management is essential. Bug bounty programs serve as a cost-effective complement to security teams, identifying vulnerabilities that internal personnel may overlook. Companies must ensure that their bounty rewards are competitive with the incentives offered to attackers. If rewards are perceived as

insufficient or if reports are managed inadequately, researchers may experience frustration or, in exceptional instances, contemplate unethical alternatives. Organizations must persist in their investment in secure development practices and timely patching; bug bounty programs serve as a supplementary measure rather than a substitute for comprehensive internal security protocols. Firms that implement bounty programs featuring equitable payouts, transparent policies, and safe harbor protections are likely to mitigate the risk of vulnerabilities being exploited by unauthorized parties.

For policymakers and regulators: The findings indicate that supportive policies can enhance the advantages of bug bounties. It is essential for governments and regulators to establish frameworks that facilitate disclosure, such as providing legal safe harbors for compliant researchers, while refraining from implementing overly broad measures that could drive hacking activities underground (Segal, 2016). Policymakers can exemplify best practices by implementing government bug bounty programs and by publicly disclosing the majority of vulnerabilities identified through official channels. Simultaneously, it is essential to address the ongoing demand aspect by implementing restraint in government procurement practices and maintaining law enforcement pressure on illicit markets. In summary, policy should prioritize adjustments in the economic incentives related to defense: it should be made more accessible and beneficial to report vulnerabilities rather than to engage in their illicit sale.

The relationship between bug bounties and dark web markets is intricate, yet it trends positively towards enhanced security. Bug bounty programs have significantly altered the hacker economy by attracting numerous participants into legitimate activities and reducing opportunities for illicit trading. The most sophisticated exploits continue to pose a significant concern; therefore, organizations and governmental entities must enhance incentives and refine processes to effectively address this specialized area. However, it seems that companies are increasingly defending against the negative aspects of the hacker economy rather than contributing to it. This establishes a foundation for recommendations aimed at strengthening these gains.

Recommendations

Governments ought to establish incentives that promote disclosure rather than exploitation (Segal, 2016). For instance, broaden legal safe harbor protections to ensure that researchers adhering to coordinated disclosure guidelines (ISO/IEC, 2018) are exempt from prosecution. Instead of trying to prohibit the sale of zero-days, which presents enforcement challenges, regulators should concentrate on positive incentives. This includes funding bug bounty programs in essential sectors and government, as well as providing rewards or recognition for the disclosure of vulnerabilities (Segal, 2016). International cooperation is essential; policymakers should strive to establish norms or agreements that deter the accumulation of critical vulnerabilities and promote the exchange of security information across borders. Continued law enforcement efforts targeting illicit exploit marketplaces are essential for increasing the risks and decreasing the rewards associated with participation in the black market (European Union Agency for Law Enforcement Cooperation, 2023).

Organizations conducting bug bounty programs should enhance these initiatives to optimize security benefits. This involves providing competitive rewards that correspond to the actual impact of vulnerabilities; for example, offering higher bounties for critical issues to deter researchers from engaging with illicit buyers. Programs must be managed with professionalism, ensuring that reports are triaged and resolved promptly, accompanied by clear communication and appropriate acknowledgment of researchers. Legal and ethical commitments, including refraining from legal action against compliant hackers and publicly recognizing their contributions, enhance trust and encourage participation. Companies may collaborate within the industry by pooling resources to sponsor bounties for open-source projects or widely utilized libraries that may otherwise lack adequate support. Bug bounties should serve as a complement to, rather than a replacement for, internal security investments; organizations must maintain strong development security, consistent patching, and ongoing employee training. Utilizing bug bounty findings to enhance internal practices enables companies to systematically diminish the vulnerabilities that may be exploited by both ethical hackers and malicious actors.

Further research and community initiatives can strengthen the transition toward ethical hacking within the security community and academia. Continued academic analysis of vulnerability market dynamics is essential (Allodi, 2017; Dellago et al., 2022) to inform evidence-based policies. For example, it is important to quantify the impact of bug bounty proliferation on supply to underground markets. Educational programs ought to incorporate modules on ethical hacking and responsible disclosure to foster robust professional ethics among emerging security practitioners (Zhou & Hui, 2020). Technologists can create improved tools and platforms for secure disclosure, such as

systems that guarantee researchers receive credit or compensation upon the resolution of a flaw, thereby enhancing the process and fostering trust. Outreach programs can effectively engage emerging hackers by directing their skills towards bug bounties, thereby steering them away from cybercrime. These initiatives illustrate that legitimate hacking can yield both financial and professional benefits. Enhancing the ethical framework and knowledge base regarding vulnerability discovery can reduce the number of individuals motivated to engage in the negative aspects of the hacker economy.

Conclusion

Bug bounty programs and dark web markets exemplify contrasting aspects of the hacker economy: one is characterized by transparency and defensive measures, while the other is defined by secrecy and offensive activities. This research aimed to ascertain whether companies are unintentionally promoting the latter through bug bounty programs. The evidence indicates that companies have catalyzed a growing economy of hackers, with the net effect being the channeling of that energy towards positive outcomes rather than the empowerment of cybercriminals.

Bug bounties have established the perception that hacking can be a legitimate and constructive endeavor. The corporate sector allocates tens of millions of dollars each year to researchers (HackerOne, n.d.; Bugcrowd, 2024), demonstrating its commitment to identifying and rectifying vulnerabilities. This has attracted numerous proficient individuals to the field of ethical hacking.

The pool of talent available to the criminal market has likely diminished, thereby increasing the opportunity cost for hackers considering the sale of vulnerabilities in underground markets. In this context, companies are financing hackers, primarily for defensive purposes.

Nonetheless, the dark web and gray markets for exploits continue to exist, and in certain niches, they flourish. High-end zero-day exploits continue to be commodities characterized by strong demand and exorbitant prices (Zetter, 2015; ZERODIUM, n.d.). No individual bug bounty can rival the financial incentive provided by a spy agency or cybercrime syndicate for a significant, unpatched vulnerability. Consequently, a portion of the vulnerability market persists in functioning beyond the parameters of responsible disclosure. The increase in vulnerability research, driven by bounties and heightened information security awareness, has resulted in a greater number of zero-day vulnerabilities being discovered. Consequently, some of these vulnerabilities are likely to be exploited by malicious actors. Furthermore, if companies improperly manage their bounty programs or fail to adequately compensate researchers, they risk alienating the

individuals upon whom they depend, potentially driving them towards unethical alternatives.

The findings indicate that companies are more effectively mitigating the criminal aspects of the hacker economy than contributing to its exacerbation. Bug bounty programs offer a legal and organized framework for harnessing hacker talent, consequently diminishing the influx of vulnerabilities into illegal avenues. To strengthen this outcome, it is essential for companies and policymakers to align incentives with defense by increasing bounty rewards when suitable, ensuring prompt and equitable processing of reports, broadening safe harbor protections, and sustaining pressure on illicit markets. This approach can shift the dynamics of the hacker economy from clandestine activities to a focus on enhancing cybersecurity collectively.

References

Bibliography

Allodi, L. (2017). Economic factors of vulnerability, trade, and exploitation. Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, 1483-1499. *https://doi.org/10.1145/3133956.3133960*

Bugcrowd. (2024, March 5). Priority One Report | BugCrowd. Retrieved September 5, 2025, from *https://www.bugcrowd.com/resources/report/priority-one-report/*

Dellago, M., Woods, D. W., & Simpson, A. C. (2022). Characterizing 0-day exploit brokers. In University of Innsbruck, University of Edinburgh, & University of Oxford, University of Innsbruck, Austria; University of Edinburgh, UK; University of Oxford, UK. *https://weis2022.econinfosec.org/wp-content/uploads/sites/10/2022/06/weis22-dellago.pdf*

EUROPEAN UNION AGENCY FOR CYBERSECURITY, Ardagna, C., Corbiaux, S., Van Impe, K., & Ostadal, R. (2023). ENISA Threat Landscape 2023 (C. Ciobanu, Ed.).

European Union Agency for Law Enforcement Cooperation. (2023). Internet Organised Crime Threat Assessment (IOCTA) 2023. Publications Office of the European Union. *https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN.pdf*

Gal-Or, E., Hydari, M. Z., & Telang, R. (2024, April 26). Merchants of Vulnerabilities: How bug bounty programs benefit software vendors. arXiv.org. Retrieved September 5, 2025, from *https://arxiv.org/abs/2404.17497*

HackerOne. (n.d.). HackerOne. Retrieved September 5, 2025, from *https://hackerone.com/hacktivity/overview?queryString=disclosed%3A true&sort Field=latest_disclosable_activity_at&sort Direction=DESC&pageIndex=0*

ISO/IEC. (2018). ISO/IEC 29147:2018. *https://cdn.standards.iteh.ai/samples/72311/06fe3b1905aa4f3f8d9c5824ebc3c396/ISO-IEC-29147-2018.pdf*

Mandiant. (2023, April 18). M-Trends 2023: Cybersecurity Insights from the Frontlines | Mandiant. Google Cloud Blog. *https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2023*

Segal, A. (2016, September 19). Using incentives to shape the zero-day market. Council on Foreign Relations. *https://www.cfr.org/report/using-incentives-shape-zero-day-market*

Verizon. (2025). 2025 Data Breach Investigations Report: Small- and Medium-Sized Business Snapshot. *https://www.verizon.com/business/resources/infographics/2025-dbir-smb-snapshot.pdf*

Wachs, J. (2022, April 14). Making Markets for Information Security: The role of online platforms in bug bounty programs. arXiv.org. Retrieved September 5, 2025, from *https://arxiv.org/abs/2204.06905*

ZERODIUM. (n.d.). ZERODIUM [Press release]. *https://cyber-peace.org/wp-content/uploads/2017/09/ZERODIUM-How-to-Sell-Your-0day-Exploit-to-ZERODIUM.pdf*

Zetter, K. (2015, July 24). Hacking team Leak shows how secretive zero-day exploit sales work. WIRED. *https://www.wired.com/2015/07/hacking-team-leak-shows-secretive-zero-day-exploit-sales-work/*

Zhou, J., & Hui, K. (2020). Sleeping with the Enemy: An Economic and Security Analysis of Bug Bounty Programs. SSRN Electronic Journal. *https://doi.org/10.2139/ssrn.3940307*

Appendix

Appendix A: Reference Integration Mapping

This table maps each mandatory reference to the sections of the research paper where it was used, ensuring transparency of source integration.

Reference	Sections Used In
HackerOne (n.d.) Hacktivity Report	Introduction, Literature Review (bug bounty growth), Results, Discussion
Bugcrowd (2024) Priority One Report	Literature Review (payouts), Results (comparative findings), Recommendations
ENISA (2023) Threat Landscape Report	Methodology (data sources), Results (disclosure practices)
Verizon (2025) DBIR SMB Snapshot	Introduction (breach statistics), Results (attacker use of exploits), Discussion
Europol (2023) IOCTA	Literature Review (IAB markets), Results (law enforcement actions), Recommendations
Zerodium (n.d.). Exploit Acquisition Program	Literature Review (exploit pricing), Results (elite zero-day values)
Mandiant (2023) M-Trendst	Results (time-to-exploit gap), Discussion (industry implications)
ISO/IEC (2018) 29147	Objectives, Literature Review (ethical frameworks), Recommendations
Dellago et al. (2022) Exploit Brokers	Literature Review (pricing), Results (broker practices)
Zhou & Hui (2020) Sleeping with the Enemy	Problem Statement, Objectives, Literature Review (coopetition)

Reference	Sections Used In
Allodi (2017) Vulnerability Trade	Literature Review (pricing), Objectives (trends analysis), Results
Gal-Or et al. (2024) Merchants of Vulnerabilities	Literature Review (game theory vendor incentives), Discussion
Wachs (2022) Bug Bounty Platforms	Literature Review (platform trust/reputation), Results (hacker motivation)
Segal (2016) CFR Zero-Day Report	Literature Review (policy), Objectives (recommendations), Recommendations
Zetter (2015) Wired Hacking Team Leak	Literature Review (case evidence), Results (exploit values), Discussion

Appendix B: Extended Table - Bug Bounty vs. Black Market Incentives

Comparison of Typical Rewards in Bug Bounty Programs and Underground Markets

Vulnerability Type	Bug Bounty Reward Range	Undergroun Market Price Range	Primary Buyer Type
Cross-Site Scripting (XSS)	$100-$500	Negligible	Companies only
SQL Injection / Web RCE	$1,000 - $5,000	$10,000 - $50,000	Criminal groups
Browser Remote Code Execution	$25,000 - $100,000	$100,000 - $500,000	Brokers, state actors
iOS / Android Full Chain Zero-Day	$500,000 - $1,000,000+	$1,000,000+	Brokers, intelligence agencies

Note. *Bug bounty values are based on program reports (HackerOne, n.d.; Bugcrowd, 2024). Underground market values are derived from academic studies and investigative reports (Allodi, 2017; Dellago et al., 2022; Zetter, 2015; Zerodium, n.d.; Segal, 2016).*

List of Figures and Tables

Tables (Main Body)

Tables (Appendices)

Index Words

- Bug bounty programs
- Zero-day vulnerabilities
- Vulnerability disclosure
- Dark web markets
- Exploit brokers
- Ethical hacking
- Responsible disclosure
- Cybercrime economy
- Coordinated vulnerability disclosure (CVD)
- ISO/IEC 29147
- Underground exploit pricing
- Hacker incentives
- Cybersecurity policy
- Mandiant M-Trends
- Europol IOCTA
- Verizon DBIR
- ENISA Threat Landscape