

8th Edition–2024/2025

# Hacker-Powered Security Report



hackerone

# Content

## Table of Contents

---

➔	Executive Summary	— x	1
➔	The Impact of AI on Security Research and Vulnerability Management	— x	5
➔	Security Researchers Expand Their Expertise Into AI, APIs, and More	— x	14
➔	Run a Top-Tier Program That Won't Break the Bank	— x	18
➔	The Top Ten Vulnerabilities Need to Change	— x	29
	<ul style="list-style-type: none"><li>• Financial Services</li><li>• Government</li><li>• Telecoms</li><li>• Retail and E-commerce</li><li>• Transportation</li><li>• Media and Entertainment</li><li>• Computer Software</li><li>• Internet and Online Services</li><li>• Crypto and Blockchain</li><li>• Travel and Hospitality</li></ul>		

# Content

## Table of Contents, Cont. ....

➔ The Best Defense Has Layers of Depth	— x 55
➔ Measuring Success: Invest in Return on Mitigation	— x 60
➔ Conclusion	— x 63



## Executive Summary

# Cyberthreats are always evolving. So must your defenses. Faster, smarter, and always ahead.

Every organization is a technology organization. Car manufacturers, government agencies, and banks do very different things, but they all conduct business digitally. With AI deployments—as well as AI-powered threat actors—now mainstream, the digital threat landscape is growing and changing faster than ever.

Just a few years ago, organizations only had to worry about one OWASP Top 10 list. Now there are OWASP Top 10 lists for mobile security, LLMs and more. What's next? And how do you stay ahead of it all?

We've been watching these trends and reporting on them for over eight years now in the Hacker-Powered Security Report. Read on to learn about the impact of AI on security research, what the researchers themselves are thinking and seeing, industry trends, and more. We report on the top vulnerability types, and how the most resilient companies have adopted a defense-in-depth strategy, fortifying every layer of their security posture and using continuous vulnerability testing throughout the software development life cycle.

# From Compliance to Competitive Advantage

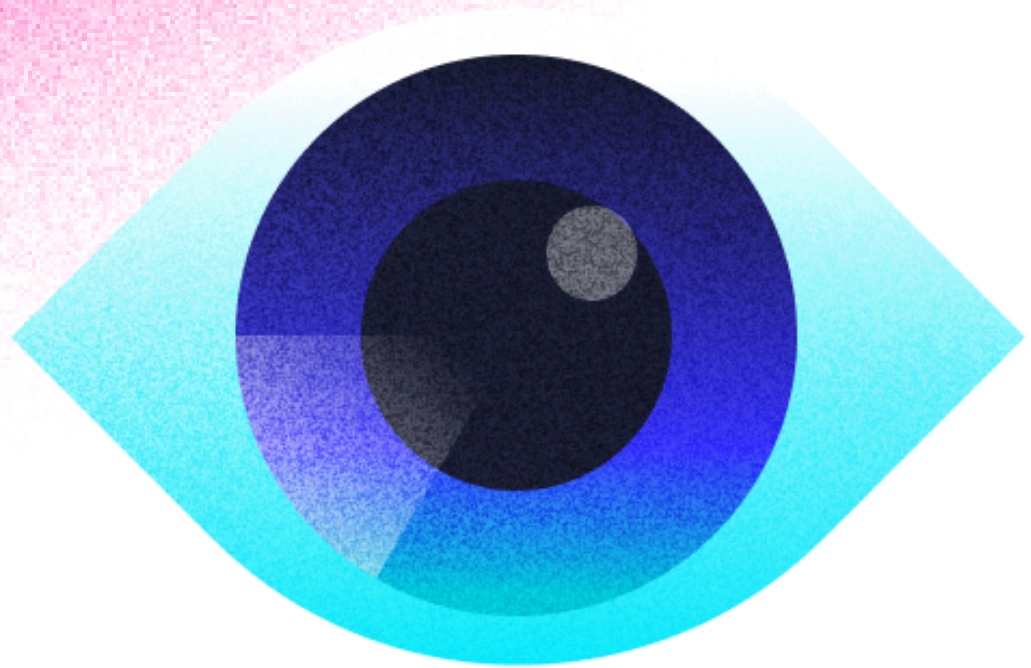
Human-powered, AI-enabled security testing remains vital in identifying vulnerabilities that automated scanners often miss, as the creativity and expertise of skilled researchers are unmatched by machines.

Since the first Hacker-Powered Security Report in 2017, the security researcher community has consistently been proven to keep pace with technological changes, deliver ongoing value, and gain the trust of even the most risk-averse organizations.

Over the past decade, we've seen significant progress for trust in good-faith research, including updated safe harbor guidelines from the Department of Justice, legislation requiring organizations to implement vulnerability reporting processes,<sup>1, 2</sup> and increasing adoption of vulnerability disclosure and bug bounty programs by leading enterprises. In fact, these programs are now cited in S1 filings as evidence of an organization's commitment to security.

<sup>1</sup> U.S. Department of Justice Office of Public Affairs. [Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act.](#)

<sup>2</sup> CyberScoop. [Vulnerability disclosure policies eyed for federal contractors in Senate bill.](#)



# About the Hacker-Powered Security Report

This 8th Annual Hacker-Powered Security Report compiles insights, data, and analysis from customers, security researchers, and HackerOne's comprehensive vulnerability database. The insights are gathered from:

- Aggregated, anonymized data from the HackerOne Platform, made up of over 500,000 valid vulnerability reports.
- A survey, conducted in partnership with Opinion Matters, of 500 security leaders globally about their approach to cybersecurity challenges.
- Our annual survey of 50 customers, representing a range of organizational sizes, structures, and industries.
- Our annual survey of 2,000+ highly skilled and active members of the security researcher community, covering topics ranging from the time they dedicate to hacking to their views on AI regulations. The respondents reflect the diversity of location, experience, expertise, and age that defines HackerOne's global community of security researchers.

*Each section is designed to provide useful insights, and includes recommendations for next steps based on these findings.*

# Key Findings from the Report

- Researchers and security professionals alike see AI as both a risk and an opportunity. 48% of security leaders said that generative AI (GenAI) was one of the most significant risks they saw impacting their organization, with data integrity being a key priority to secure.
- The security researcher community is maturing its skill sets to meet the demands of customers, with more members focusing on mobile, APIs, and AI deployments as testing scope expands to more varied attack surfaces. Nearly 10% of researchers now specialize in AI to meet the growing demand of AI testing engagements.
- The top vulnerability reported to a bug bounty program is cross-site scripting (XSS), whereas for a pentest it's misconfiguration. Pentests tend to uncover more systemic or architectural vulnerabilities while security researchers working on bug bounty programs focus more on real-world attack vectors, user-level issues, and business logic flaws.
- The most security-resilient organizations have refined their engagement with the researcher community to achieve the ideal formula for impactful results, focusing on a broad scope and a select team of trusted researchers. High-impact programs—those with over 30% of valid vulnerability submissions rated as high or critical—work with fewer researchers; the average number of researchers on a high-impact program is 56, vs. 97 on lower-impact programs.
- The most technologically advanced industries are seeing results when it comes to the efforts to reduce common vulnerabilities in production, with Web3 companies seeing 65% fewer reports for cross-site scripting than the industry average.

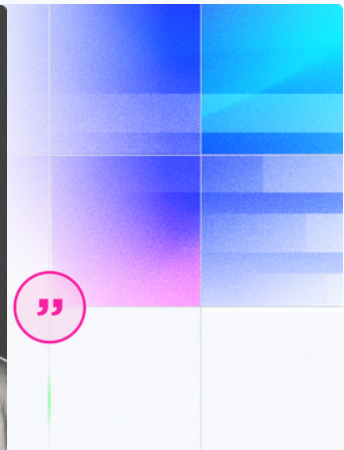
# The Impact of AI on Security Research and Vulnerability Management

Last year we introduced a dedicated AI section in the Hacker-Powered Security Report, recognizing the growing influence of GenAI on how organizations operate and plan ahead. This year we're digging deeper into both security for AI (how organizations manage risks in AI deployments) and AI for security (how researchers and organizations use AI to improve vulnerability management). We also highlight the crucial role human expertise plays in keeping AI innovation trustworthy and secure for everyone.

*"The downside of AI is that it introduces more vulnerabilities. If a company uses it, we'll find bugs in it. AI is even hacking other AI models. It's going so fast and security is struggling to catch up."*

**Jasmin Landry, @jr0ch17**

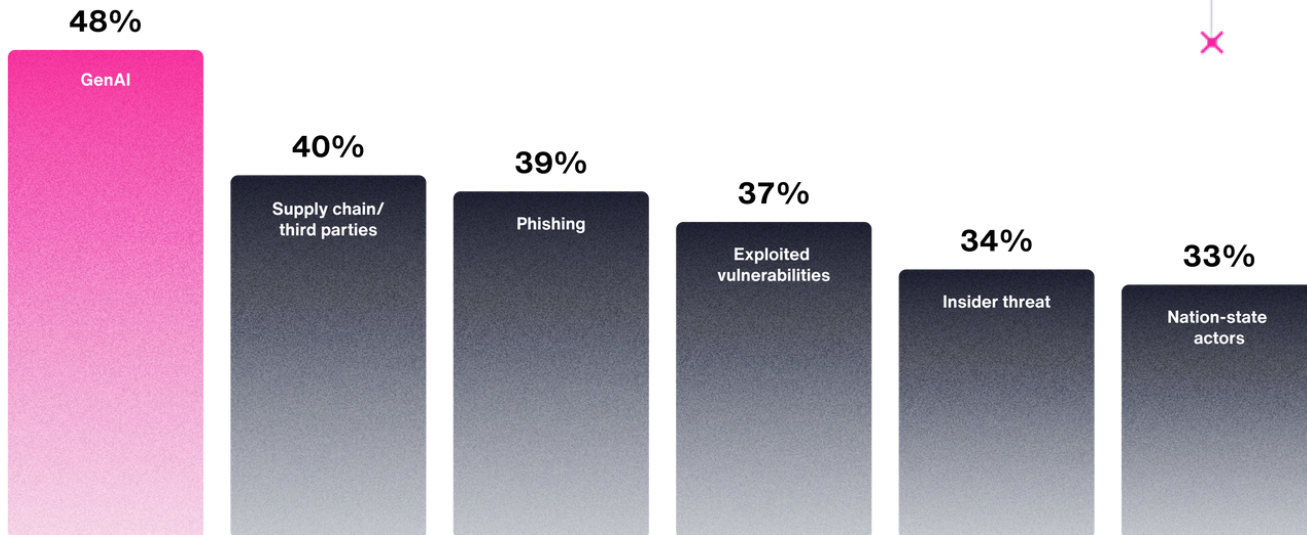
Security Researcher and HackerOne Pentester



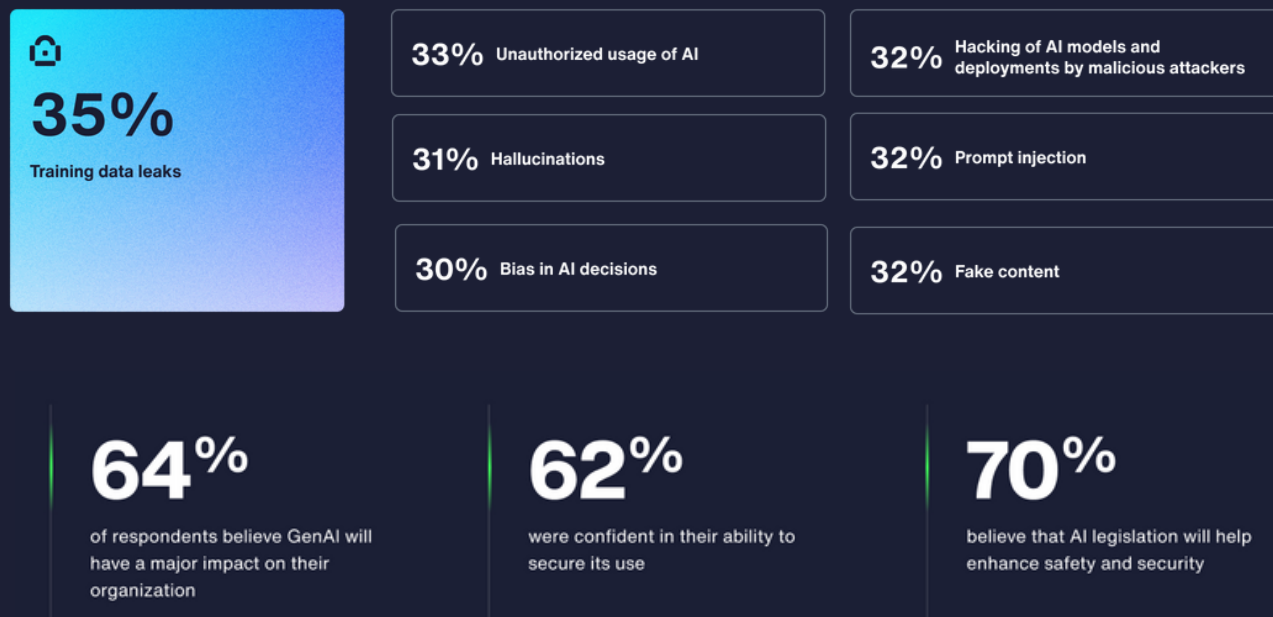
# Security for AI

We surveyed 500 security professionals to understand their experiences and opinions around AI adoption within their industries and organizations. Nearly half (48%) cited GenAI as one of the most significant risks facing their organizations. The top concerns included training-data leaks (35%), unauthorized AI usage within their organizations (33%), and the hacking of AI models by external parties (32%).

Which of the following  
IT-related risks are of most  
concern to your organization?



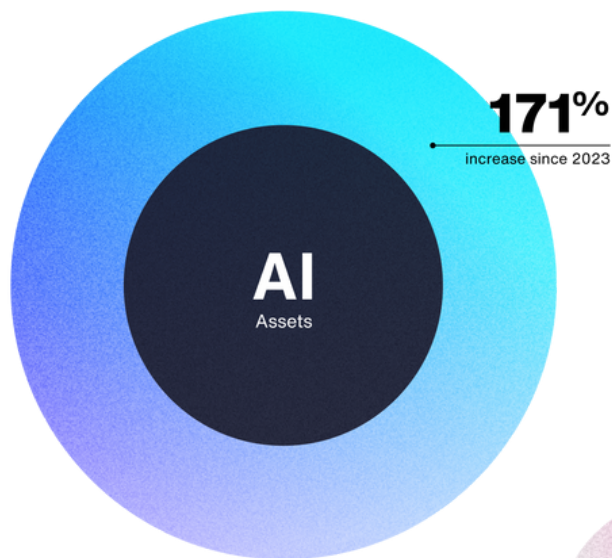
## Which of the following GenAI risks are of most concern to your organization?



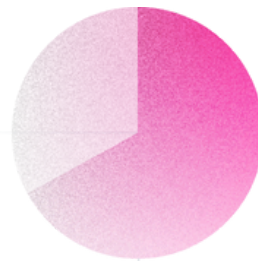
64% of respondents believe GenAI will have a major impact on their organization, with 62% confident in their ability to secure its use. Additionally, 70% believe that AI legislation will help enhance safety and security. However, 51% are concerned about the reputational risks tied to AI, and another 51% highlight that basic security practices are being overlooked in the rush to implement GenAI.

When we asked the same questions to a group of HackerOne customers, we found similar views on the impact of GenAI—64% agreed it would significantly affect their operations. However, only 38% felt confident in their ability to defend against AI-related threats, and just 39% believed that legislation would make AI safer.

As highly knowledgeable and technologically advanced organizations, HackerOne's customers have a deep understanding of the challenges involved in securing this rapidly evolving technology. Interestingly, they were less concerned about the reputational risks of AI than non-customers were, with 48% of customers expressing worry.



HackerOne customers are taking proactive steps to avoid AI-related security incidents. The number of AI assets included in HackerOne programs has surged by 171% over the past year and will soon surpass 1,000 assets.



67%

AI red teaming—where organizations invite security researchers to identify safety and security flaws in their AI products—is gaining traction as a best practice for testing GenAI deployments. **In fact, 67% of security leaders and HackerOne customers believe that an external, unbiased review of GenAI implementations is the most effective way to uncover AI safety and security issues.**

believe that an external, unbiased review of GenAI implementations is the most effective way to uncover AI safety and security issues

“

*“It’s been previously observed in research from red teaming exercises of AI models that some individuals are significantly more effective at breaking the models’ defenses than others. I was surprised that many of the researchers did not know much about AI but were able to use creativity and persistence to get around our safety filters.”*

**Ilana Arbisser**

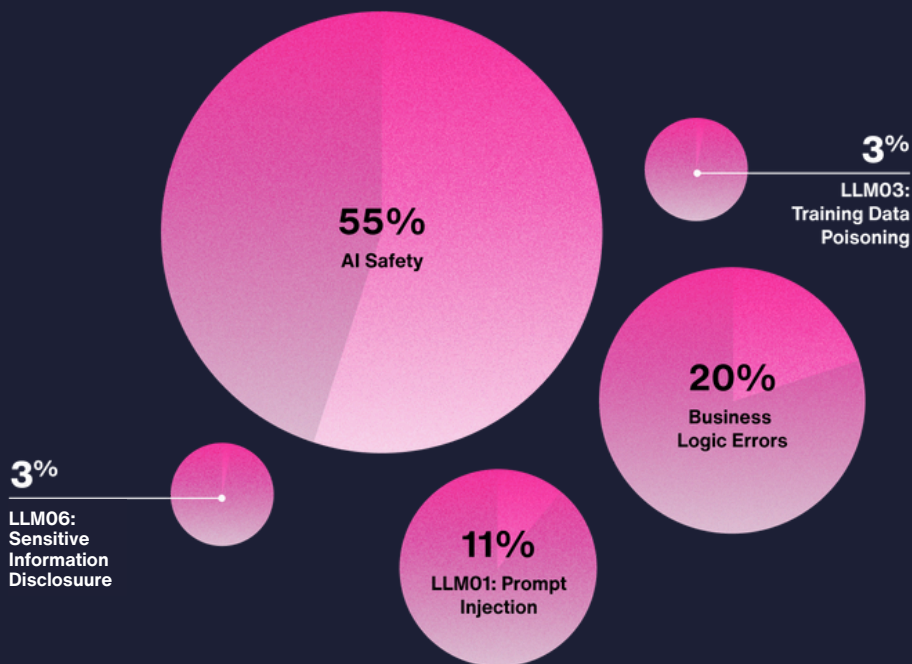
Technical Lead, AI Safety, Snap Inc.



*“When you’re performing prompt injection, you’re getting the system to behave in a way that the developers who built something with that API don’t want it to do. To anyone who thinks that prompt injection is just getting the model to say something it shouldn’t, I would say that my findings reveal that attackers can exfiltrate a victim’s entire chat history, files, and objects. There are significant vulnerabilities that can pop up as a result of prompt injection.”*

**Joseph Thacker, @rez0**  
Security Researcher Specializing in AI

## The 5 Most Commonly Reported Vulnerabilities on AI Programs



Concerns about AI safety are driving more organizations to seek third-party testing. Of all AI vulnerability reports submitted, 55% are related to AI safety issues. AI safety issues often have a lower barrier to entry for valid reporting and present a different risk profile compared to traditional security vulnerabilities. The reduced barriers to entry for AI safety reports means bounties for these reports are slightly lower, with an average payout of \$401, versus \$689 for AI security programs. While AI safety vulnerabilities are currently in scope for a limited number of programs, the volume of reports is notably higher, making AI safety one of the top five reported vulnerabilities.

# AI Safety vs. AI Security

What's the difference between AI safety and AI security?

## AI Safety

Focuses on preventing AI systems from generating harmful content, from instructions for creating weapons to offensive language and inappropriate imagery. It aims to ensure responsible use of AI and adherence to ethical standards.

## AI Security

Involves testing AI systems with the goal of preventing bad actors from abusing the AI to, for example, compromise the confidentiality, integrity, or availability of the systems the AI is embedded in.

## Recommendations

- ✓ Establish continuous testing, evaluation, verification, and validation throughout the AI model life cycle. Provide regular executive metrics and updates on AI model functionality, security, reliability, and robustness. Regularly scan and update the underlying infrastructure and software for vulnerabilities.
- ✓ Determine country-, state-, or government-specific AI compliance requirements. Some regulations exist around specific AI features, such as facial recognition and employment-related systems. Establish an AI governance framework outlining roles, responsibilities, and ethical considerations, including incident response planning and risk management.
- ✓ Train all users on ethics, responsibility, legal issues, AI security risks, and best practices such as warranty, license, and copyright. Establish a culture of open and transparent communication on the organization's use of predictive or generative AI.

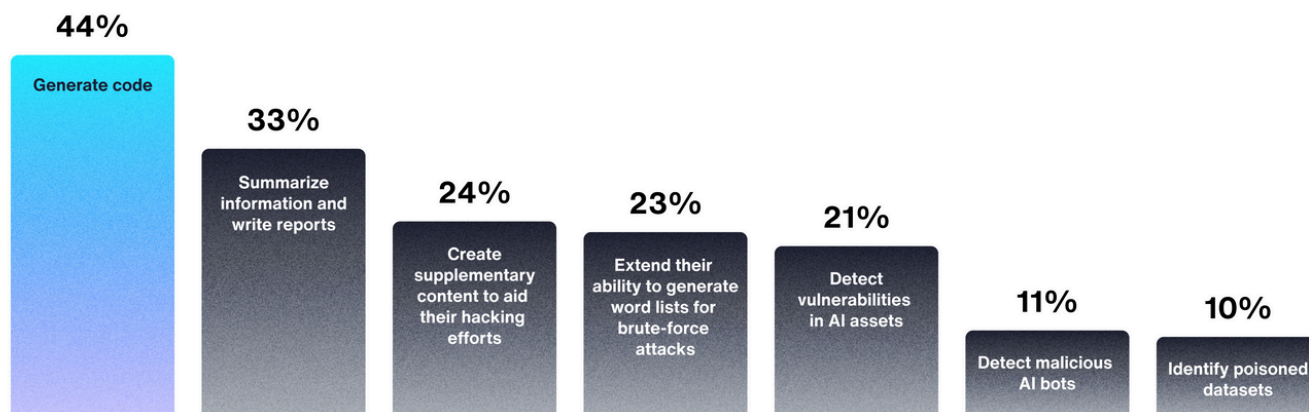
For a more detailed checklist for both safety and security testing engagements, download [The Ultimate Guide to Managing Ethical and Security Risks in AI](#).

# AI for Security

AI and automation are powerful efficiency tools, saving organizations an average of \$2.2 million per breach<sup>3</sup> by helping to detect and contain breaches faster, reducing overall impact. Companies without AI and automation face longer response times and higher breach costs.

In a survey of over 2,000 security researchers on the HackerOne Platform, 20% now see AI as an essential part of their work, up from 14% in 2023. However, only 38% reported using AI in any capacity, down from 53% last year, suggesting that researchers who find real value in AI are investing more deeply, while others may have pulled back after finding less success with initial experiments.

## Are you currently using, or do you plan to use, GenAI for any of the following purposes?



<sup>3</sup> IBM. [Cost of a Data Breach Report 2024](#).



*"I leverage AI-powered vulnerability scanners to quickly identify potential weak points in a system, allowing me to focus on more complex and nuanced aspects of security testing. I also use AI for reporting. Previously, I spent 30-40 minutes writing reports to ensure all details were included, the tone was appropriate, and there were no grammatical mistakes. AI has streamlined this process, reducing the time to an average of 7-10 minutes per report."*

“

**Hazem Elsayed, @hacktus**  
Security Researcher

*"When pentesting, I use AI to automate repetitive and time-consuming tasks so I can concentrate on finding security issues. I also use AI to summarize documentation when I want a general overview of a new technology. When I do content discovery before my pentest, AI allows me to generate customized wordlists to find niche content that can fly under the radar of commonly used wordlists."*

”

**Adam Deziri, @a\_d\_a\_m**  
Security Researcher

## Accelerate Vulnerability Remediation with Hai

33% of security researchers are using AI to summarize information and write reports. HackerOne customers can also use AI to streamline and enhance their vulnerability management process via the platform's GenAI copilot, Hai. Hai provides a deeper, more immediate understanding of incoming reports, enabling faster decision-making and quicker fixes.



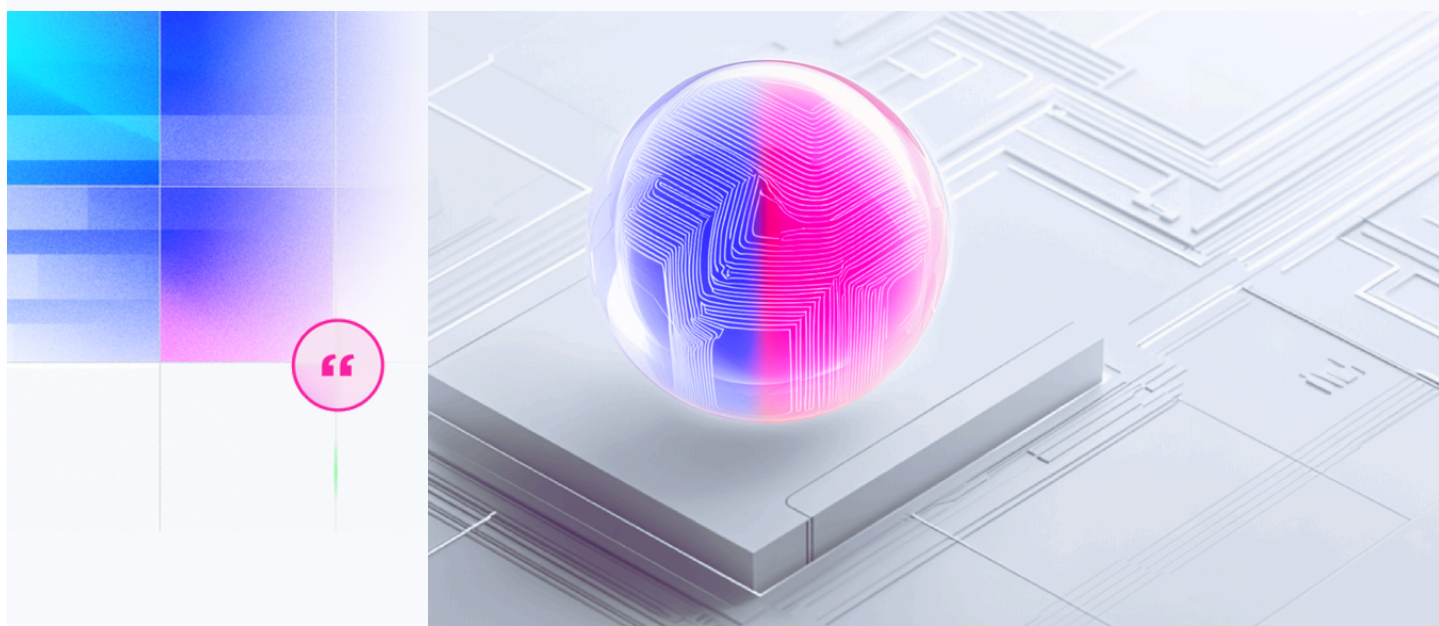
**HackerOne Hai**  
Reported a vulnerability

# 33%

of security researchers are  
using AI to summarize  
information and write reports

## Recommendations

- ✓ Use Hai's tailored advice to quickly interpret complex vulnerability reports with concise summaries and deeper insights for faster decision-making in the context of your unique technology stack and business needs.
- ✓ Use Hai to optimize vulnerability reports by having it suggest accurate titles, CVSS scores, and vulnerability classifications. Hai can also help you craft clear and succinct messages for effective communication between security, development teams, and researchers.
- ✓ Automate tasks by integrating Hai to assist with writing assistance, generating custom vulnerability scanner templates, and managing large reports, reducing manual effort.



*"Hai is a game-changer for our communication with researchers. Managing relationships and keeping messages clear and concise can be challenging, especially with high expectations from both researchers and managers. Short replies can be misunderstood, while longer responses are time-consuming. Hai helps us craft more precise and neutral messages, proofreads our communications, and maintains a consistent tone. This efficiency allows us to engage with more researchers and allocate time to other critical tasks."*

**Cybersecurity Consultant,**  
Enterprise, Financial Services

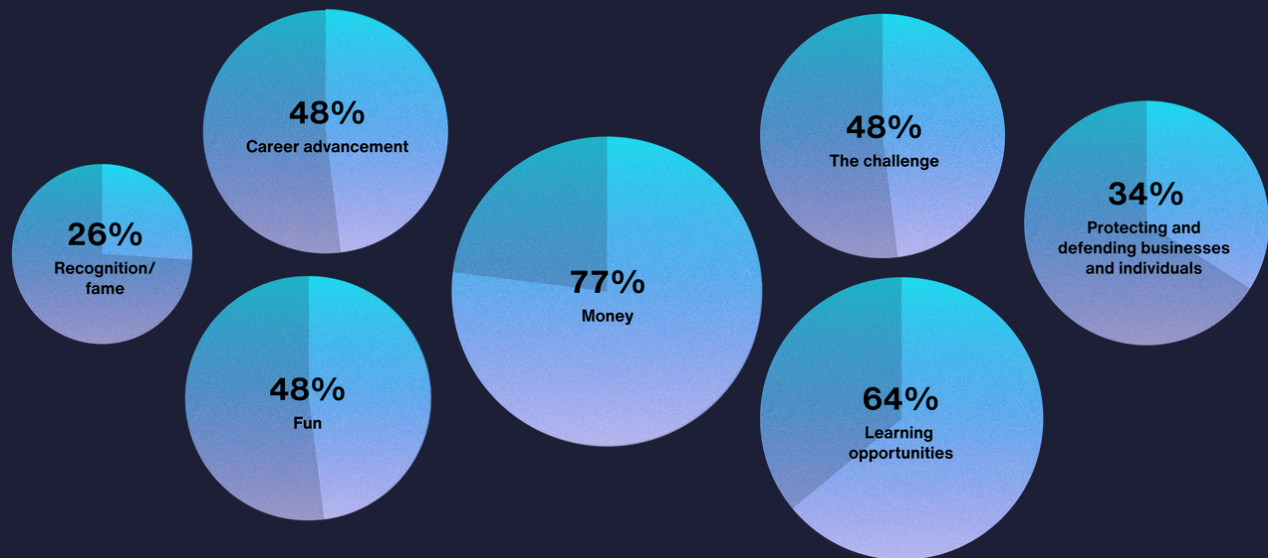


# Security Researchers Expand Their Expertise Into AI, APIs, and More

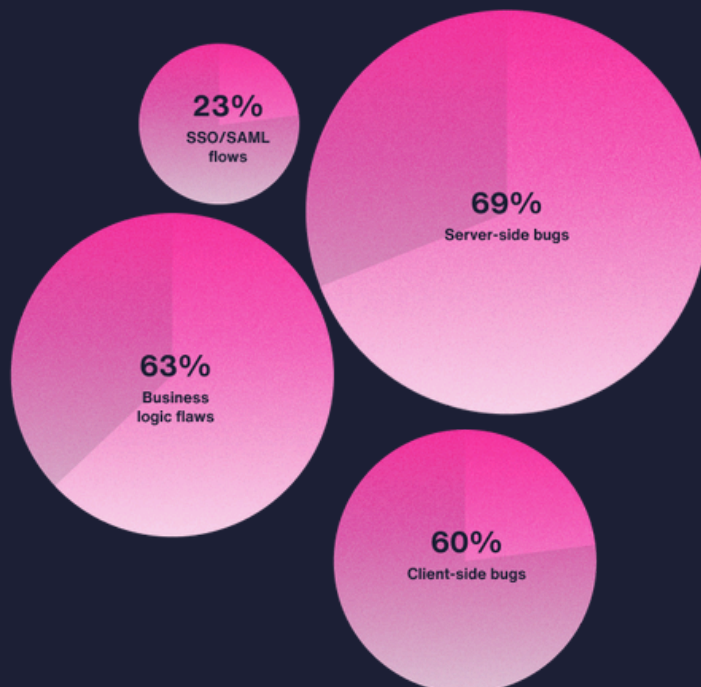
More of the security researcher community is choosing the flexibility of a full-time career as security researchers are dedicating more hours to developing their skills. 30% now hack full-time, up from 24% in 2023, and 44% spend over 20 hours a week hacking, compared to 35% the previous year.

While 77% of researchers cite earning money as a key motivator, 64% view hacking as a valuable way to learn and develop their skills, and 48% do it to advance their careers. Additionally, 34% are driven by a strong desire to protect businesses and end users, highlighting the community's commitment to making a positive impact.

# What motivates you to hack?

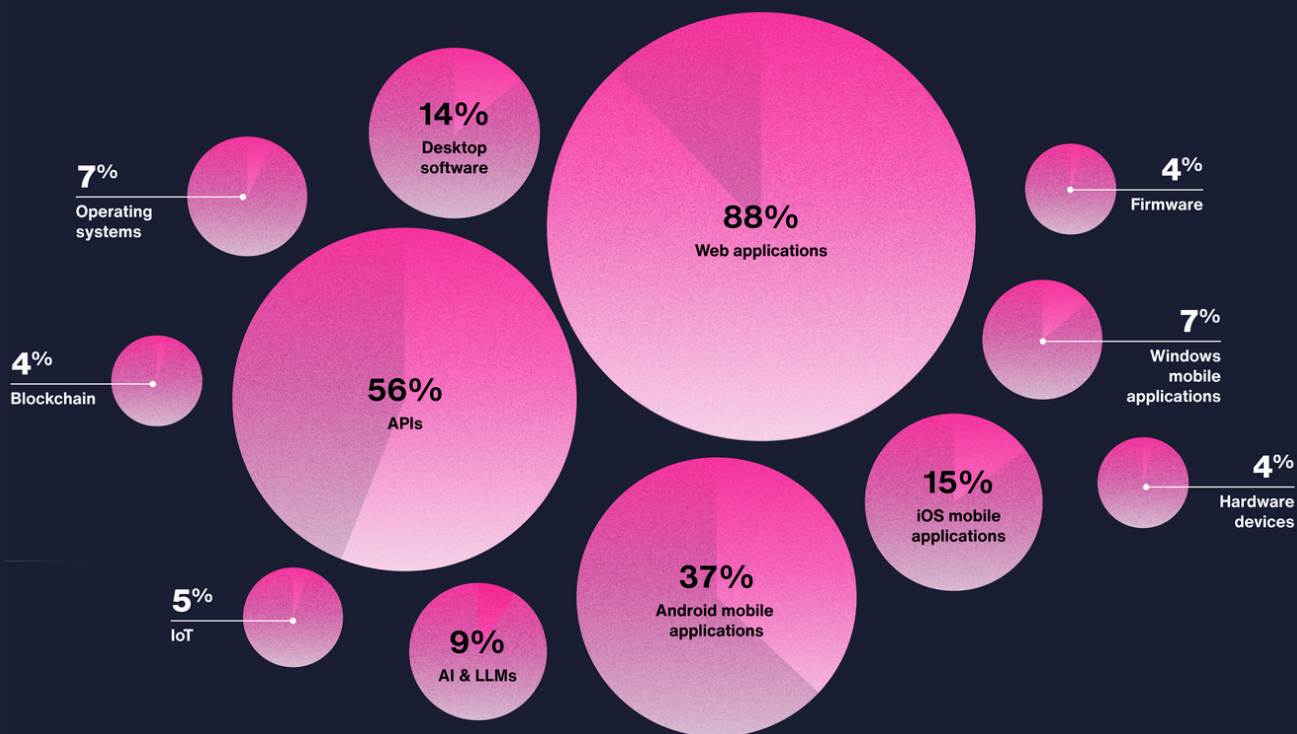


When HackerOne first launched, most hacking activity focused on web applications, and while 88% of researchers still specialize in this area, the landscape is shifting. Organizations are now calling on the community to test a wider range of products and technologies. 56% of researchers also specialize in APIs, while almost 10% now focus on AI and large language models (LLMs). Although the number of AI-focused researchers has grown by just 2% since last year, it's promising that nearly 10% are already working to secure this emerging technology. As more organizations include AI models in their scope, we expect this number to keep growing.



## When hacking web applications, what vulnerability types do you focus on?

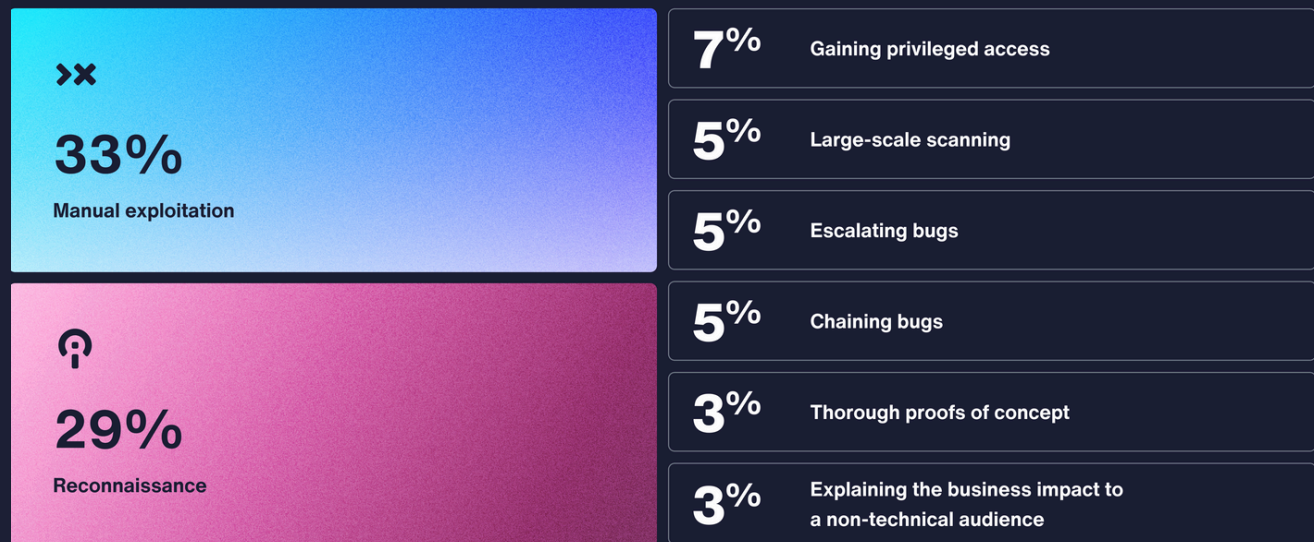
# Which asset types do you focus on in the bug bounty programs you participate in?



Security researchers excel in reconnaissance and manual exploitation—two key hacking skills that automated scanners can't match. These tasks require human creativity, like uncovering an unsecured, overlooked domain or spotting a unique vulnerability from an outsider's view. Even more advanced is exploit chaining, where vulnerabilities are combined into a larger, more impactful exploit. While chaining might be more challenging for individuals, researchers often collaborate, blending their strengths to create powerful, high-impact exploits.

Data indicates many researchers feel less confident in writing detailed reports, but GenAI tools are bridging this gap, enabling clearer communication of findings and higher-quality reports.

# What part of the hacking process do you consider yourself most skilled at?



The more you and your organization know and understand about researchers and their skills, motivation, and approaches, the stronger the relationship will be and the more impactful your program will be.

*"With scanning tools, false positives are through the roof. A human researcher, however, can provide more information and context about a vulnerability, often leading to Goldman fixing the problem quickly. We don't want problems to sit around."*

**Matt Levine**

Global Head of Technology Risk Advisory, Goldman Sachs

## Recommendations

- ✓ Clearly communicate expected response times for report acknowledgment, triage, and resolution. This builds trust and helps researchers understand when they can expect feedback.
- ✓ Offer constructive feedback on the report, explaining the vulnerability's impact and any necessary remediation steps.
- ✓ Respond to researchers with respect and professionalism, even if the report is invalid or a duplicate. Positive interactions encourage ongoing collaboration.

# Run a Top-Tier Program That Won't Break the Bank

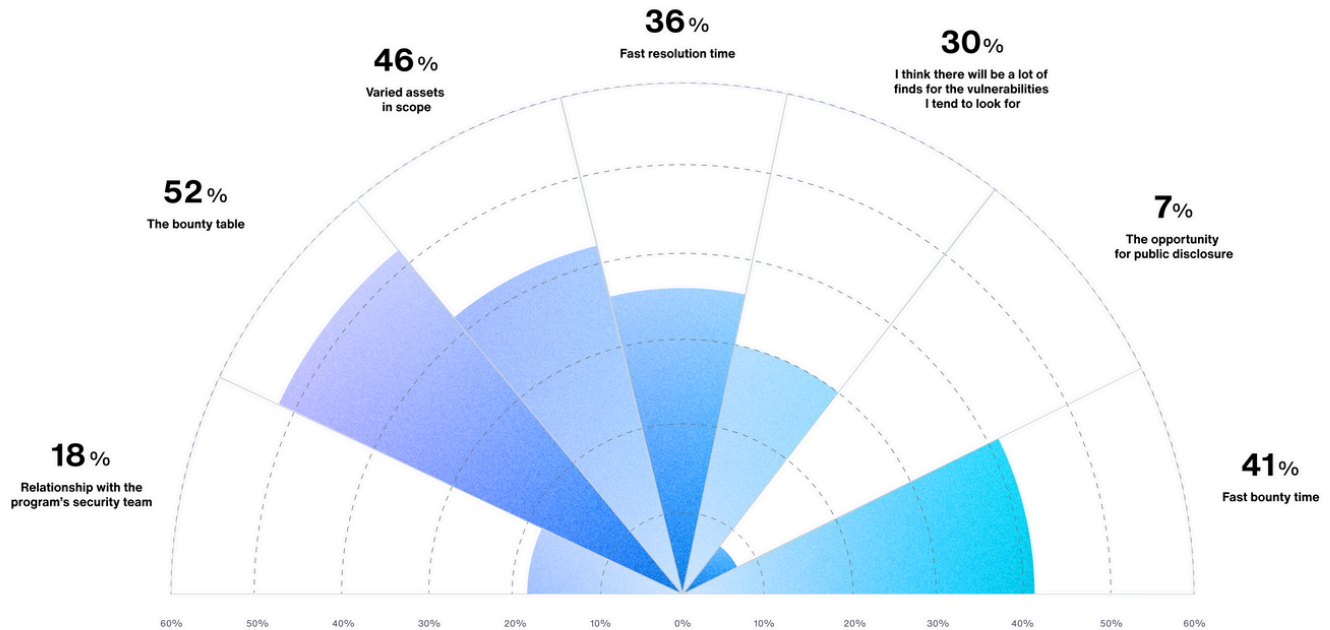
The most security-resilient customers on the HackerOne Platform share the following attributes:

- Thoughtfully designed rewards that direct researcher attention toward the organization's priorities
- Excellent communication with researchers who report vulnerabilities
- Clear expectations set from the start, including a well-defined scope and descriptive policy
- Safe harbor legal protections for security researchers

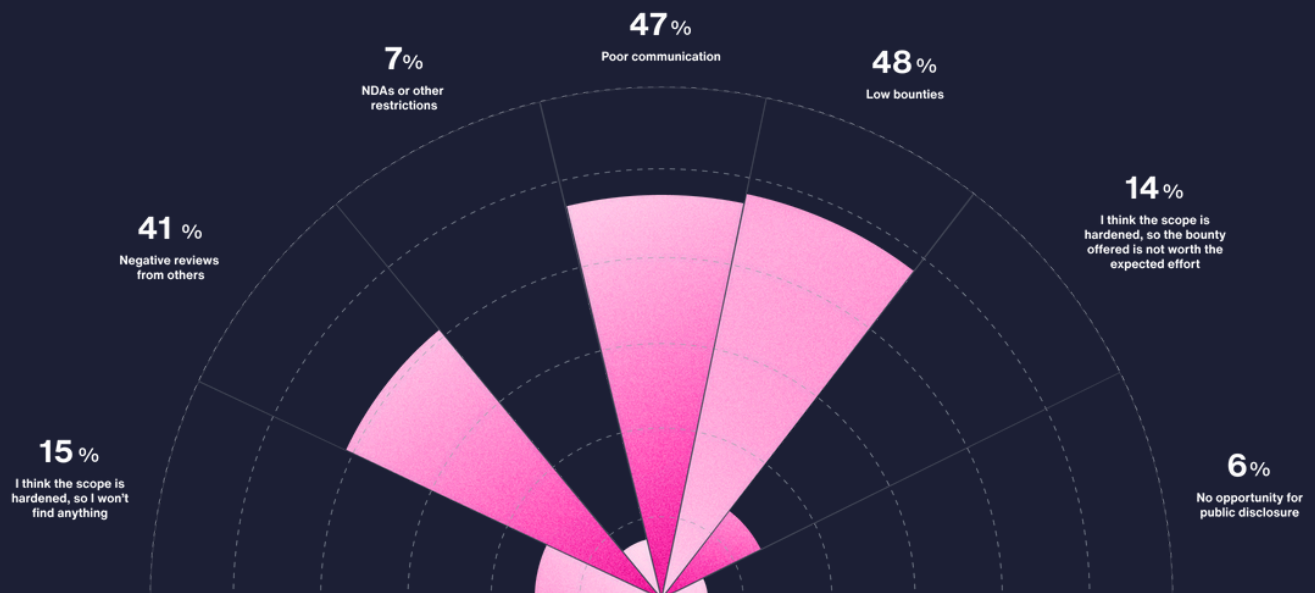
[Read about HackerOne's Platform Standards to learn more.](#)

***We asked our researcher community what features attract them to or deter them from joining a security program. No surprise: bounties topped the list, with 52% saying the bounty table draws them in, while 48% are turned off by low bounties.***

## How do you choose the companies you hack?



## What would make you decide not to hack on a program?





*“The bounty table is important. but I invest in programs that **give back to me in the way they communicate and their time to fix**. If they fix bugs fast, there will be fewer duplicates, which provides greater motivation for me.”*

**Jasmin Landry, @jr0ch17**

Security Researcher and HackerOne Pentester

Beyond the financial aspect, researchers value strong relationships with security teams, transparent communication, and quick responses to bounties and report resolutions. Clear updates on report status build trust, and offering context when a report's criticality is downgraded helps foster collaboration. Additionally, 41% mentioned that negative peer reviews would discourage them from participating, underscoring how important perception is for attracting researchers, driving engagement, and scaling a program effectively.

## Recommendations

- ✓ Focus researchers' efforts on the most critical components of your attack surface. These could be assets that have stagnant testing, have lacked attention, are new feature investments, or are recent acquisitions.
- ✓ Offer more advanced testing opportunities with unique scope or access to gated assets.
- ✓ Provide researchers with additional documentation to clarify scope, free test accounts, or even company swag to maximize impact without solely relying on increased bounties.

# Perspectives From the Hacker Advisory Board


HackerOne's annual Hacker Advisory Board meetings bring together some of the most experienced and active security researchers to understand how they evaluate the ROI of joining specific bug bounty programs. Key factors they consider include:

- Bounty table alignment with industry standards
- Brand impact and target organization profile (e.g., a Fortune 500 financial services company under media scrutiny may offer higher payouts than a local bank)
- Transparent, collaborative communication with the researcher community
- The organization's reputation among researchers
- Opportunities for public disclosure and transparency of vulnerabilities



*"Gather feedback from hackers to improve your program. Ask what they'd like to see, such as adding assets to scope—something I've requested in the past, which led to discovering additional vulnerabilities. Lower barriers to entry; extra policies or special requirements may discourage researchers from participating."*

**Jim Green, @greenjam**  
Security Researcher



***Most security researchers are attracted to a wide range of assets in scope, and only a few shy away from targets seen as tough to crack. With the right incentives, they're more than ready to take on the challenge.***

Our analysis this year centered on top-performing security programs, both private and public, identified as those with more than 30% of valid vulnerability submissions rated high or critical. The data reveals that fostering a smaller, highly engaged group of researchers and offering competitive rewards across a wider testing scope result in a significantly higher proportion of high and critical findings.

We found that high-impact programs have three key traits:

- **Higher bounties:** Offering average payouts of \$3,300 at the 95th percentile, compared to \$2,000 for lower-impact programs.
- **Smaller, focused communities:** Engaging fewer researchers, with an average of 56 versus 97 in lower-impact programs. However, being able to curate a smaller, highly engaged group depends on having a large researcher pool from which to choose the most applicable talent for your program.
- **Broader testing scope:** Providing more assets for testing, averaging 60 assets compared to 34 in lower-impact programs.

## Recommendations

- ✓ Collaborate with a select group of skilled researchers who align well to your program's scope.
- ✓ Establish reward structures aligned with the criticality of the assets being tested, ideally offering compensation above market standards.
- ✓ Ensure your testing scope is broad and varied, allowing researchers with diverse skill sets to contribute meaningfully. This targeted approach fosters deeper engagement and drives more impactful security outcomes.

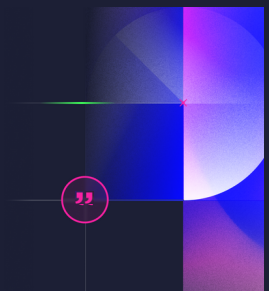
[Read more about how HackerOne customers get the best results from researchers.](#)



*"I believe in a blanket approach when it comes to which assets to test with bug bounty. Test everything across the board. People say, 'We don't want to put everything out there,' but, if one asset is compromised, then the next is too. If it's external facing, it should be tested."*

**Jose Ramos**

Leader in Offensive Security and Penetration Testing, Uber



# Community Events Bring the Best and the Brightest Together for Maximum Impact

HackerOne's most security-resilient customers excel at incentivizing researchers to focus on specific scopes at strategic times. Through high-caliber, targeted engagements, HackerOne replicates real-world threats to pinpoint vulnerabilities, especially during flagship community events.



## Live Hacking Events

Live Hacking Events (LHEs) bring together top security researchers to focus on high-priority scopes for mature customers. These events produce 34% high and critical vulnerability reports, compared to the platform average of 27%. Collaboration is a major factor, with 48% of valid reports and 69% of bounty awards in 2023 resulting from joint efforts. LHEs also have lasting benefits, boosting post-event engagement by an average of 15%, making them a key driver of impactful security improvements.

*“Capital One puts the security of our customers and our systems at the forefront of everything we do. Live Hacking Events are a key component of our robust security testing strategy and are a unique and dynamic way to engage with the ethical hacking community, allowing us to form close partnerships with each of the hackers. Across the industry, these types of events are considered a gold standard to ensure companies are approaching risk from every potential angle, and we're grateful for the hackers' hard work and partnership to help us further bolster our defenses.”*

**Kathryn Torelli**  
Bug Bounty Lead, Capital One

*“A Live Hacking Event is an experience removed from day-to-day hacking with new scope, higher bounties, and direct access to the customer team. The customers benefit from having nearly 100 of the most elite hackers in the world concentrating on their program for a solid three weeks. My approach to hacking at an LHE is to pick an obscure scope early on, something that I know other people won't be looking at.”*

**Douglas Day, @arch\_angel**  
LHE Researcher, Most Valuable Hacker Award Winner



## Ambassador World Cup

The Ambassador World Cup (AWC) is an annual event that brings international researcher teams together for a friendly competition, with the goal of delivering the most impactful results for participating customers. While more accessible than a Live Hacking Event, the Ambassador World Cup still provides customers with dedicated attention from highly motivated and skilled researchers. Beyond the contributions of the competing teams, the event's visibility encourages wider community engagement, as researchers are drawn to test on high-profile customer programs after seeing the activity through their networks and social media. In the 2023 Ambassador World Cup, researchers reported over 800 valid vulnerabilities for the 11 participating customers, demonstrating the event's ability to drive meaningful security outcomes.

*"Participating in the Ambassador World Cup was an incredible opportunity for Adobe to build deep relationships with the hacker community. I received great feedback about our bug bounty program and the AWC experience. Many hackers were new to our program, which was a great way to expand Adobe's outreach to the hacking community."*

**Daniel Ventura**

Product Security Manager, Adobe PSIRT & Bug Bounty, Adobe

*"The Ambassador World Cup was transformative, offering a unique chance to enhance my skills on programs like Mercado Libre, where I had one of my best triage experiences. AWC introduced me to new programs, expanding my horizons."*

**Sandip Oli, @notsandip**

Team Nepal of the AWC





## Budgeting for Bounties

Bounties can make or break a bug bounty program, the bounty table being the number-one factor for researchers making a decision on which programs to spend time, with half being put off a program that has uncompetitive bounties.















Average bounty payouts have remained steady over the past 12 months, with a 5% increase year over year, from \$1,066 to \$1,116. However, that's a decrease of 10% from 2021, when the average bounty was \$1,246. Organizations need to be wise to the fact that without competitive compensation, talented researchers may move to more lucrative programs, or focus only on low-hanging fruit that doesn't require detailed research effort, resulting in less exploitable, less critical vulnerabilities. Dynamic, fair compensation is key to keeping researchers engaged and improving organizational security.

Bounties are typically more competitive in the critical vulnerability category, with the most technology-reliant organizations seeing an increase of between 20% (internet and online services) and 450% (crypto and blockchain) since 2023.

Low-severity bounties, however, have not changed significantly year over year. This could be as a result of an increase in automated tools that surface low-level vulnerabilities before researchers can find them, reducing the competition.

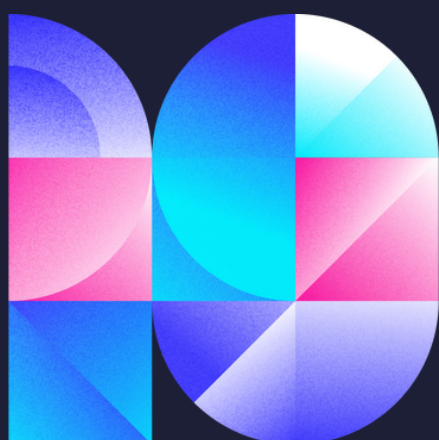
The following table shows the median, average, and 95th percentile bounty payouts across various industry sectors. As in previous years, crypto and blockchain organizations continue to pay well above the average for vulnerabilities. The high financial risk, technical complexity, and reputational stakes in this space drive these organizations to offer significantly higher bounties to attract top-tier security researchers. We also see more differences between the industries when we look at the 95th percentile, with traditionally security-mature industries like internet and online services and retail and e-commerce paying toward the top end of the average across all levels of severity.

# Median, Average, and 95th Percentile Bounty Rewards

	● Critical			● High			● Medium			● Low		
	Median	Average	95th Percentile	Median	Average	95th Percentile	Median	Average	95th Percentile	Median	Average	95th Percentile
 Computer Hardware & Peripherals	\$3,000	\$3,000	\$3,000	\$1,500	\$1,500	\$1,950	\$450	\$450	\$495	\$150	\$150	\$150
 Computer Software	\$5,000	\$10,065	\$22,500	\$2,000	\$3,858	\$10,000	\$500	\$1,069	\$2,875	\$200	\$271	\$575
 Crypto & Blockchain	\$55,000	\$244,900	\$1,000,000	\$7,500	\$22,500	\$96,000	\$2,000	\$8,575	\$40,750	\$550	\$2,045	\$9,150
 Energy & Utilities	\$4,000	\$4,000	\$4,900	\$1,500	\$1,500	\$1,500	\$500	\$500	\$500	\$150	\$150	\$150
 Financial Services	\$5,000	\$6,360	\$11,000	\$2,500	\$3,064	\$5,000	\$750	\$750	\$2,050	\$200	\$249	\$600
 Government	\$5,000	\$6,231	\$10,000	\$2,000	\$3,010	\$5,775	\$750	\$750	\$1,500	\$200	\$266	\$550
 Healthcare	\$4,000	\$5,250	\$12,250	\$1,750	\$2,188	\$5,450	\$500	\$500	\$1,725	\$250	\$242	\$400
 Industrial Manufacturing	\$4,000	\$4,000	\$5,000	\$2,000	\$2,000	\$2,500	\$500	\$500	\$500	\$200	\$200	\$250
 Internet & Online Services	\$5,000	\$10,810	\$25,000	\$2,000	\$4,998	\$10,000	\$500	\$1,542	\$4,500	\$200	\$349	\$1,000
 Media & Entertainment	\$3,000	\$4,700	\$9,000	\$1,500	\$2,058	\$4,792	\$500	\$809	\$2,204	\$225	\$275	\$500
 Retail & E-commerce	\$5,000	\$7,080	\$24,000	\$2,000	\$3,030	\$9,700	\$750	\$1,010	\$3,300	\$250	\$252	\$500
 Telecommunications	\$5,000	\$6,743	\$15,500	\$2,000	\$2,889	\$7,750	\$750	\$1,043	\$2,775	\$138	\$215	\$601
 Transportation	\$4,000	\$5,125	\$11,500	\$1,500	\$2,569	\$7,200	\$638	\$638	\$3,512	\$200	\$297	\$746
 Travel & Hospitality	\$5,000	\$4,763	\$7,750	\$2,000	\$2,174	\$4,305	\$500	\$753	\$1,693	\$200	\$236	\$622

## Recommendations

- ✓ Make a strong business case for your budget that speaks to the priorities of your stakeholders and board members. Check out the [Measuring Success](#) section of this report to see how the most security-resilient organizations are making the financial case for their bounty budgets using a return on mitigation (ROM) approach.
- ✓ Take a tiered-award approach, with bounty awards weighted by asset type. Bounty award amounts can be adjusted to incentivize testing on your most critical assets as well as assets that may require a more unique skill set.
- ✓ Set bounties high enough to attract interest. If you're falling behind your budget and not receiving reports on business-critical assets, it's a clear sign that your bounties may need adjustment.



# The Top Ten Vulnerabilities Need to Change

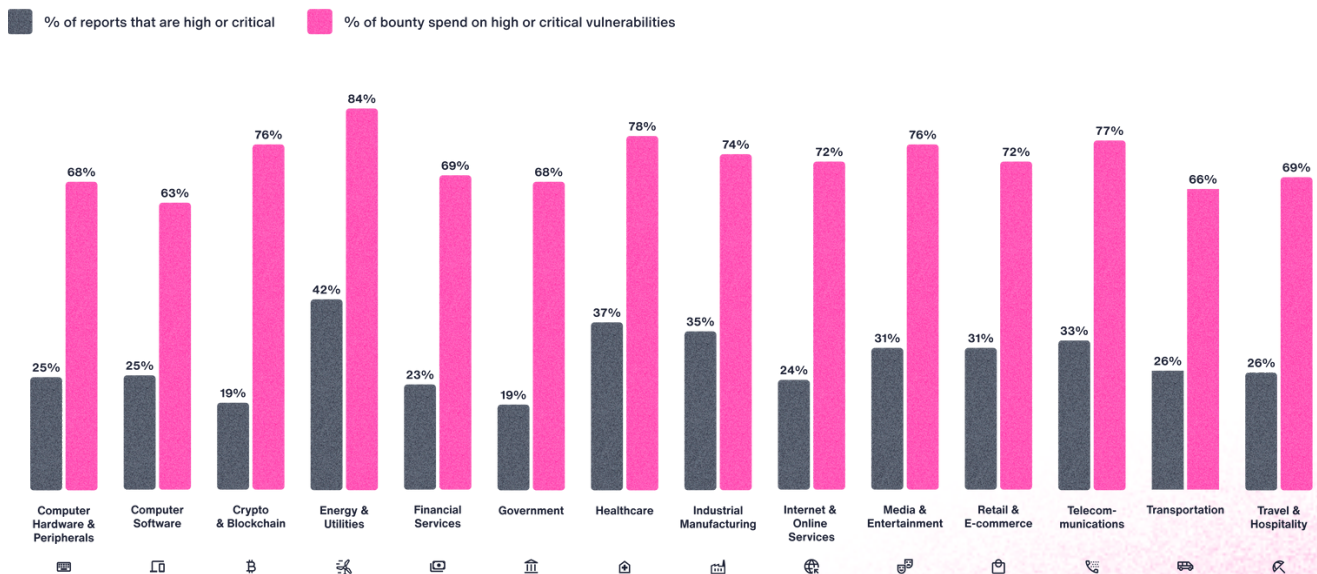
HackerOne has been measuring the top ten vulnerabilities reported on our platform for eight years. Despite the investment in security, and industry calls for better security practices earlier in the software development life cycle (SDLC), we see steady increases in vulnerability reports year over year and most industries are still seeing the most common vulnerabilities reported again and again.

Valid vulnerabilities on the HackerOne Platform have jumped 12% over the past year, with 78,042 valid issues found across 1,300+ customer programs. Impressively, 27% of these are rated high or critical. While organizations are making efforts to reduce vulnerability reports by identifying trends and putting measures in place to catch them earlier in development, we do expect vulnerability reports to keep rising as more organizations embrace human-led security.

## # of Valid Reports per Year



## What Percentage of Vulnerability Reports Is High or Critical for Your Industry?



# Looking at the percentage of valid high or critical reports reveals an interesting trend:

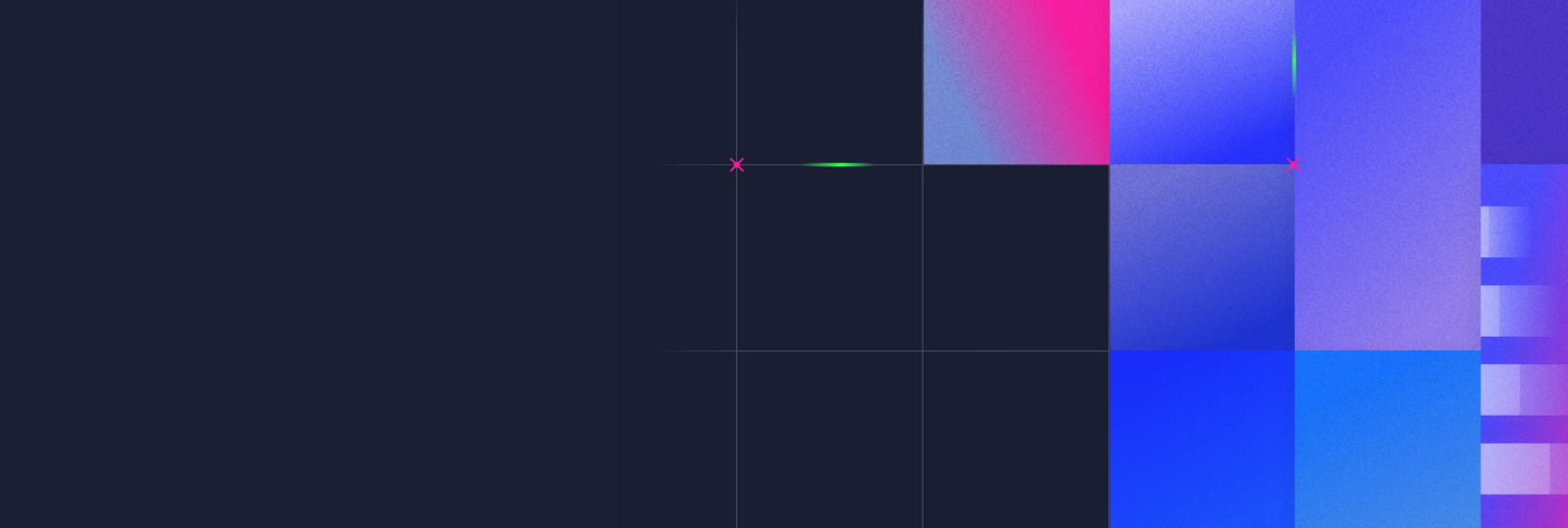


**Organizations that spend less on technology often see more severe vulnerabilities, sometimes hitting 42%.** In comparison, tech-focused sectors like crypto, travel, and internet services show around 20% for severe issues, while critical infrastructure areas like energy and healthcare exceed 35%. Telecoms and media, with their large asset counts, also face a higher rate of critical findings, suggesting that as an attack surface grows, it's harder to stay on top of potential vulnerabilities.


**High and critical reports might be a smaller portion of overall findings, but they account for most of the bounty spend, especially as severe reports increase.** This trend is even more pronounced in the crypto and blockchain sectors, where top bounties can hit up to \$1 million in the 95th percentile.

**Over the past year there was a sharp 180% jump in breaches exploiting vulnerabilities, according to Verizon's Data Breach Investigations Report.<sup>4</sup>** Incidents like MOVEit and other zero days fueled this surge, mainly driven by ransomware and extortion-focused attackers, with web applications being the primary entry point.

<sup>4</sup> Verizon. [2024 Data Breach Investigations Report](#).



Despite the rising threat, vulnerabilities are often still seen as just part of the tech landscape. As Jen Easterly, Director of CISA, stressed in her 2024 Black Hat address,<sup>5</sup> the industry needs a shift toward building software with security as a priority.



**The good news? There's a clear path to stronger security.** HackerOne data shows that the top ten vulnerabilities reported to customer programs are common and mostly preventable with proactive measures. Catching these issues early in the SDLC can significantly cut down on bounty costs. Check how your industry stacks up against the average for common vulnerabilities, and see the [defense-in-depth](#) section of this report for tips on reducing these risks and boosting your overall security.

**Reports for the three most common vulnerabilities are all down by a small percentage platform-wide since 2023, with reports for cross-site scripting down 10%, suggesting that some of the tactics to reduce common vulnerabilities are having an impact.** When we look at where specific industries are seeing the most reports, however, we see a different trend, with significant increases in reports for the vulnerability types most common in their systems.

<sup>5</sup> Cyberscoop. [Easterly: Cybersecurity is a software quality problem.](#)

# The Top Ten Vulnerabilities Reported to Customer Programs

■ Above average performance
 ■ Below average performance
 ■ Average performance

Most common platform vulnerability	Platform Average	 Financial Services	 Government	 Telecoms	 Retail & E-commerce	 Transportation	 Media & Entertainment	 Computer Software	 Internet & Online Services	 Crypto & Blockchain	 Travel & Hospitality
Cross-Site Scripting (XSS)	20%	19% <span style="color: green;">—</span>	40% <span style="color: red;">—</span>	15% <span style="color: green;">—</span>	19% <span style="color: green;">—</span>	34% <span style="color: red;">—</span>	21% <span style="color: gray;">—</span>	19% <span style="color: green;">—</span>	17% <span style="color: green;">—</span>	7% <span style="color: green;">—</span>	27% <span style="color: red;">—</span>
Information Disclosure	10%	11% <span style="color: gray;">—</span>	13% <span style="color: gray;">—</span>	12% <span style="color: gray;">—</span>	16% <span style="color: red;">—</span>	13% <span style="color: gray;">—</span>	9% <span style="color: green;">—</span>	9% <span style="color: green;">—</span>	13% <span style="color: gray;">—</span>	7% <span style="color: green;">—</span>	10%
Improper Access Control	9%	12% <span style="color: gray;">—</span>	5% <span style="color: green;">—</span>	10% <span style="color: gray;">—</span>	8% <span style="color: green;">—</span>	8% <span style="color: green;">—</span>	10% <span style="color: gray;">—</span>	13% <span style="color: red;">—</span>	13% <span style="color: red;">—</span>	10% <span style="color: gray;">—</span>	8% <span style="color: green;">—</span>
Misconfiguration	6%	7% <span style="color: gray;">—</span>	2% <span style="color: green;">—</span>	6% <span style="color: green;">—</span>	8% <span style="color: gray;">—</span>	5% <span style="color: green;">—</span>	12% <span style="color: red;">—</span>	8% <span style="color: gray;">—</span>	7% <span style="color: gray;">—</span>	6% <span style="color: green;">—</span>	9% <span style="color: gray;">—</span>
Insecure Direct Object Reference (IDOR)	6%	7% <span style="color: gray;">—</span>	1% <span style="color: green;">—</span>	12% <span style="color: red;">—</span>	9% <span style="color: red;">—</span>	6% <span style="color: gray;">—</span>	8% <span style="color: gray;">—</span>	6% <span style="color: gray;">—</span>	8% <span style="color: gray;">—</span>	2% <span style="color: green;">—</span>	6%
Improper Authentication	2%	3% <span style="color: gray;">—</span>	2% <span style="color: gray;">—</span>	7% <span style="color: red;">—</span>	3% <span style="color: gray;">—</span>	2% <span style="color: gray;">—</span>	3% <span style="color: gray;">—</span>	3% <span style="color: gray;">—</span>	3% <span style="color: gray;">—</span>	4% <span style="color: red;">—</span>	2%
Privilege Escalation	2%	3% <span style="color: gray;">—</span>	1% <span style="color: green;">—</span>	3% <span style="color: gray;">—</span>	2% <span style="color: gray;">—</span>	2% <span style="color: gray;">—</span>	4% <span style="color: red;">—</span>	4% <span style="color: red;">—</span>	3% <span style="color: gray;">—</span>	2% <span style="color: gray;">—</span>	4% <span style="color: gray;">—</span>
Open Redirect	2%	4% <span style="color: red;">—</span>	1% <span style="color: green;">—</span>	2% <span style="color: gray;">—</span>	4% <span style="color: red;">—</span>	4% <span style="color: red;">—</span>	4% <span style="color: red;">—</span>	2% <span style="color: gray;">—</span>	2% <span style="color: gray;">—</span>	2% <span style="color: gray;">—</span>	4% <span style="color: red;">—</span>
Business Logic Errors	2%	2% <span style="color: gray;">—</span>	0% <span style="color: green;">—</span>	2% <span style="color: gray;">—</span>	3% <span style="color: gray;">—</span>	1% <span style="color: green;">—</span>	3% <span style="color: gray;">—</span>	2% <span style="color: gray;">—</span>	3% <span style="color: gray;">—</span>	10% <span style="color: red;">—</span>	1% <span style="color: green;">—</span>
SQL Injection	2%	2% <span style="color: gray;">—</span>	7% <span style="color: red;">—</span>	4% <span style="color: red;">—</span>	3% <span style="color: gray;">—</span>	4% <span style="color: red;">—</span>	1% <span style="color: green;">—</span>	1% <span style="color: green;">—</span>	1% <span style="color: green;">—</span>	0% <span style="color: green;">—</span>	2%

# Financial Services

## Featured vulnerability:

Insecure direct object reference (IDOR)  
(up 47% from 2023)

Financial services is one of the most targeted and regulated sectors, having experienced 70 compromises in Q1 2023, impacting about 1.7 million victims.<sup>6</sup> Due to strict regulations like GDPR and PCI-DSS, they tend to receive more vulnerability reports, as these standards incentivize researchers to flag potential issues.

Insecure direct object reference vulnerabilities are particularly prevalent in financial services because of their complex, multi-layered applications that manage sensitive data, like personal financial information and transactions. The frequent user actions, such as money transfers and account access, heighten the risk of IDOR exploits when access controls are weak, making them prime targets for bug bounty hunters.

## Insecure Direct Object Reference (IDOR)

Percentage of total reports

Percentage of total bounty rewards

Percentage of total platform reports

6%

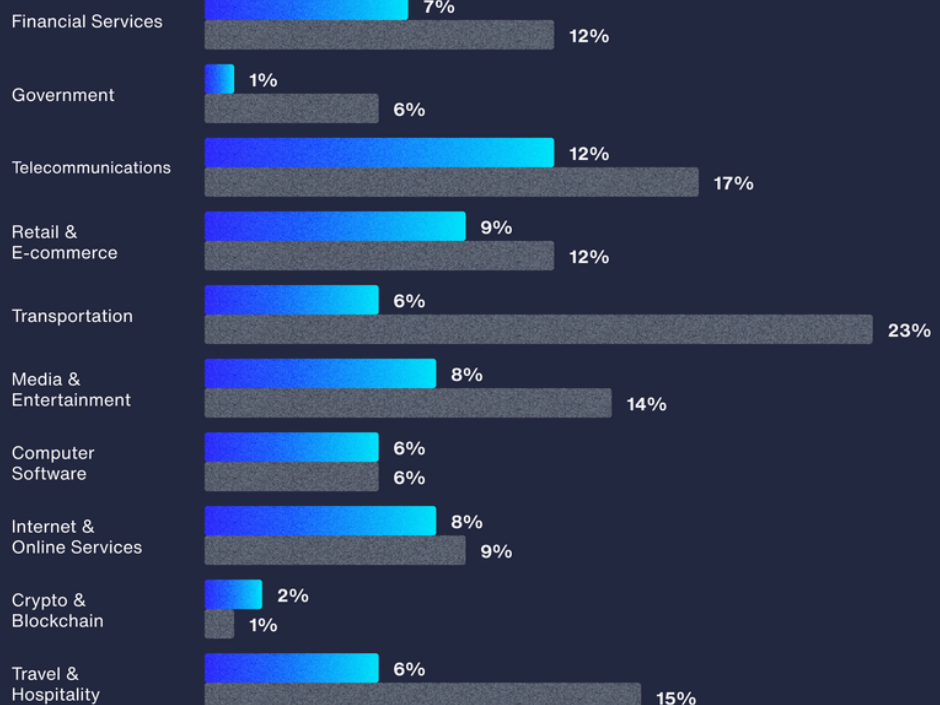
↓ 3% YOY decrease

Percentage of total platform bounty rewards

10%

Average bounty payout

\$1,285



<sup>6</sup> [SANS 2023 Attack and Threat Report](#).



*“The most frequent vulnerabilities that I have come across in the financial services sector tend to be misconfigurations and vulnerabilities common in legacy software. This is likely due to the complexity of financial systems, large amounts of sensitive data handled, and the pressure to launch new products in the market. Financial services organizations have significant security challenges, ranging from protecting sensitive data to regulatory compliance. However, this also offers them the opportunity to improve cybersecurity, foster collaboration, and develop innovations that strengthen security and trust.”*

**Richard Alvarez, @Rhack**

Security Researcher Specializing in Financial Services Organizations

*“Having hacked on a variety of financial service targets, I've noticed that these organizations often have a wider and more complex attack surface due to their company structures, which often include numerous acquisitions and subsidiaries. As a result, I've found vulnerabilities on obscure hosts—sometimes on newly launched or less commonly known domains. Due to the need to obtain an account for deeper testing, which is difficult and sometimes even impossible due to geographical restrictions (applying for a loan/credit card), a significant portion of the attack surface remains untouched.”*

**Iustin Ladunca, @youstin**

Security Researcher Specializing in Financial Services Organizations

## Recommendations



Implement a strong authorization framework that relies on user policies and hierarchy, and validate authorization for every request that involves accessing sensitive objects or resources.



Avoid using functions that automatically bind a client's input into variables, internal objects, or object properties.



Use indirect, random, and unique identifiers instead of exposing direct references to internal objects and resources. Map these identifiers to the actual objects on the server side while validating and authorizing user-supplied input.

# Government

## Featured vulnerability:

Cross-site scripting (XSS) (up 17% from 2023)



Government agencies see a much higher rate of XSS vulnerability reports than the industry average. This is likely due to their many complex web environments, as they manage a wide range of websites and services for various public functions. This diversity can lead to inconsistent security practices, making some sites more vulnerable. Plus, many government systems run on older, legacy technologies that lack modern security tools. The slower pace of updates in government IT further increases their exposure to vulnerabilities, putting them at greater risk compared to more agile industries.

## Cross-Site Scripting (XSS)

Percentage of total reports Percentage of total bounty rewards

Percentage of total platform reports

20%

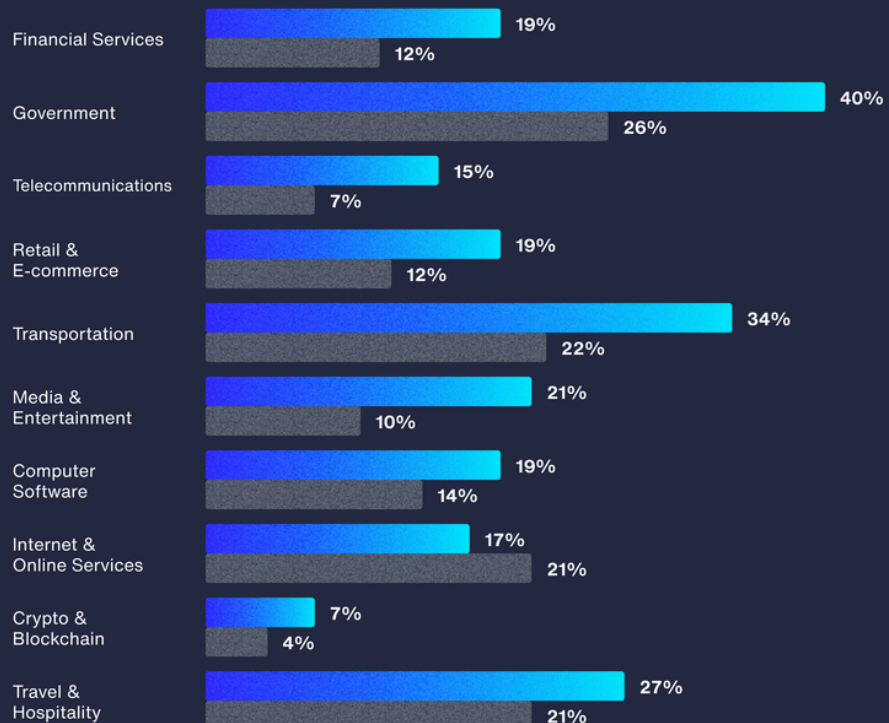
↓ 10% YOY decrease

Percentage of total platform bounty rewards

16%

Average bounty payout

\$577



## Recommendations

- ✓ Treat all input as malicious and create a list of what is expected or valid input.
- ✓ Encode output that, depending on the output context, might require applying combinations of HTML, URL, JavaScript, and CSS encoding.
- ✓ Implement a content security policy (CSP) to restrict the sources of executable scripts and limit the potential impact of XSS attacks.



*“The vulnerabilities I see most often in government programs involve legacy software or applications that have been deployed for a long period of time and have SSRF, XSS, and authorization issues. These are mainly due to the applications' legacy nature, which was written before penetration testing was widely performed. Hacking on government programs is fun because the data within the applications or infrastructure is often very sensitive, and knowing I was able to help secure the data is rewarding.”*

**Sean Melia, @meals**

Security Researcher Specializing in Government Organizations

*“When working with government programs, there is often an onus on the responsible handling of data encountered during testing—data classifications are a core component of these institutions. For me, this often means taking more care and planning my approach to working on these systems so as to not inadvertently expose or mishandle this data, thus causing wider impacting issues. With that said, technology stacks within government programs are vast, ranging from small legacy applications written in 20-year-old ASP code and a single backend database to huge cloud deployments utilizing modern components and infrastructure. This makes these programs interesting targets and certainly provides a real sense of depth when it comes to security testing.”*



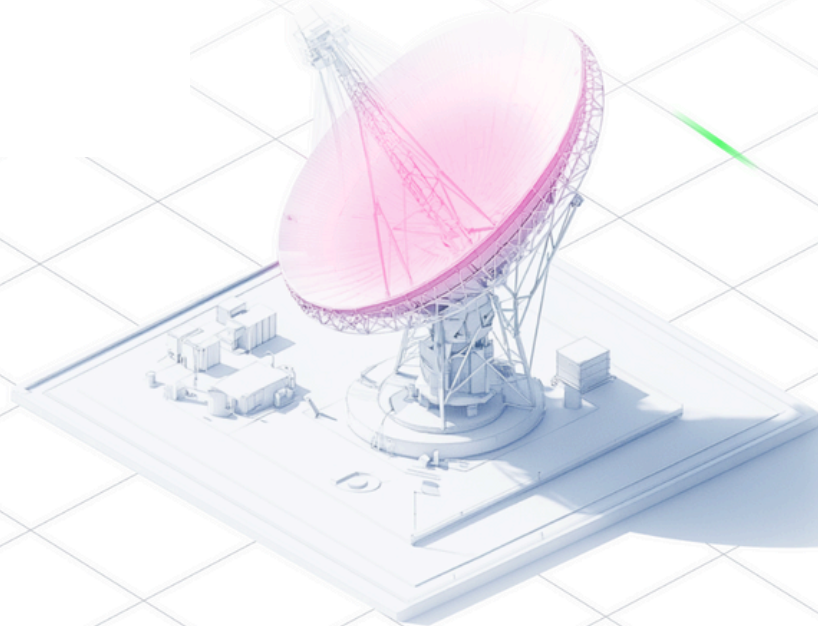
**Trevor Shingles, @sowhatsec**

Security Researcher Specializing in Government Organizations

# Telecoms

## Featured vulnerability:

Improper authentication  
(up 55% from 2023)



Telecom organizations manage vast networks with millions of connected users and devices, and authentication across such a complex infrastructure is prone to misconfigurations or weak implementations. The telecoms' diverse customer base, from individual users to large enterprises, often leads to inconsistencies in authentication practices, heightening the risk of improper authentication vulnerabilities.

Many telecom companies rely on legacy systems that lack robust authentication mechanisms or may have outdated encryption standards. Telecom companies also integrate with third-party services, such as mobile apps, payment gateways, and other providers in which improperly configured APIs or authentication mechanisms can cause vulnerabilities.



## Improper Authentication

Percentage of total reports Percentage of total bounty rewards

Percentage of total platform reports

2%

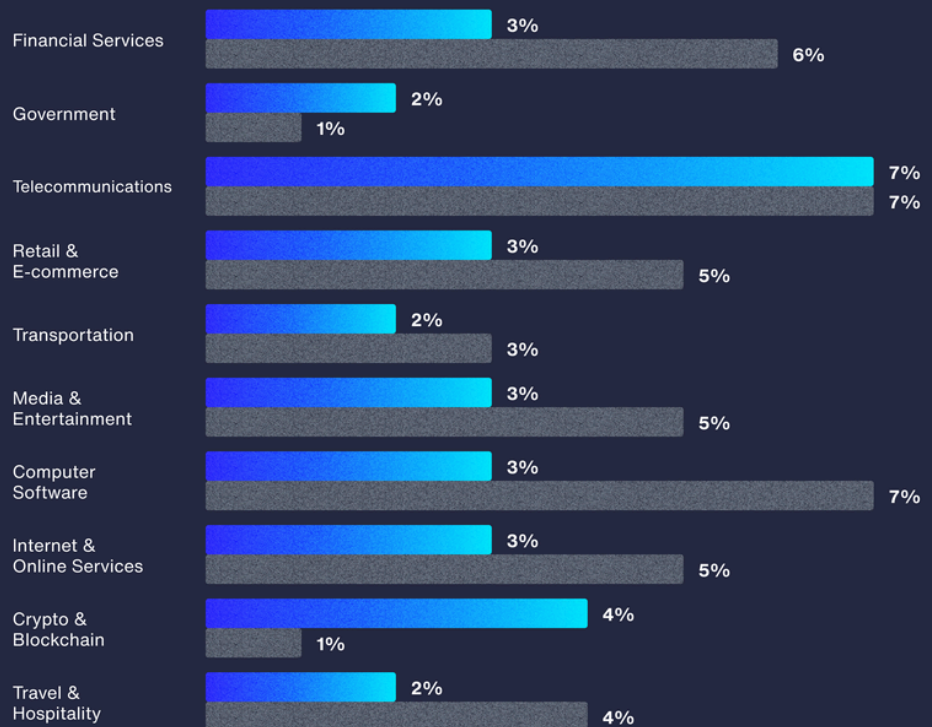
↓ 17% YOY decrease

Percentage of total platform bounty rewards

3%

Average bounty payout

\$793



## Recommendations

- ✓ Implement robust and secure authentication methods, such as strong password requirements, multi-factor authentication (MFA), secure password storage, and account lockout mechanisms.
- ✓ Manage session and authentication tokens by generating random, unique, and unpredictable tokens, securely storing them on the server side, implementing proper session expiration and logout mechanisms, and avoiding persistent tokens unless necessary.
- ✓ Avoid exposing unnecessary data in APIs, error messages, or logs, and use generic error messages to prevent attackers from gaining insights.

# Retail and E-commerce

**Featured vulnerability:**  
Information disclosure  
(up 71% from 2023)



Retail and e-commerce are prime targets for cybercrime, with 16 breaches in Q1 2023 affecting 170,000 victims in total.<sup>7</sup> This sector sees the most vulnerability reports for information disclosure due to handling vast amounts of sensitive customer data. The complexity of e-commerce platforms, featuring dynamic websites and applications, increases the risk of information leaks through improperly secured APIs, mishandled user inputs, and flawed data-management practices.

## Information Disclosure

Percentage of total platform reports

**10%**

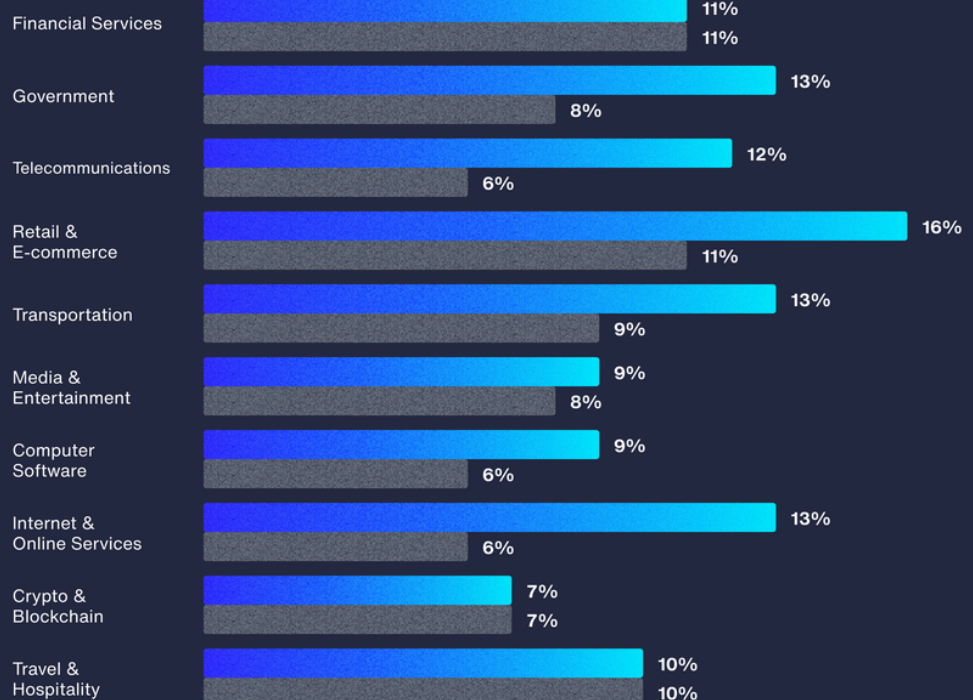
↓ 21% YOY decrease

Percentage of total platform bounty rewards

**7%**

Average bounty payout

**\$511**



<sup>7</sup> [SANS 2023 Attack and Threat Report](#).

## Recommendations

- ✓ Ensure that sensitive data, such as user credentials, payment details, and personal information, is encrypted in transit and at rest.
- ✓ Avoid exposing unnecessary data in APIs, error messages, or logs, and use generic error messages to prevent attackers from gaining insights.
- ✓ Follow the principle of least privilege. Grant users and processes the minimum permissions necessary to perform their tasks.

“

*“The most common issues I encounter in a [retail] chain’s bug bounty program are due to the many entry points—APIs, user inputs, etc. The organization is constantly developing and shipping promotions and new systems, which makes it challenging for them to secure all the integrations and user data. The huge number of endpoints and systems do make this program a bit tricky, but it’s also rewarding; new features are continuously appearing, and the security team is highly communicative and always excellent to work with as a researcher.”*

**Diego Adelantado, @godiego**

Security Researcher Specializing in Retail and E-commerce Programs

*“The vulnerabilities I see the most in retail and e-commerce programs are improper access control, information disclosure (PII), and account takeover. These kinds of vulnerabilities mostly depend on manual testing and the hacker’s understanding of the application, and are unlikely to be discovered by using automated scanning tools. The challenge is that these organizations do not always pay bounties that are proportionate to the seriousness of the vulnerabilities, which causes hackers to move on from the program, leaving the organization exposed.”*

**Tan See Jou, @pinkmeimei**

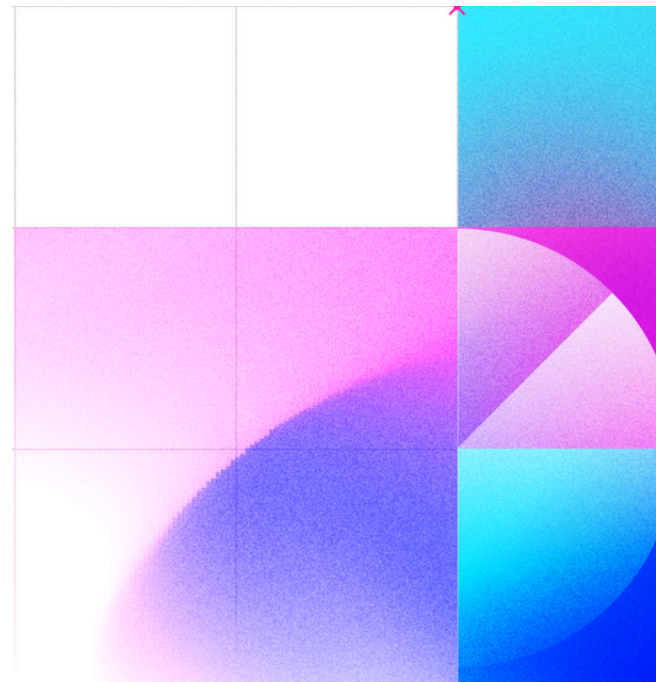
Security Researcher Specializing in Retail and E-commerce Programs

# Transportation

## Featured vulnerability:

SQL injection (up 93% from 2023)

Many transportation organizations, especially in aviation and automotive, still rely on legacy systems developed before modern security practices became widespread. These older systems often lack proper input validation and secure coding, making them vulnerable to SQL injection, especially with the growing demand for web and mobile interfaces. Further, complex networks of interconnected systems, such as booking, navigation, and maintenance, can introduce vulnerabilities through poor integration practices. Additionally, third-party integrations for services like payment processing, navigation, and maintenance platforms may expose organizations to SQL injection if the third-party systems don't enforce strict security standards.



## SQL Injection

Percentage of total reports Percentage of total bounty rewards

Percentage of total platform reports

2%

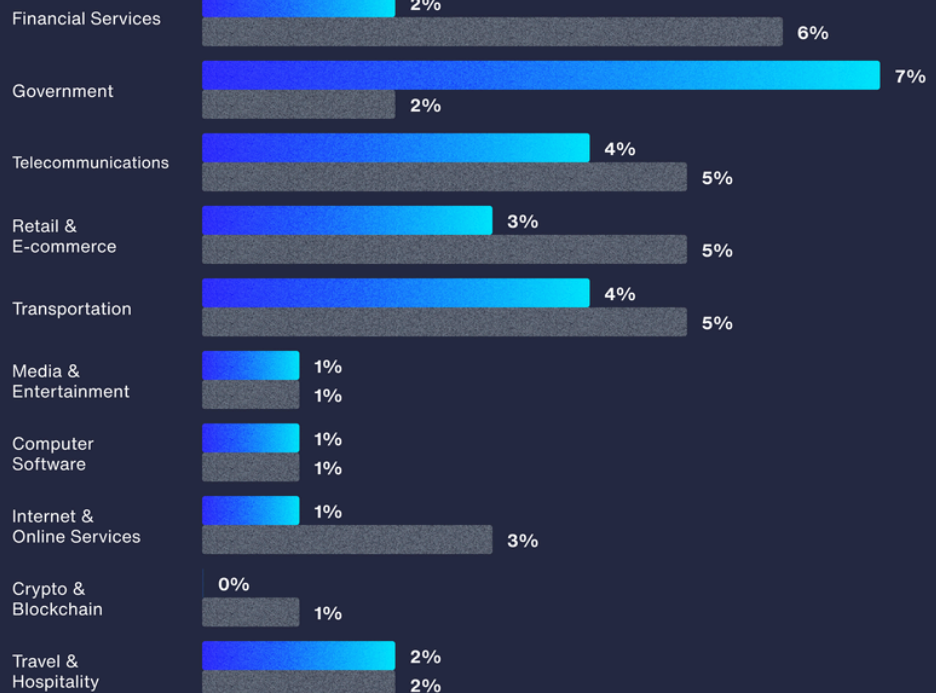
↑ 1% YOY increase

Percentage of total platform bounty rewards

3%

Average bounty payout

\$1,084



## Recommendations

- ✓ Implement prepared statements (parameterized queries) to separate SQL code from data, ensuring that user input cannot alter the query structure and intent.
- ✓ Validate and sanitize all user input to identify and remove potentially malicious data before processing any SQL query.
- ✓ Employ web application firewalls (WAFs) to detect and block SQL injection attempts, conduct regular security audits and penetration tests, and educate developers on secure coding practices.

*"You can either have a managed ethical hacker program or an unmanaged hacker program, because we all know that the threat vectors exist, and it's just a matter of time before they get identified in the wild."*

**Maurice Stebila**  
CISO, General Motors



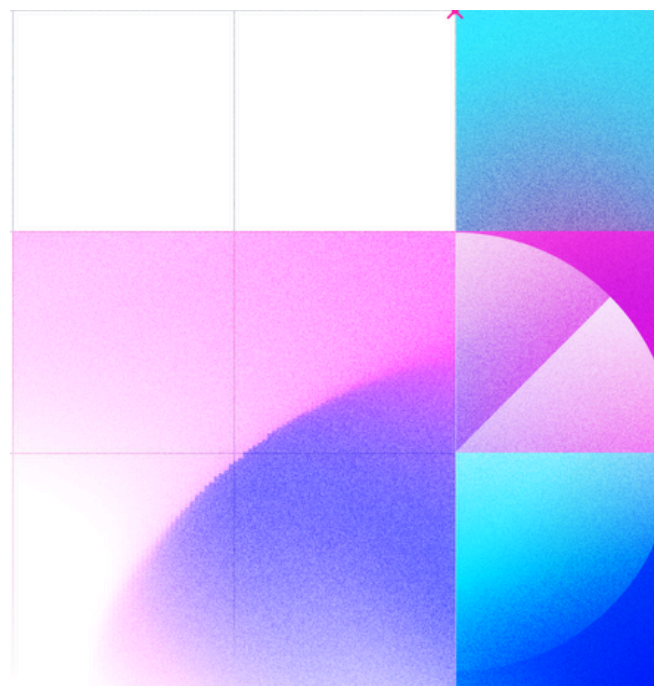
# Media and Entertainment

## Featured vulnerability:

Misconfiguration  
(up 69% from 2023)



Media and entertainment organizations see the highest proportion of reports for misconfigurations. This sector typically relies on complex content delivery networks (CDNs) and streaming platforms to distribute their content globally. The complexity and scale of these networks can lead to misconfigurations, especially when it comes to security settings and access controls.



## Misconfiguration

Percentage of total reports Percentage of total bounty rewards

Percentage of total platform reports

6%

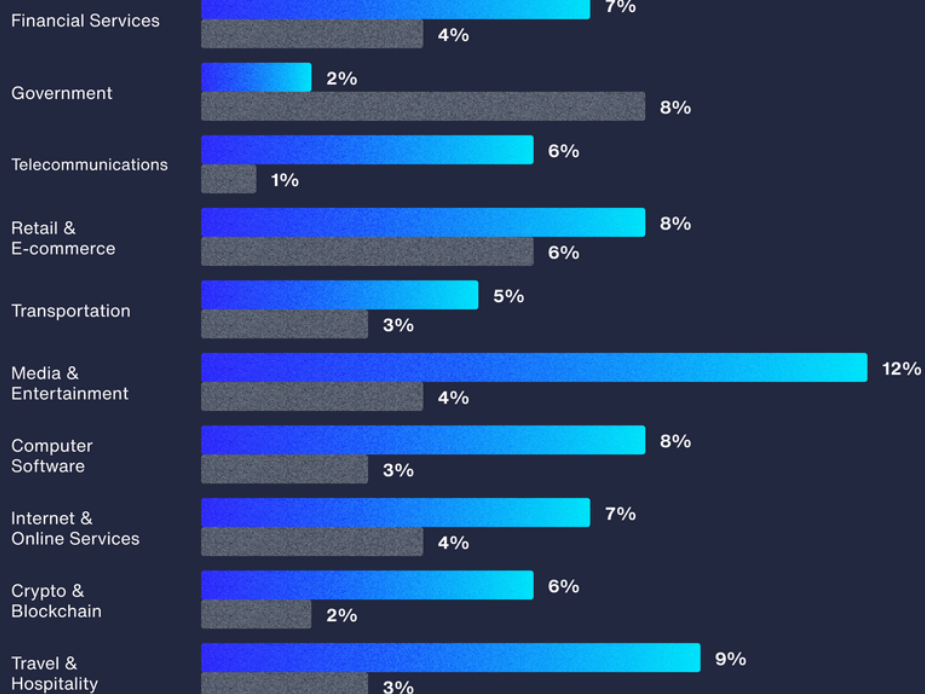
↑ 19% YOY increase

Percentage of total platform bounty rewards

4%

Average bounty payout

\$439



## Recommendations



Implement automated configuration management tools and create standardized patterns to maintain consistent and secure settings across the system.



Regularly perform security audits and reviews of system configurations and network architecture to identify and remediate any misconfigurations, unnecessary services, and open ports that could lead to security breaches.



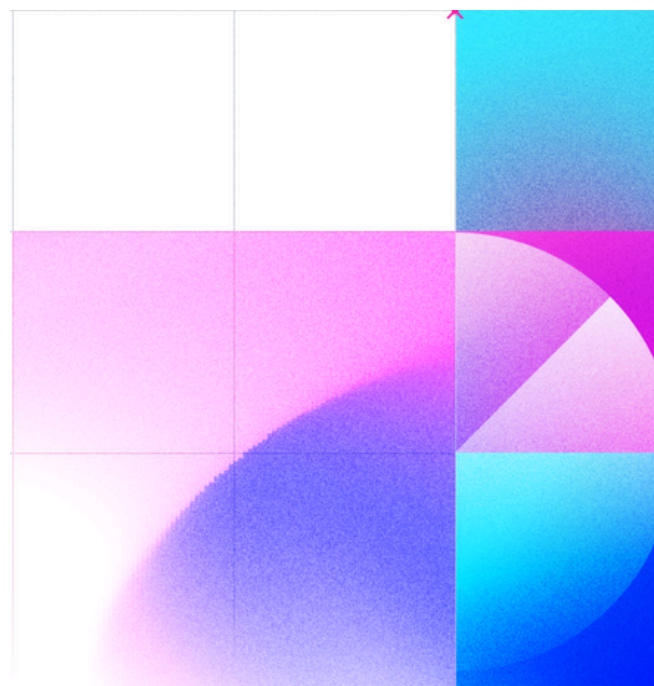
Implement a “least privilege” policy to restrict users, accounts, and computing processes' access to only the resources necessary for their legitimate functions.

# Computer Software

**Featured vulnerability:**  
Privilege escalation  
(down 2% from 2023)



While reports for privilege escalation are slightly down for the computer software industry, the sector still sees more reports for this vulnerability than the industry average. Software products often serve a range of user roles, from regular users to administrators, each needing different access levels. Inconsistent permission checks, especially in enterprise software, can open the door for attackers to escalate privileges. The use of open-source libraries and third-party dependencies adds to the risk if these components have privilege escalation vulnerabilities or are misconfigured. Tracking security issues in third-party code can be tough, leading to more reported vulnerabilities. Plus, maintaining secure privilege management across different platforms like Windows, Linux, and macOS, each with its own security model, further increases the risk of privilege escalation vulnerabilities.



## Privilege Escalation

Percentage of total reports Percentage of total bounty rewards

Percentage of total platform reports

2%

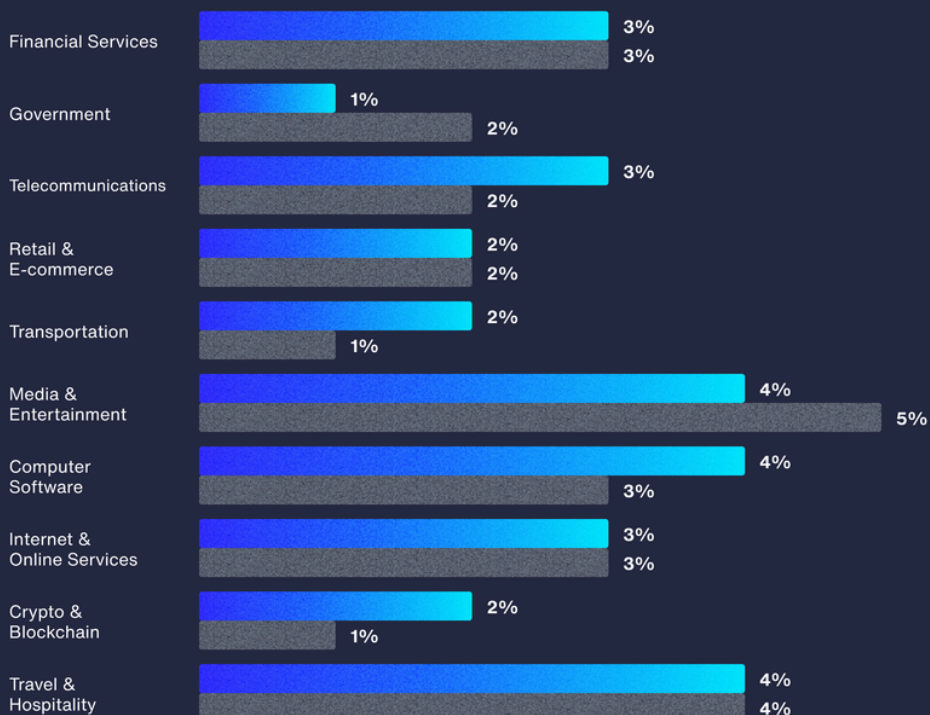
↓ 38% YOY decrease

Percentage of total platform bounty rewards

5%

Average bounty payout

\$1,550

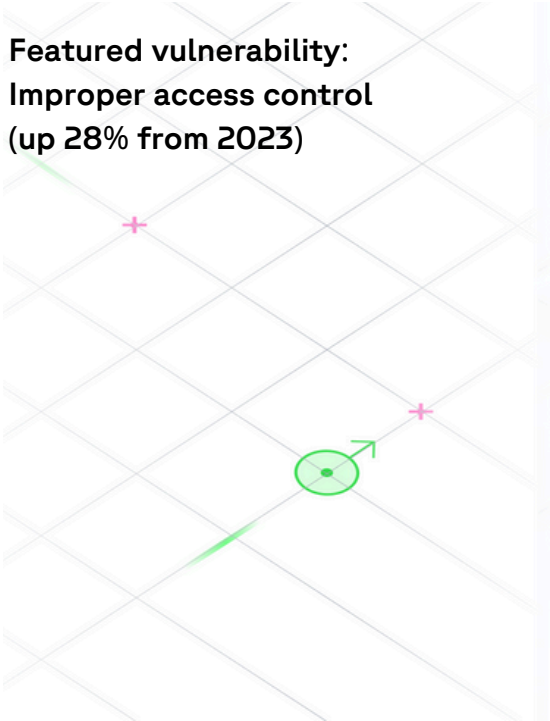


## Recommendations

- ✓ Implement the “least privilege” policy and role-based access control (RBAC) to restrict user permissions, ensuring access is limited to necessary resources based on specific roles.
- ✓ Implement security tools such as privileged access management (PAM) for granting access, and intrusion detection/intrusion prevention systems (IDS/IPS) for monitoring and alerting of any privilege misuse or anomalies.
- ✓ Keep your applications and systems up to date and perform regular security audits and prompt patching of software and dependencies to help address potential vulnerabilities.

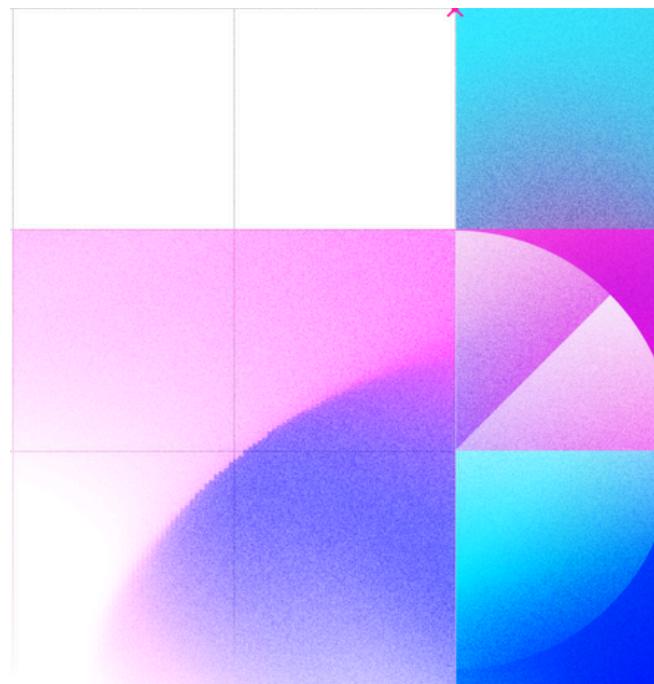
# Internet and Online Services

**Featured vulnerability:**  
**Improper access control**  
(up 28% from 2023)



In 2023, the technology sector suffered 33 breaches, impacting around 22.3 million victims.<sup>8</sup> Internet and online service companies see more improper access control vulnerabilities than average, mainly due to their complex, fast-changing systems. The push to scale quickly and roll out new features makes it tough to enforce strict access controls consistently. Agile development practices, with continuous integration and deployment, often prioritize speed and innovation over rigorous security checks, which can lead to access control vulnerabilities slipping through.

<sup>8</sup> [SANS 2023 Attack and Threat Report](#).



## Improper Access Control

Percentage of total reports Percentage of total bounty rewards

Percentage of total platform reports

9%

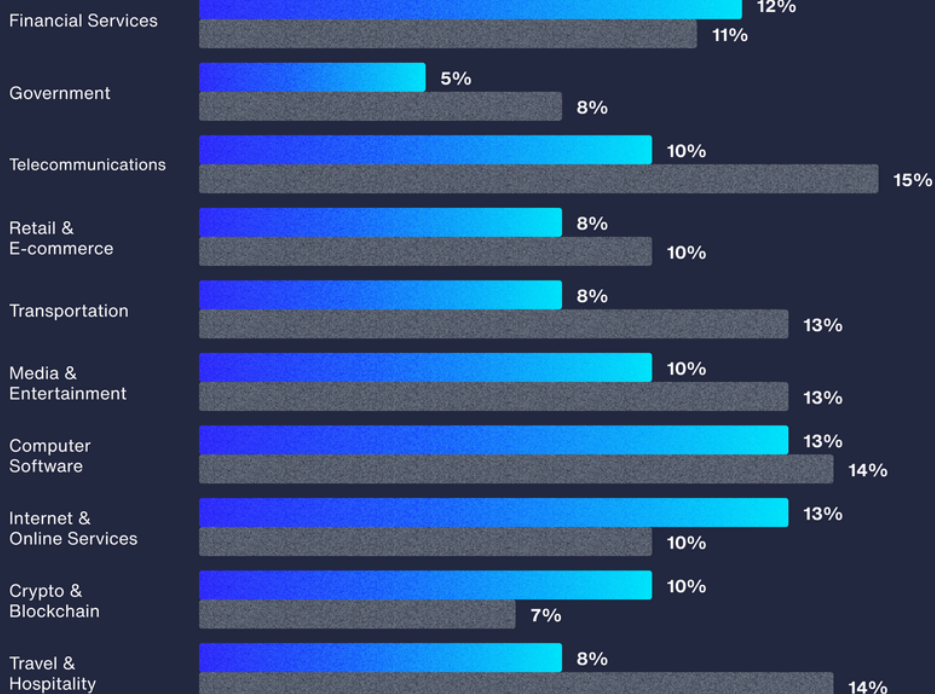
↓ 5% YOY decrease

Percentage of total platform bounty rewards

12%

Average bounty payout

\$930



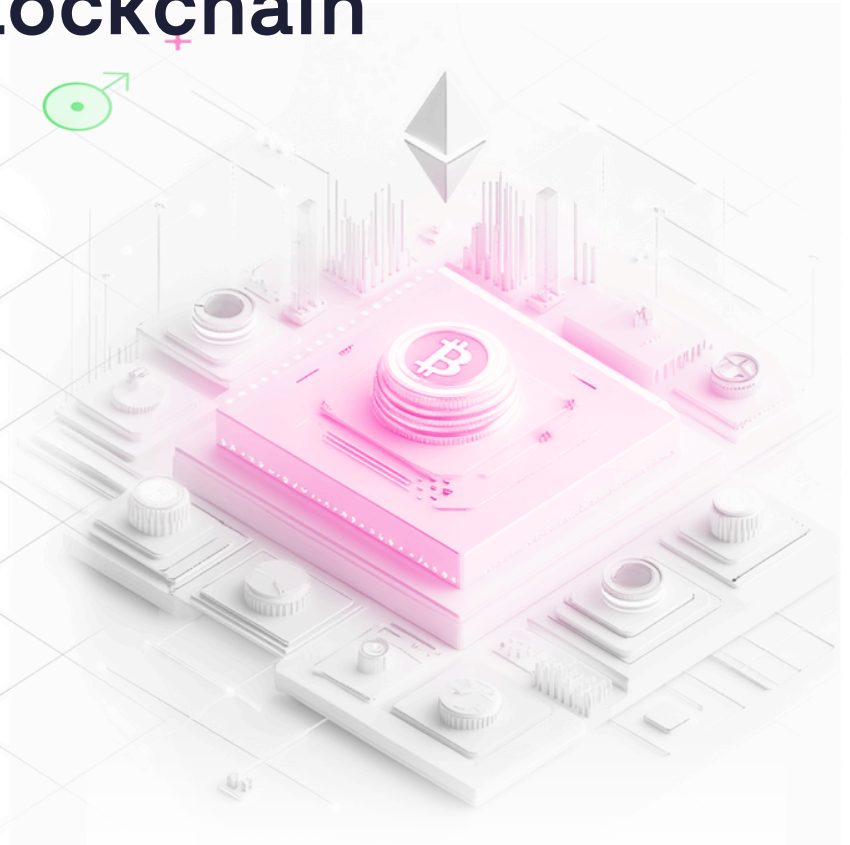
## Recommendations

- ✓ Define and enforce user roles and permissions using role-based access control (RBAC). Use the “least privilege” principle to grant users and systems the minimum level of access they require to perform their functions.
- ✓ Use multi-factor authentication (MFA) for secure access. Re-authenticate users when executing sensitive functions.
- ✓ Ensure proper session management is implemented by using secure cookies, expiring sessions appropriately, and avoiding persistent tokens unless necessary.

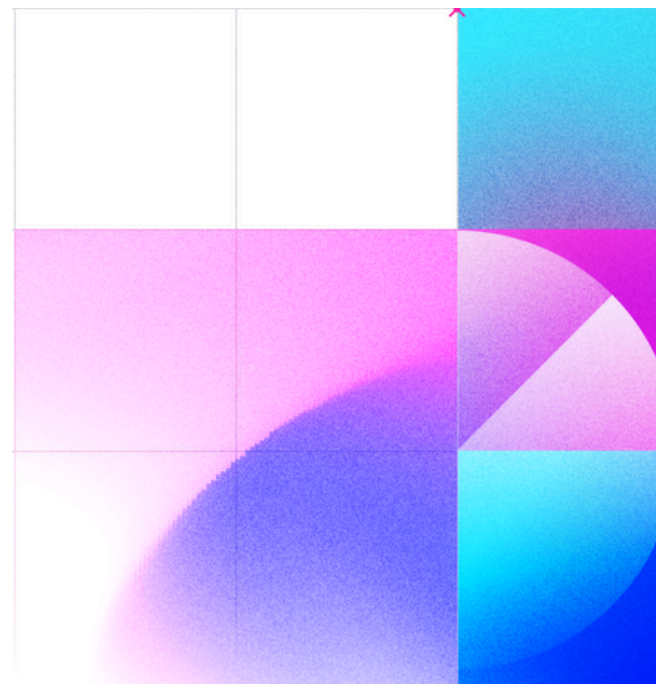
# Crypto and Blockchain

## Featured vulnerability:

Business logic errors  
(up 37% from 2023)



Crypto and blockchain organizations stand out for their many outliers, mainly due to the unique nature of their technology and operations. These companies prioritize security because they handle sensitive financial transactions and digital assets, often building rigorous security practices from the start. One major outlier is the high rate of business logic errors compared to the cross-industry average. With their complex, experimental business models and intricate transaction mechanisms, it's tough to secure against edge cases or unintended uses. For example, smart contracts, which run on the blockchain and execute automatically, are immutable once deployed—meaning any flaws or logic errors are hard to fix. These vulnerabilities can lead to financial loss, making them prime targets for bug bounty hunters.



## Business Logic Errors

Percentage of total reports Percentage of total bounty rewards

Percentage of total platform reports

2%

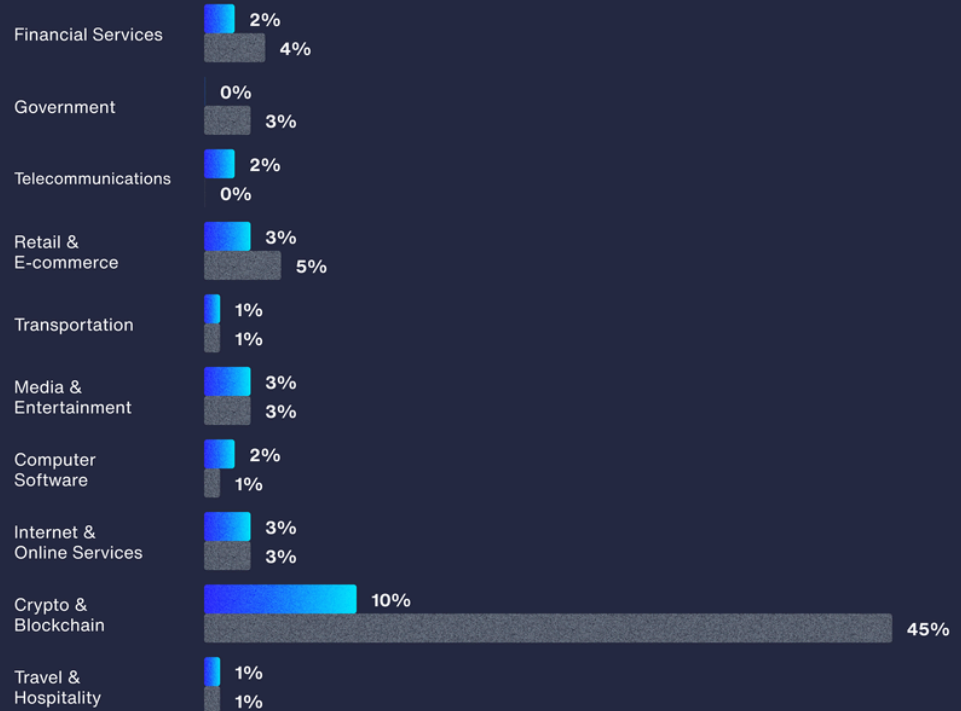
↑ 5% YOY increase

Percentage of total platform bounty rewards

4%

Average bounty payout

\$1,293



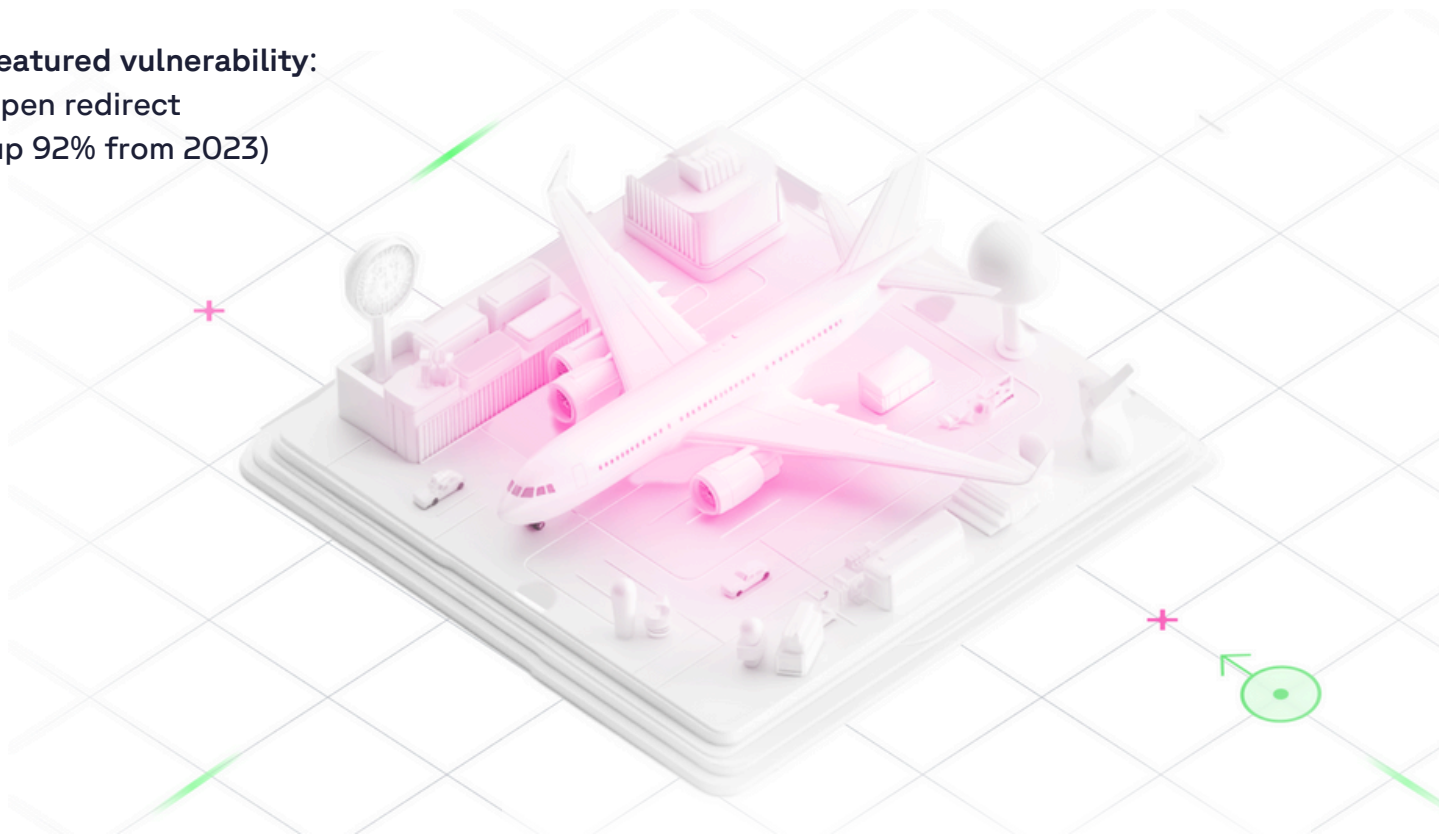
## Recommendations

- ✓ Use test-driven development (TDD) and extensive unit and integration testing to simulate various scenarios and edge cases.
- ✓ Enforce multi-signature requirements for critical operations to reduce the risk of flawed transactions.
- ✓ Design smart contracts with role-based modules to isolate critical operations, ensuring that only authorized users or entities can execute high-risk functions.

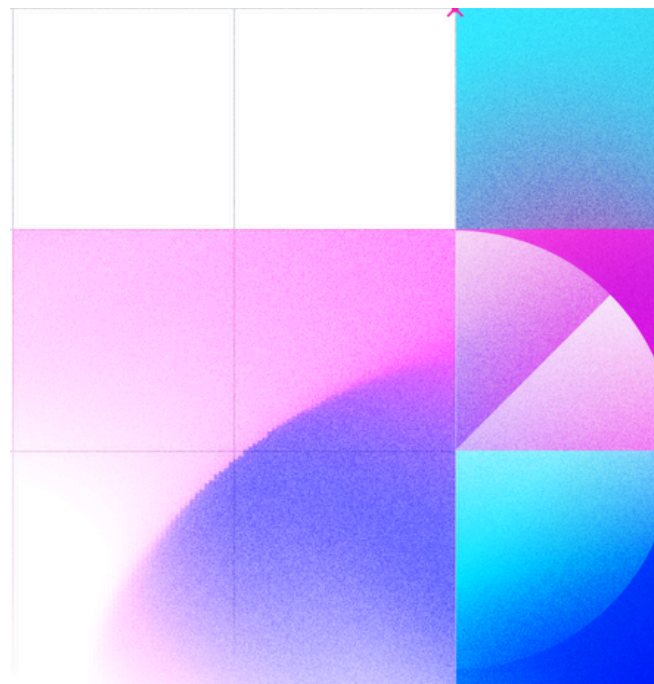
# Travel and Hospitality

## Featured vulnerability:

Open redirect  
(up 92% from 2023)



Travel and hospitality organizations rely heavily on marketing, often embedding referral and affiliate links. Attackers may exploit open redirect vulnerabilities by tampering with these links to lead users to malicious sites. This industry's focus on seamless navigation between internal and external sites can compromise security checks on redirection mechanisms. Additionally, integrations with third-party services like booking systems, payment gateways, and ads can increase the risk of open redirect vulnerabilities if user inputs, such as URLs, are not properly validated.



## Open Redirect

Percentage of total reports Percentage of total bounty rewards

Percentage of total platform reports

2%

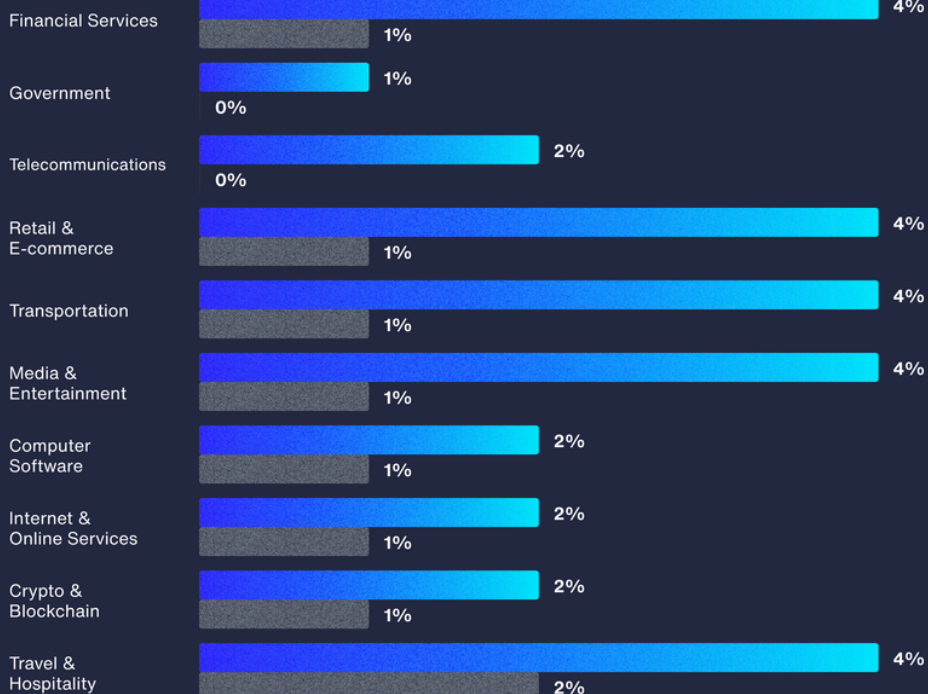
↑ 10% YOY increase

Percentage of total platform bounty rewards

1%

Average bounty payout

\$241



## Recommendations

- ✓ Implement input validation and sanitization for all user inputs and avoid using user-controllable data in URLs.
- ✓ Provide clear warning for all redirects, notify users they are leaving the site, display the destination, and require a confirmation click.
- ✓ Sanitize input by creating a list of trusted URLs (lists of hosts or a regex). Implement the use of an allow list rather than a deny list.

# 63% of your bounty budget will be spent on the top ten

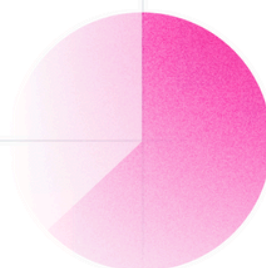
The vulnerabilities organizations allocate their budgets to don't always align with the volume of reports for those vulnerabilities.

For example, even though open redirects rank among the top ten reported issues on the HackerOne Platform, they account for only a small slice of bounty budgets.

This is because open redirects are seen as lower risk compared to more severe vulnerabilities like remote code execution, SQL injection, and privilege escalation. With low exploitability, open redirects rarely lead to sensitive data exposure on their own.

# 63%

of your bounty budget will be spent on the top 10 common vulnerabilities



In contrast, organizations allocate a larger share of their budgets to indirect object reference (IDOR) vulnerabilities due to their potential for unauthorized access, modification, or deletion of sensitive data. IDORs often have a much higher impact and severity compared to other issues, as they can lead to large-scale breaches of personally identifiable information (PII). With high exploitability, they expose data like user profiles, financial records, or confidential documents, carrying legal risks, including GDPR violations. This makes IDORs a top priority for organizations, resulting in higher payouts for valid reports.

## Recommendations

- ✓ Identify the critical systems, applications, and data that will be in scope for the program, prioritizing high-value assets.
- ✓ As your program evolves, monitor report volume, payout levels, and researcher feedback to adjust budgets over time.
- ✓ Prepare for unexpected high-severity vulnerabilities by having a buffer in the budget for critical vulnerabilities that may require higher-than-anticipated payouts, ensuring that you can address major security threats without financial constraints.

# The Best Defense Has Layers of Depth

Strengthen your security posture proactively.

## Continuous Vulnerability Discovery

### Secure by design

Secure-by-default frameworks and liabilities

### Automated testing

Analysis on code changes and live applications

### Secure code review

Human-led auditing of your code base

### Penetration testing

Frequent testing to validate coverage

### Bug bounty

Continuous testing by security experts

 HackerOne Response

 HackerOne Code Security Audit

 HackerOne Pentest

 HackerOne Challenge

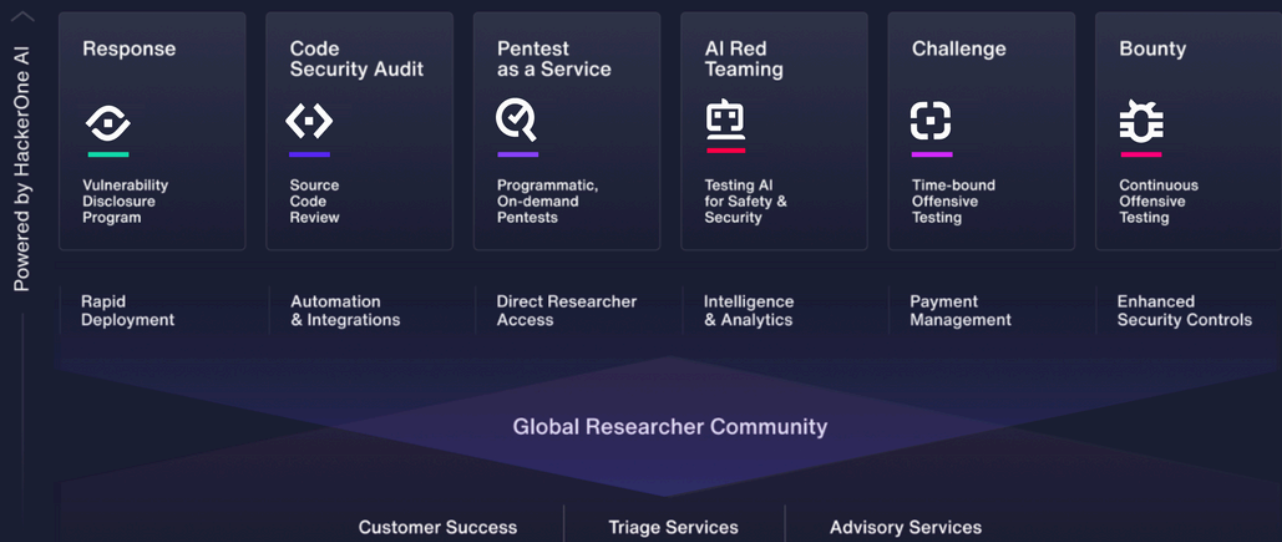
 HackerOne AI Red Teaming

 HackerOne Bounty

We believe the best security programs are built around a defense-in-depth strategy. Our goal is to empower organizations to continually strengthen every layer of their security posture.

HackerOne's approach to offensive security ensures continuous vulnerability detection throughout the SDLC, maximizing coverage from the earliest stages of development through deployment and beyond.

Each layer in this approach is not just a step in the process but a critical element on its own, offering unique insights that enhance your overall security posture. These insights create a continuous feedback loop, where findings from one layer inform and refine the effectiveness of the others. This iterative process ensures that your security strategy is always evolving, becoming more robust and adaptive over time.



*"Working with HackerOne, we have had a solid return on investment while reducing risk. Zebra has scaled our security program across the different product offerings within HackerOne, from security assessments for product releases, bug bounty for continuous testing, and a mechanism for third-party security researchers to submit vulnerabilities. The ability to log into a platform portal, receive a notification when a vulnerability is reported, and remediate bugs in the same workflow allows us to be efficient in our approach to risk management."*

**Dr. Jasyn Voshell**

Director of Product Security, Zebra Technologies





# Bug Bounties and Pentests Prove: Vulnerability Discovery Is Key to Every Stage of Development

Pentest as a Service (PTaaS) is gaining momentum as organizations shift to community-driven, SaaS-based models that offer greater flexibility, access to a diverse pool of vetted security researchers, and wider coverage than traditional methods. At HackerOne, we've seen a 67% increase in pentesting over the past year, with rapid start times—often within a week.

HackerOne pentests uncover an average of 12 vulnerabilities per engagement, with 16% classified as high or critical, demonstrating the effectiveness of community-driven pentesting in detecting critical vulnerabilities before deployment. Combined with HackerOne's bug bounty programs, which report 25% of findings as high or critical, this approach ensures comprehensive security coverage.



*“We’re a highly regulated market, so we have to run pentests. But the more we onboarded onto our bug bounty program, the more we see there are issues we haven’t found before—and they’re introduced all the time. When applications are updated, we can say we did our due diligence, but we also have hackers looking at it around the clock. It’s incredible, and we find bugs all year round now.”*

**Alex Hagenah**

Head of Cyber Controls, SIX Group

Pentests tend to identify systemic or architectural vulnerabilities, such as cryptographic weaknesses or secure design issues, which are essential for long-term security but may not be immediately apparent to attackers. In contrast, bug bounty programs focus on real-world attack vectors, targeting user-level issues like privilege escalation and business logic flaws. This explains the frequent discovery of privilege escalation and authentication issues in bug bounties compared to pentests.

The integration of findings from both bug bounties and pentests into the software development life cycle (SDLC) highlights the need for continuous vulnerability assessment.

Notably, 42% of organizations report discovering the most critical bugs during the deployment phase when pentests often reveal systemic issues. Together, pentesting and bug bounties provide comprehensive security coverage, reinforcing resilience across all development stages.

**At which stages of your software development life cycle (SDLC) do you typically observe the most critical bugs? (Select up to three.)**

**32%**  
Design

**34%**  
Testing

**38%**  
Requirements  
and Planning

**34%**  
Implementation  
(Coding)

**38%**  
Maintenance

**42%**  
Deployment

## Recommendations

- ✓ Define clear scopes for your PTaaS and bounty program so they complement each other rather than overlap. Use PTaaS for scheduled, structured assessments of high-priority systems and bug bounty for continuous, exploratory testing across a broader range of assets.
- ✓ Centralize reporting and communication to track vulnerabilities from both programs and avoid duplicate efforts by ensuring both sets of testers can see past reports and updates, making it easier and more transparent for your internal teams, as well.
- ✓ Rotate pentesters to bring fresh eyes and perspectives to each assessment. Keep bug bounty always on to ensure 24x7, continuous testing by diverse security researchers.

# Measuring Success: Invest in Return on Mitigation

Data breach costs are more significant than ever, seeing a 10% year-over-year rise in the global average, now at \$4.88 million—the largest increase since the pandemic.<sup>9</sup> A major driver of this is the growing shortage of security staff, with over half of breached organizations reporting this issue—a 26% jump from last year. This shortage adds an average of \$1.76 million to the overall breach cost.

In contrast, even top-tier bounty payouts in the 95th percentile are relatively small investments. However, many organizations still struggle to measure the ROI of proactive security measures like bug bounty programs. Securing budget for these initiatives often requires stakeholder buy-in, which means translating bug bounty success into clear financial value.

<sup>9</sup> IBM. [Cost of a Data Breach Report 2024](#).

## How does your organization measure the ROI of its security programs?

	Our panel of security professionals	HackerOne customers
Absence of incidents or breaches	41%	57%
Risk assessment	39%	48%
Financial savings estimated from avoiding risk or avoiding breaches	37%	45%
Agility and speed of security teams responsiveness	36%	32%
Discount on cyber insurance	36%	9%
Estimated savings of reputational or customer-related impacts as a result of a security program	35%	45%



*“The bug bounty program is the highest ROI across all of our spend. It’s really hard to show ROI, but with bug bounty, I have a baseline. I can say, ‘This vulnerability was able to be found by someone outside the organization. Someone that was not authorized to access this system was able to access it.’ Even with vulnerabilities that are not within our program, bug bounty allows me to put a price tag on them. I can explain this business case and our stakeholders are able to prioritize bug bounty higher than other tools that also generate ROI.”*

**Eric Kieling**  
Head of Application Security, Booking.com

# Introducing Return on Mitigation

HackerOne recently introduced the concept of return on mitigation (ROM), an extension of ROI that is specific to cybersecurity. ROM compares the cost of mitigating risks to the potential financial losses from cyber incidents, providing a clear metric to measure how security efforts protect businesses from costly breaches.

ROM’s nuanced view offers both the qualitative and quantitative benefits of proactive security investments, considering factors including:

- Restoring compromised systems
- Lost revenue due to downtime
- Legal and regulatory penalties
- Damage to public trust and reputation

$$ROM = \frac{\text{Total mitigated losses} - \text{Cost of investment}}{\text{Cost of investment}} \times 100$$

ROM provides a practical framework for evaluating the true value of security investments by substituting net profit for mitigated losses. It shifts the focus from short-term cost savings to long-term resilience, highlighting the importance of risk management and the overall business benefits of proactive security measures.

Read more about the concept in the [SANS White Paper: Human-Powered Security Testing](#).

## Recommendations

- ✓ Track your response times, your ability to stay within your agreed SLAs to remediate vulnerabilities, and your time to bounty payout to understand the health of your program and efficacy of your processes.
- ✓ Understand the goals and success metrics of your different stakeholders, from engineering teams to the board, so you can align your reporting to their priorities and focus areas.
- ✓ Adopt a return-on-mitigation strategy to effectively put an avoided incident into financial terms.

*"Paying \$15k for a critical vulnerability that could cost us millions in the wild is the best discount."*

**Security Leader**  
Media & Entertainment Industry

“



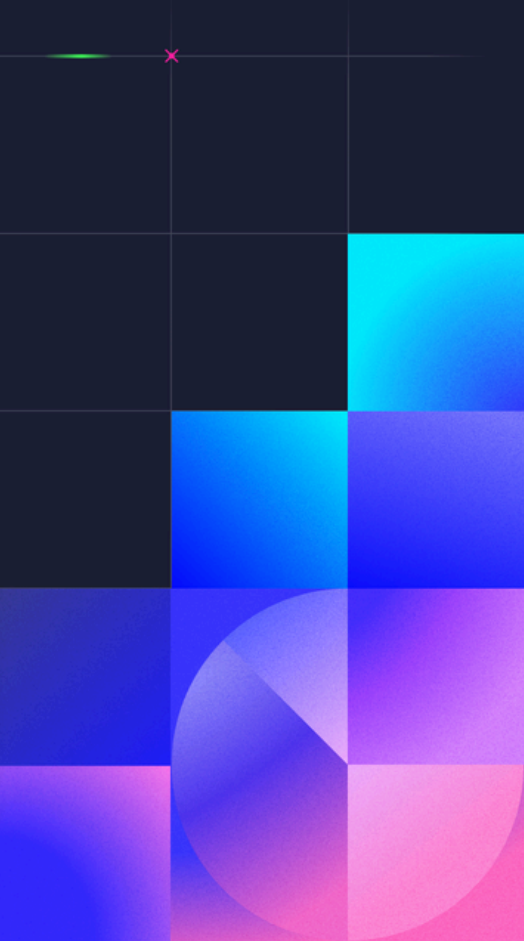
# Conclusion

We're seeing the maturation of human-powered security. The increasing trust that traditionally conservative industries and organizations are placing in the security researcher community is evident from the validation of government guidance, growing adoption of the model, and public promotion as a signifier of security best practices. The 8th Annual Hacker-Powered Security Report shows that as the security researcher community is diversifying in skills and experience, organizations will need to ensure they are maintaining researchers' focus and enthusiasm via accurate bounty tables, expanding scope, and a commitment to developing positive relationships.

The collaboration between researchers and organizations is resulting in more high and critical vulnerabilities discovered than ever before. However, a successful reduction of the most easily avoidable vulnerabilities is going to take a more concerted approach to examine which vulnerabilities are most prevalent in your organization, their causes, where they're introduced, and the tactics to phase them out of development. AI will likely play a significant role in elevating security teams' ability to manage vulnerability reports and fixes. Meanwhile, the researcher community will be crucial in ensuring the safety and integrity of the AI tools we're coming to rely on.

HackerOne is firmly behind these efforts and we strive for a safer internet where cross-site scripting and improper authentication are things of the past and instead our researchers are incentivized to maximize their human skill and creativity, finding the most novel and exclusive vulnerabilities.

**contact us**  
[sales@hackerone.com](mailto:sales@hackerone.com)



## Data Sources

HackerOne's annual community survey surveyed 2,321 security researchers that were active on the platform in the 30 days prior to the survey. *The survey took place between June 24, 2024, and August 4, 2024.*

The data collected from HackerOne's platform is from the period *between June 2023 and June 2024.*

HackerOne's customer survey was conducted via UserEvidence and surveyed 50 HackerOne customers *between July 15, 2024, and August 15, 2024.*

The survey of security professionals was conducted by Opinion Matters and surveyed 500 security professionals across the US and Europe. *The survey was conducted between July 31, 2024, and August 6, 2024.*

## About HackerOne

HackerOne is the global leader in human-powered, AI-enabled security, fueled by the creativity of the world's largest community of security researchers plus cutting-edge AI to protect your digital assets. The HackerOne Platform combines the expertise of our elite community and the most up-to-date vulnerability database to pinpoint critical security flaws across your attack surface. Our integrated solutions—including bug bounty, pentesting, code security audits, spot checks, and AI red teaming—ensure continuous vulnerability discovery and management throughout the software development life cycle. Trusted by industry leaders such as Coinbase, General Motors, GitHub, Goldman Sachs, Hyatt, PayPal, Snap Inc., and the U.S. Department of Defense, HackerOne was named a Best Workplace for Innovators by Fast Company in 2023 and a Most Loved Workplace for Young Professionals in 2024.

8th Edition-2024/2025

# Hacker-Powered Security Report



If you want to turn this data into real impact  
for your organization, speak to our experts

[sales@hackerone.com](mailto:sales@hackerone.com)

hackerone