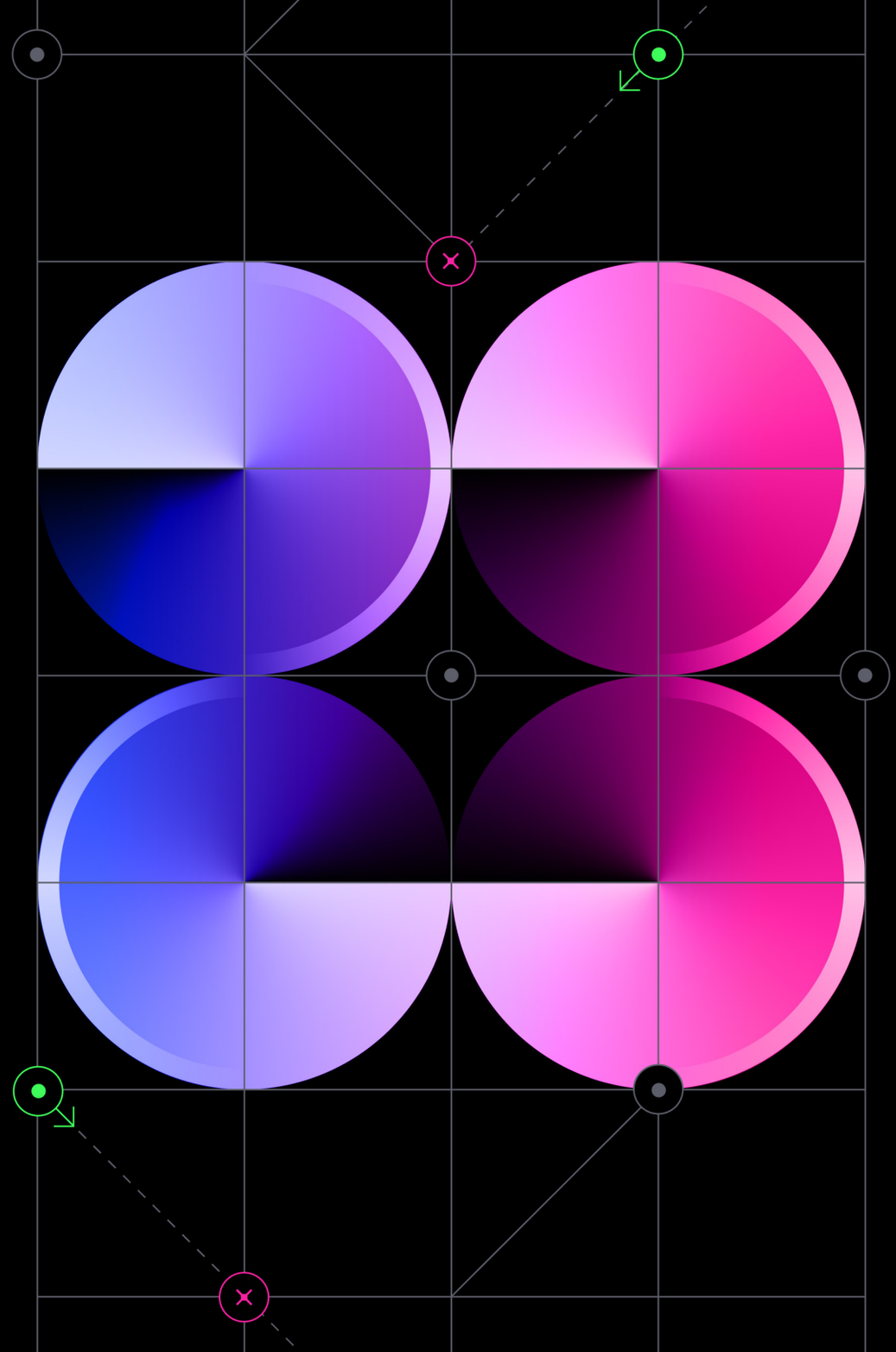
hackerone

Hacker-Powered Security Report

2023



Contents

Hack•er / *noun*

One who enjoys the intellectual challenge of creatively overcoming limitations.

It's Riskier Not to Work With Hackers

Cybercrime continues to rise at the same time CISOs are being challenged to do more with less. Research from early 2023[1] revealed that one-third of companies had made security budget cuts in the past 12 months and that a quarter were planning to make cuts in the following 12 months, with 40% saying they were planning to make headcount cuts in the same timeframe. Of the security professionals surveyed, 67% said they believed reducing budget and headcount in security would negatively affect their ability to handle cybersecurity incidents.

In this climate, you're more at risk if you're ignoring the benefits a huge community of talented and tenacious ethical hackers can bring to your organization's security. Thousands of the world's most influential brands trust hackers to deliver impactful findings and vulnerabilities.

[1] Survey conducted by CensusWide March 29-31, 2023. Censuswide abides by and employs members of the Market Research Society, which is based on the ESOMAR principles. Respondents include 100 US cybersecurity professionals aged 18+.

96%

of HackerOne customers say their organization is better positioned to resist cyberattacks

70%

of HackerOne customers say hacker efforts have helped them avoid a significant security incident

96% of HackerOne customers say their organization is better positioned to resist cyberattacks by accepting vulnerability reports from third parties, and 70% say hacker efforts have helped them avoid a significant security incident.

The 7th annual Hacker-Powered Security Report goes deeper than ever before with customer insights, in addition to the opinions of some of the world's top hackers. We also take a more comprehensive look at the top ten vulnerabilities and how various industries are performing when it comes to incentivizing hackers to find the vulnerabilities that are most important to them.

"The greatest challenge for businesses right now is the requirement to drive down rising costs while continuing to enhance security against an evolving threat landscape.... From an ROI perspective, bug bounty is one of the most effective programs in our security strategy."

Seema Sangari

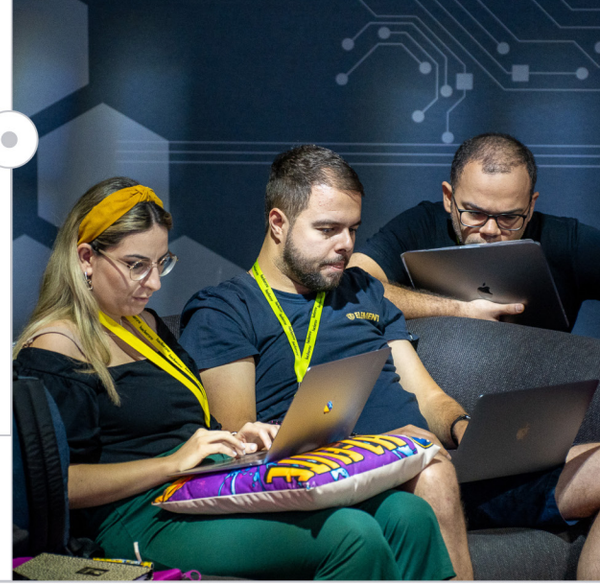
Vice President of Security Technical Program Management

salesforce

What You Will Learn From the Hacker-Powered Security Report

55%

of hackers say that generative AI (GenAI) tools themselves will become a major target for them in the coming years



How hackers are using AI and what they can tell you about the security risks

55% of hackers say that generative AI (GenAI) tools themselves will become a major target for them in the coming years, and 61% said they plan to use and develop hacking tools using GenAI to find more vulnerabilities. Another 62% of hackers said they plan to specialize in the OWASP Top 10 for Large Language Models (LLMs).

How to attract the top hackers to your program

While nondisclosure agreements (NDAs) remain a hot topic in the hacking community, only 9% of hackers say NDAs put them off hacking a target (down from 11% in 2022) and only 14% are put off by the inability to publicly disclose vulnerabilities (down from 17% in 2022), showing hackers' adaptability and willingness to work within these constraints.

How your industry compares against the top ten vulnerability stats and why your program may return different results than the HackerOne platform averages

When we look at the high and critical vulnerabilities compared against all vulnerability reports, we see a higher ranking for insecure direct object references (IDOR), for example, because these are not vulnerabilities you can scan for. This highlights the importance of human intelligence in seeking out these weaknesses.

How you can save money by incorporating code security audits and pentesting into your bug bounty strategy

A code security audit could save you a potential $18,000 on your bounty program.

The latest bounty data and how your median and top bounties stack up against your peers'

The median cost of a bug on the HackerOne platform is $500, the average cost is $1,048, and the 90th percentile is $3,000.

What Motivates Hackers to Find and Report Vulnerabilities

Only one-quarter of hackers hack full-time: nearly two-thirds of hackers spend less than 20 hours a week hacking. Almost one-third of hackers have day jobs in the cybersecurity industry.

One-quarter of hackers hack full-time

Nearly two-thirds of hackers spend less than 20 hours a week hacking

Almost one-third of hackers have day jobs in the cybersecurity industry

While hackers are always looking for generous bounties, they're motivated by more than just money:

80%

of hackers hack to earn money (up from 71% in 2022)

78%

of hackers also say they do it to learn

47%

of hackers say they hack to protect and defend businesses and end users

"Of course I'm motivated by money, but I also choose programs that offer great communication with the community."

Tom Anthony

Hacker

The Industries Hackers Focus On

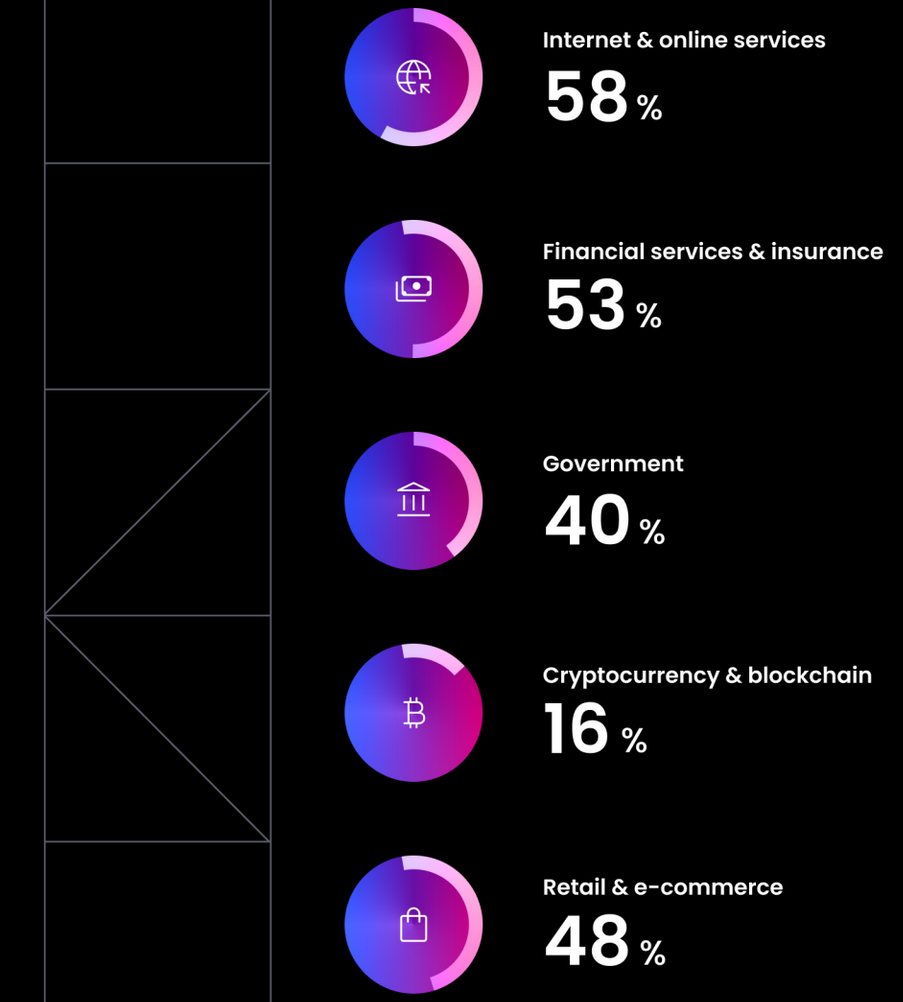
Internet and online services are a top target for hackers, with 58% spending time on programs in this realm. These organizations pay top bounties and are a dominant presence on the HackerOne platform, making up 25% of all customer programs.

Financial services is a growing sector, with 53% of hackers spending time on these organizations' programs, up from 44% in 2022.

40% of hackers now hack government organizations, up from 33% in 2022.

Conversely, cryptocurrency and blockchain, which had seen increased ethical hacker activity in prior years, now have fewer hackers focusing on them—down to 16% from 17% in 2022.

Retail and e-commerce platforms remain popular, with 48% of hackers spending time on them, but this is a decrease from 54% in 2022.

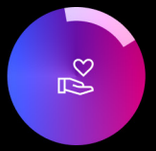


The Industries Hackers Focus On

Financial services & insurance
53%

Retail & e-commerce
48%

Cryptocurrency & blockchain
16%

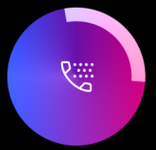


Non-profit
19%

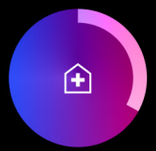
Government
40%

Media & entertainment
40%

Professional services
30%



Telecommunications
29%



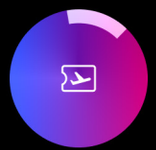
Healthcare
33%

Automotive & ground transport
19%

Computer hardware & peripherals
14%

Medical technology
24%

Computer software
43%

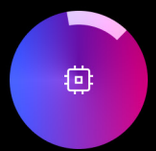


Aviation & aerospace
15%

Education
41%

Consumer goods
30%

Internet & online services
58%



Electronics & semiconductor
15%

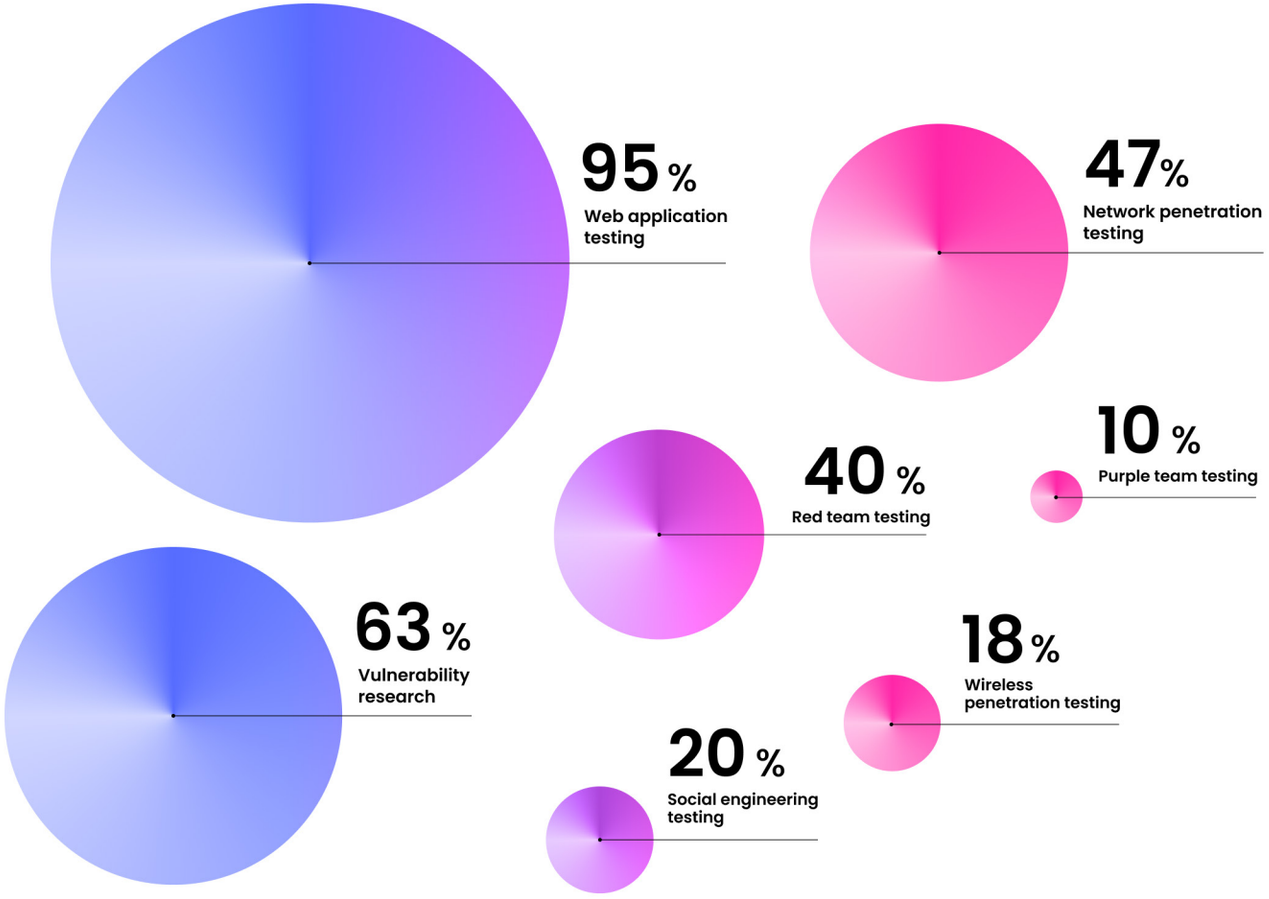
Travel & hospitality
32%

The Diverse Skill Sets of the Hacking Community

Hackers use a plethora of techniques; while 95% of hackers specialize in web application testing, they also span a range of new and emerging technologies. 47% specialize in network application testing, 20% have experience with social engineering, and 63% do vulnerability research. 36% of hackers say they are most skilled at the reconnaissance part of hacking, and 20% say they are best at exploitation.

"So many hackers specialize in web applications because the majority of internet interactions take place via web applications, meaning that hackers are already very familiar with their mechanisms. Moreover, the attack surface of web applications provides a particularly wide and rich testing ground, with organizations having huge sets of assets across the internet. I also specialize in social engineering. It's always fascinated me; instead of hacking technical systems, we're trying to open a window into the human mindset. While it seems that our brain is immensely more complex than a computer, social engineering is the easiest way for a malicious actor to reach their target. Social engineering is more challenging to run as an ethical hacking exercise since the hacker needs to have an understanding of psychology and sociology, while also understanding the ethics behind any assessment."

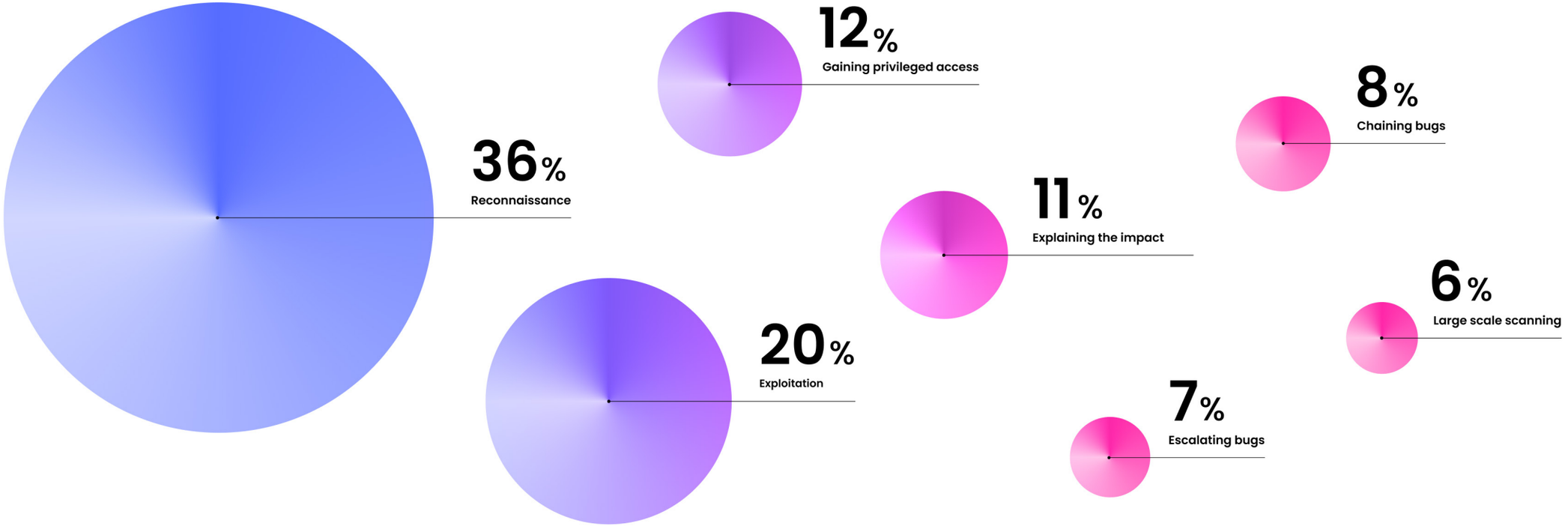
Roni Carta a.k.a. @arsene_lupin
Hacker and co-founder of Lupin & Holmes



Where Hackers Consider Themselves Most Skilled

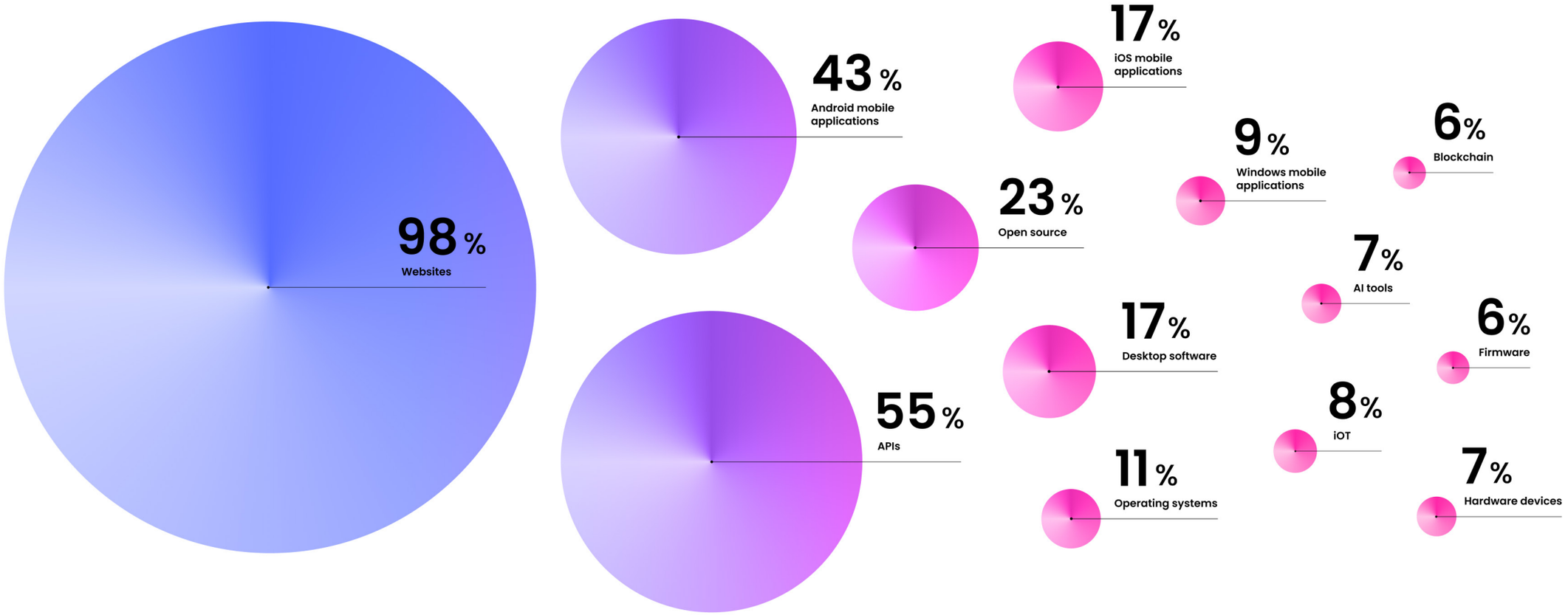
36%

of hackers consider themselves most skilled in reconnaissance



Where Hackers Focus Their Efforts

When it comes to the different types of technologies and applications that hackers specialize in, websites are still a key target. 98% of hackers say they hack websites, 17% hack iOS applications (up from 15% in 2022), and 43% hack Android applications (up from 39% in 2022). Eight percent specialize in IoT technology, and, with the explosion of GenAI in the past year, 7% of hackers now specialize in these tools, while blockchain specialization is down to 6% (compared to 8% in 2022).



What Hackers Can Tell You About Securing AI

The pressure to rapidly adopt generative artificial intelligence to boost productivity and remain competitive has ramped up to an incredible level. Concurrently, security leaders are trying to understand how to leverage GenAI technology while ensuring protection from inherent security issues and threats. This challenge includes staying ahead of adversaries who may discover and exploit malicious uses before organizations can address them. Ethical hackers have been experimenting with GenAI since 2022 and are already becoming the experts you need on your side.

- GenAI has become a "significant tool" for 14% of hackers, and 53% of hackers are using it in some way.
- 66% of hackers said that they do or will use GenAI to write better reports, 53% say they will use it to write code, and 33% say they will use it to reduce language barriers.
- 55% of hackers say that GenAI tools themselves will become a major target for them in the coming years, and 61% said they plan to use and develop hacking tools that employ GenAI to find more vulnerabilities. Another 62% of hackers said they plan to specialize in the OWASP Top 10 for Large Language Models.
- When we asked hackers to rank their concerns about the risks GenAI poses, 28% were most concerned about criminal exploitation of the tool, 22% about disinformation, and 18% about an increase in insecure code.
- While 38% of hackers say they think GenAI will reduce the number of vulnerabilities in code, 43% say it will lead to an increase in vulnerabilities. Find out more in our blog post on the potential risks GenAI poses.

53%

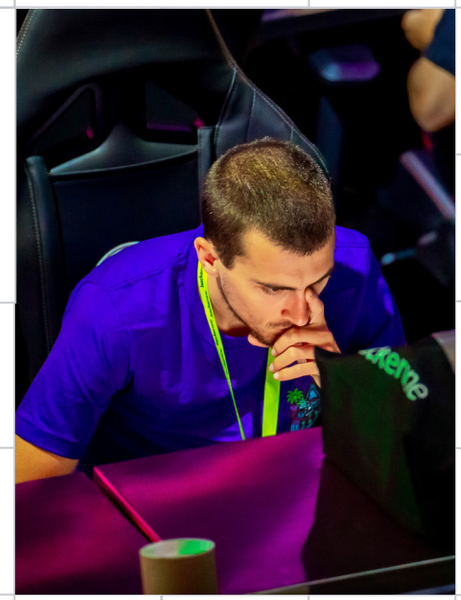
of hackers are using GenAI in some way

28%

of hackers are concerned about criminal exploitation of AI

66%

of hackers said that they do or will use GenAI to write better reports



"There are now suddenly a whole host of attack vectors for AI-powered applications that weren't possible before. At the simplest level, it's about tricking the AI into doing or revealing something it shouldn't. For example, chatbots often have access to company documentation and frequently asked questions. You want the responses to be able to answer users' questions intelligently but not completely siphon off internal documentation or leak data. Accidental exposure of internal documentation is a very possible attack scenario. One of the reasons for AI security issues is that these applications are new and developing really fast; they don't necessarily take security very seriously. I've spent a lot of time this year looking for those security issues and reporting them to the development teams.

The big companies that are creating their own versions of AI tools are more likely to bake security in because they already have a culture that prioritizes security. Hackers are also more likely to be given alpha or beta access to these tools so they can see it first and reveal those vulnerabilities before it goes out the door. From the hacker side, we're experimenting with using AI to write tools that will help us hack better, but the AI models are getting harder to convince to help with that. However, I think that to be able to compete with the malicious actors, we need access to the same tools and techniques."

Joseph Thacker, aka @rez0
Hacker specializing in AI

The OWASP Top Ten Vulnerabilities for Large Language Models

OWASP has already published their top ten vulnerabilities for LLM applications. Check out the HackerOne blog for more information about these vulnerabilities.

#1 Prompt injection

The most commonly discussed LLM vulnerability, in which an attacker manipulates the operation of a trusted LLM through crafted inputs, either directly or indirectly.

#2 Insecure output handling

Occurs when an LLM output is accepted without scrutiny, potentially exposing backend systems. This can, in some cases, lead to severe consequences like XSS, CSRF, SSRF, privilege escalation, or remote code execution.

#3 Training data poisoning

Refers to the manipulation of data or fine-tuning of processes that introduce vulnerabilities, backdoors, or biases and could compromise the model's security, effectiveness, or ethical behavior.

#4 Model denial of service

Happens when attackers trigger resource-heavy operations on LLMs, leading to service degradation or high costs.

#5 Supply chain vulnerabilities

The supply chain in LLMs can be vulnerable, impacting the integrity of training data, machine learning (ML) models, and deployment platforms. Supply chain vulnerabilities in LLMs can lead to biased outcomes, security breaches, and even complete system failures.

#6 Sensitive information disclosure

Happens when LLMs inadvertently reveal confidential data, resulting in the exposure of proprietary algorithms, intellectual property, and private or personal information, leading to privacy violations and other security breaches.

#7 Insecure plugin design

The power and usefulness of LLMs can be extended with plugins. However, this does come with the risk of introducing more vulnerable attack surfaces through poor or insecure plugin design.

#8 Excessive agency

Typically caused by excessive functionality, permissions, and/or autonomy. One or more of these factors enables damaging actions to be performed in response to unexpected or ambiguous outputs from an LLM.

#9 Overreliance

When systems or people depend on LLMs for decision-making or content generation without sufficient oversight. Organizations and the individuals that comprise them can over-rely on LLMs without the knowledge and validation mechanisms required to ensure information is accurate, vetted, and secure.

#10 Model theft

Where there is unauthorized access, copying, or exfiltration of proprietary LLM models. This can lead to economic loss, reputational damage, and unauthorized access to highly sensitive data.

What Are Your Biggest Security Risks?

We asked customers where they thought their biggest risks came from. 57% of customers said the greatest threat to their organization is exploited vulnerabilities. 10% said nation-state actors, 22% said phishing, and 12% said insider threats.

We also asked hackers what they think are the biggest security challenges organizations face. Lack of in-house skills and expertise was the top response, with 32% saying this was the biggest challenge. 91% of HackerOne customers say that hackers provide more impactful and valuable vulnerability reports than AI or scanning solutions.

What is your organization most concerned about?

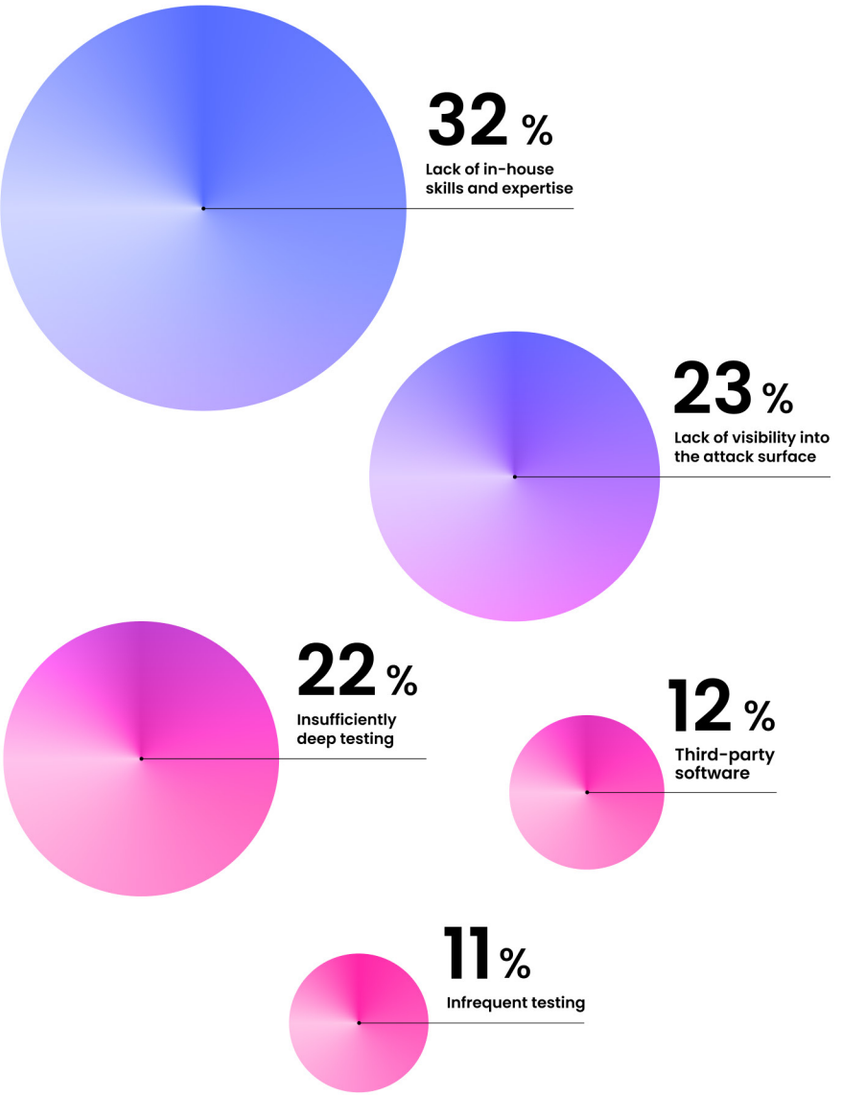
9%
Nation-state actors

20%
Phishing

59%
Exploited vulnerabilities

13%
Insider threats

What are organizations biggest security risks according to hackers?



How to Keep Hackers Motivated for the Best Results

Whether you're running a bug bounty, pentest, or code security audit program, you benefit by attracting the best hackers to participate. We asked hackers what makes for a program they want to hack on.

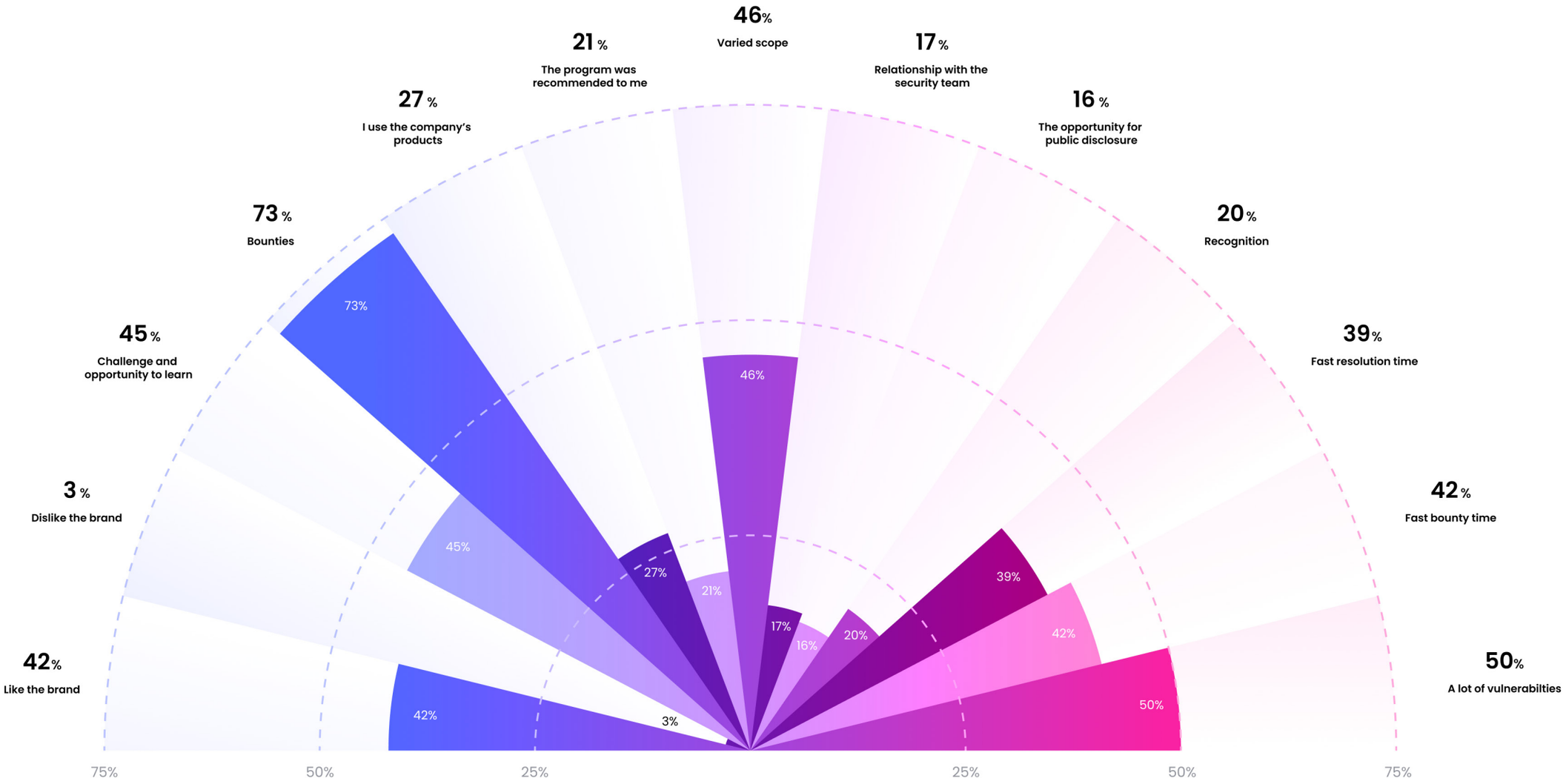
Bounties are the main attraction to a program, with 73% choosing a program because it pays generous bounties. However, other attractive factors include the anticipation that a lot of vulnerabilities will be available to find on a target (50% of hackers named this), and a varied scope (which attracts 46% of hackers). 17% of hackers will spend time on a program due to the relationship they have with the organization's security team.

When it comes to turning hackers off a program, it's all about the experience; poor communication puts off 55% of hackers and slow response times put off 60%. Just 9% of hackers say NDAs disincentivize them to hack a target, and only 14% are put off by a prohibition on publicly disclosing vulnerabilities they find. Both of those numbers are down slightly from 2022. These numbers illustrate the adaptability of hackers—and the viability of ethical hackers as a solution even for organizations that may require these common legal and disclosure restraints.

"When I'm looking at a new program, I will look at the metrics in terms of time to triage and bounty and to what degree the program is hitting those metrics. I would advise companies to have both a public and private program. The public program, will screen and interview researchers that can be moved into the private program where you can provide them with more access and resources. A private program allows you to have an elite group of hackers really digging in and finding those critical vulnerabilities. For example, some hackers specialize in reconnaissance and finding those corners of infrastructure that no one is thinking about and looking in the corners, then you have other hackers that have hundreds of servers scanning for vulnerabilities. Novelty and scale are important for delivering impactful reports."

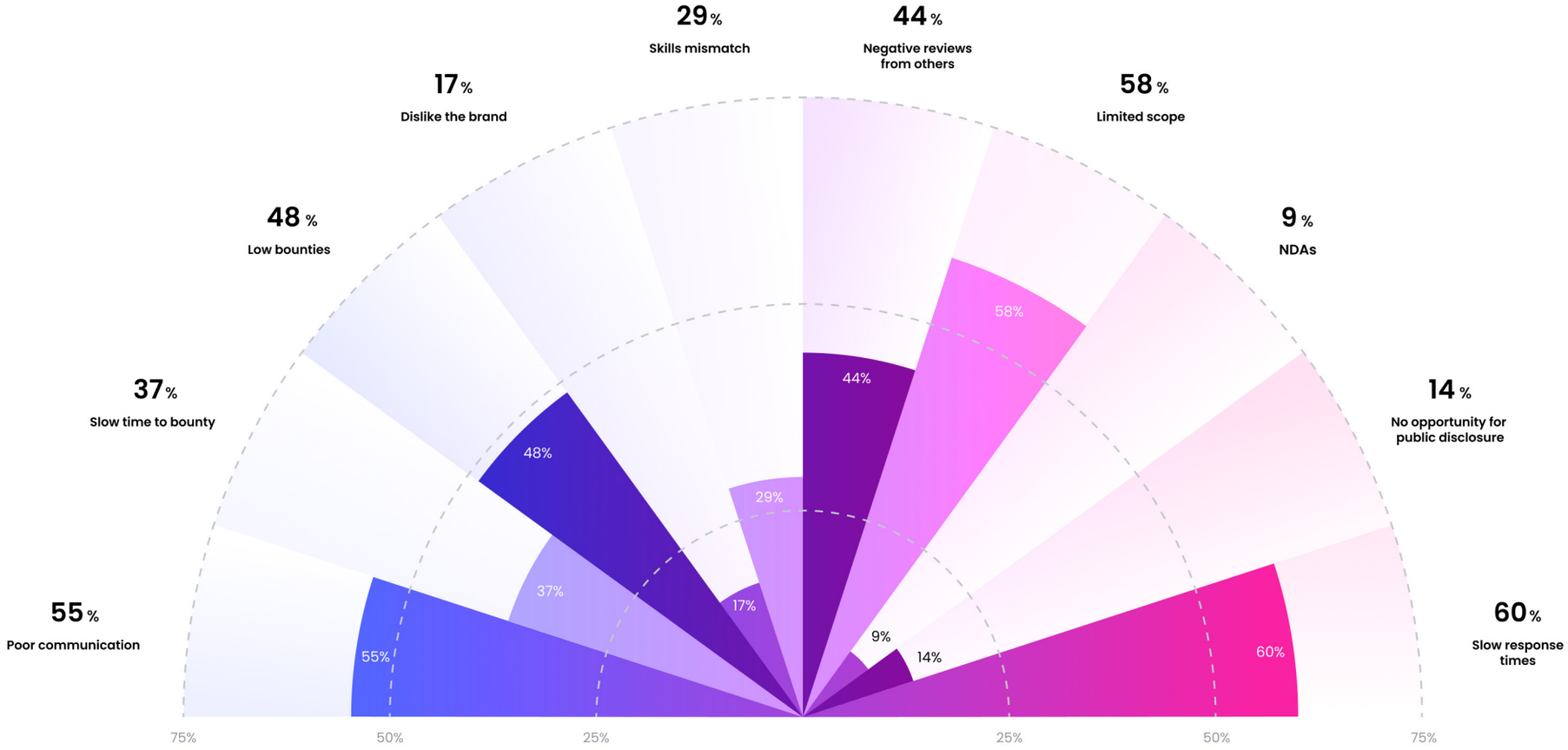
Tom Anthony
Hacker

Why Hackers Choose a Particular Program



What Puts Hackers Off a Program

The number of hackers who have not disclosed a vulnerability they've found declined to 46%, down from 51% in 2022. Of the hackers that have held back on a disclosure, 45% said it was because there was no channel through which to disclose. 13% cited threatening legal language on an organization's website as the reason they didn't disclose the vulnerability. There remains a critical need for organizations to establish clear, accessible, and well-communicated vulnerability disclosure policies and mechanisms to ensure vulnerabilities are reported and addressed promptly.



How Much Can You Expect to Pay for a Bug?

The median price of a bug on the HackerOne platform is $500, up from $400 in 2022. The average bounty in the 90th percentile is up from $2,500 to $3,000. The automotive industry, which is just emerging on the HackerOne platform, has seen the largest increase in bounties. As security leaders in this sector gain understanding and confidence in ethical hacking, hackers are increasingly incentivized to seek out impactful bugs.

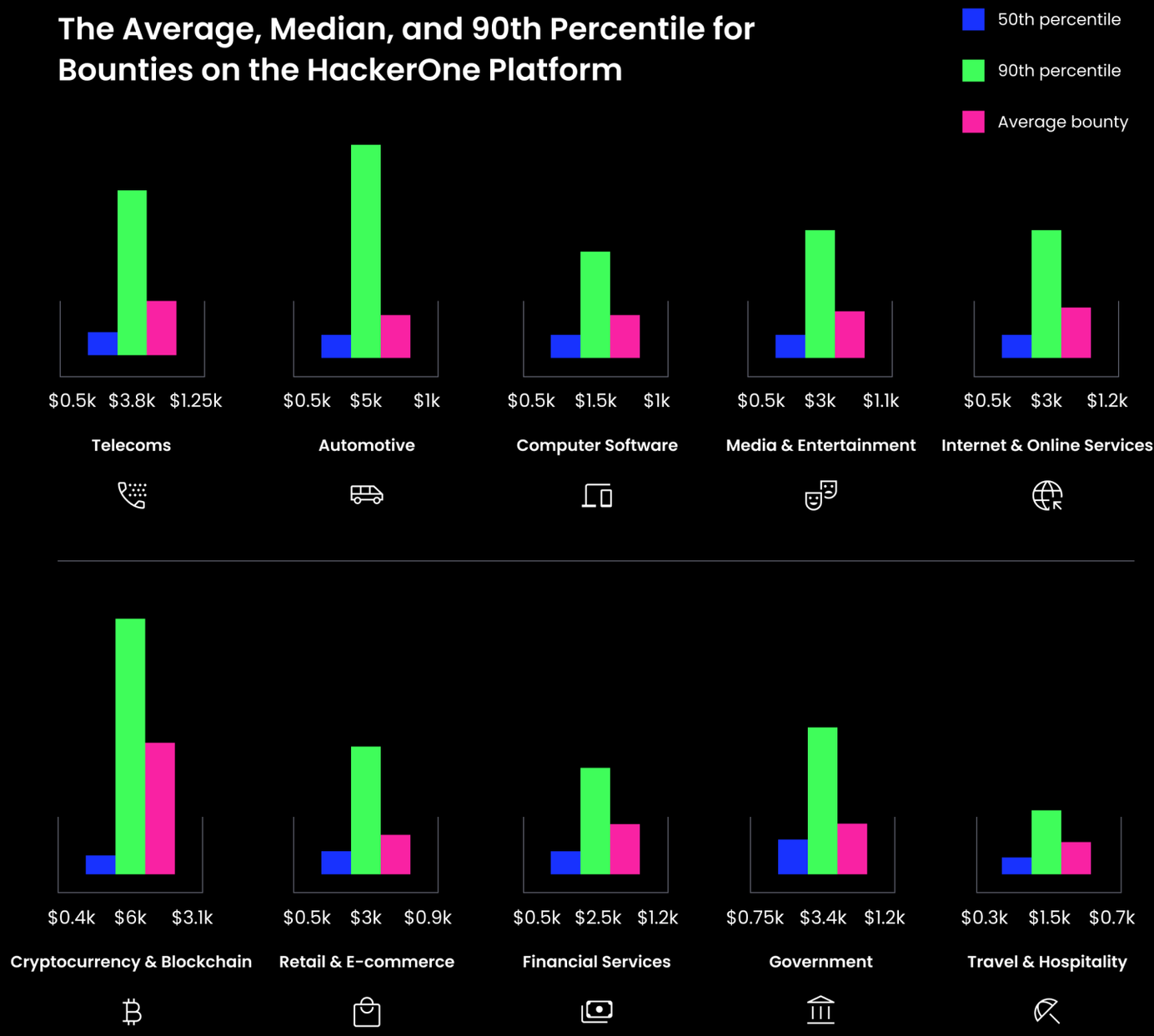
$1k

Average bounty for all industries

$3k

90th percentile average for all industries

The Average, Median, and 90th Percentile for Bounties on the HackerOne Platform



How Much Can You Expect to Pay for a Bug?

Things get more interesting when we break down bounties by high and critical vulnerabilities. Crypto and blockchain organizations continue to pay the highest bounties, with the top award reaching $100,050 in this industry. Computer software and internet and online services are also offering highly competitive rewards for the most critical vulnerabilities. The more security-mature industries can afford to be more generous with the top bounties, as they receive fewer high and critical vulnerabilities. 26% of vulnerabilities reported to internet and online services organizations are high and critical, and only 22% of those reported to crypto and blockchain are high or critical.

The Average, Median, and 90th Percentile for Bounties on the HackerOne Platform

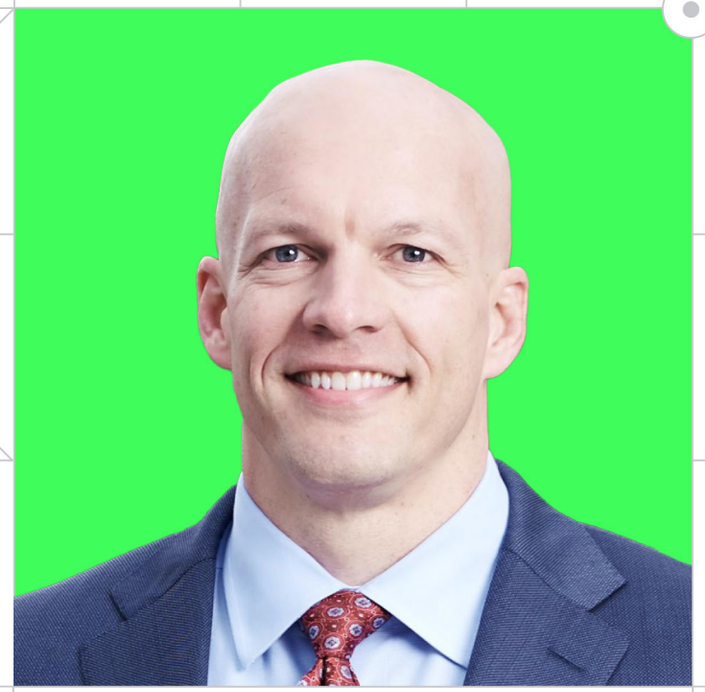
$3.7k

Average bounty for all industries

$12k

90th percentile average for all industries

There are now 29 hackers that have earned over $1 million in bounties on the HackerOne platform.



"Since 2019, Zoom has worked with 900 hackers, of which 300 have submitted vulnerabilities that we have had to quickly move on. We've paid out over $7 million. It's a substantial investment but the returns are worth it: we find world-class talent to find real-world solutions before it's a real-world problem."

Michael Adams, CISO, Zoom

zoom

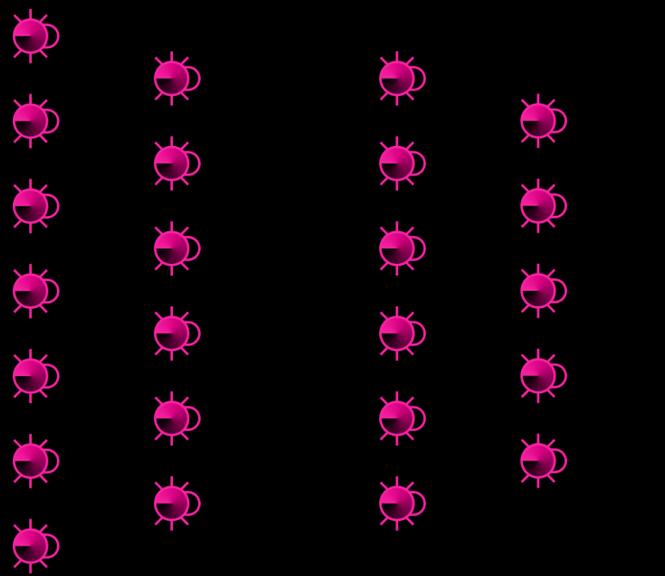
More Than Just Bug Bounty

Ethical hackers can support customers at multiple points across the software development life cycle (SDLC). Development is where organizations can introduce (and find) the most bugs.

SDLC

Customer

HackerOne

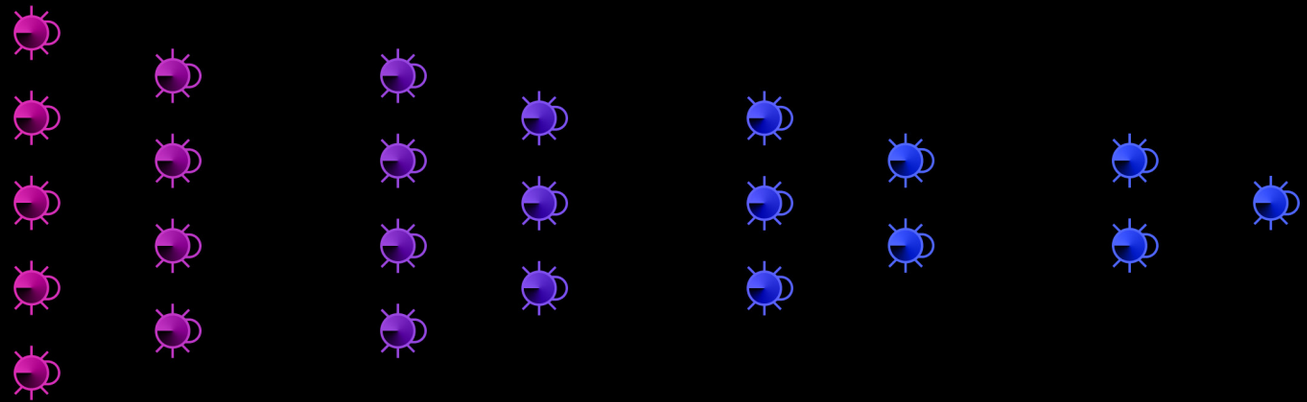


Development

Secure by design frameworks and libraries

Automated Testing

Analysis on code changes and live applications



Stage 1

Code Security Audit

Secure auditing of your code base

Stage 2

Pentest

Frequent testing to validate coverage

Stage 3

Bug Bounty Program

Continuous testing by security experts

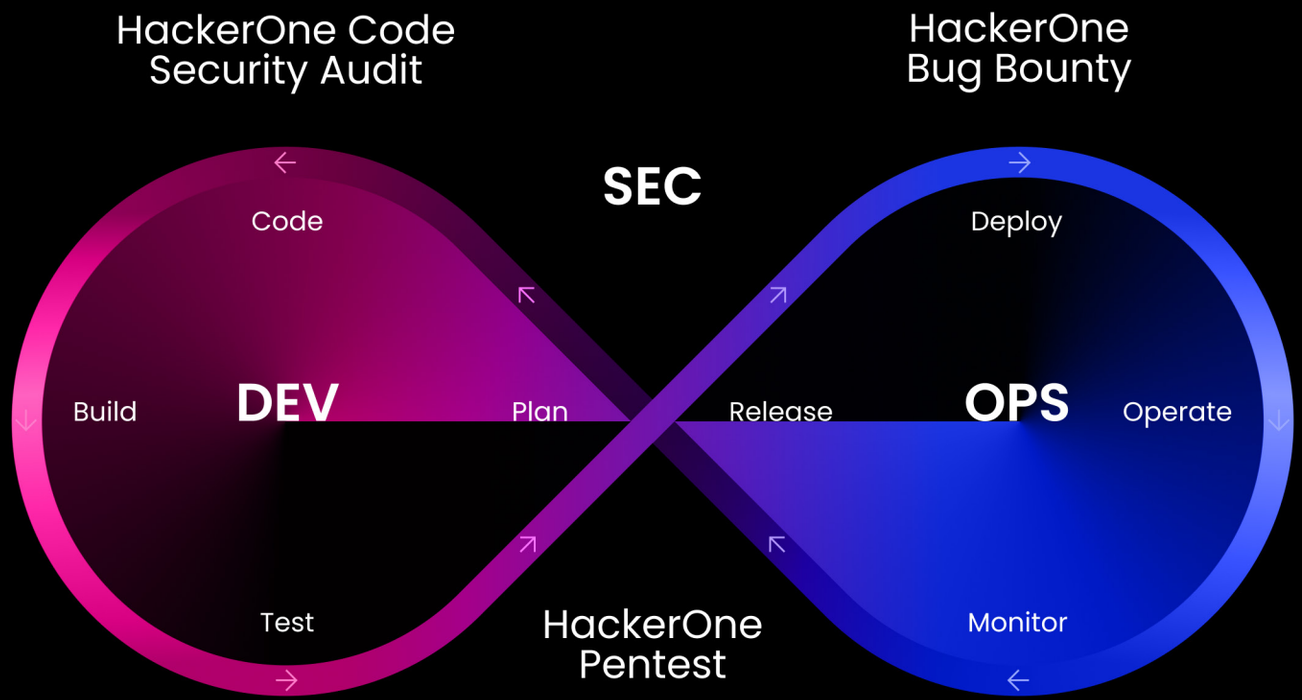
In fact, bug bounty is truly a last line of defense because it covers all of your assets in production.

Top programs use bug bounty as a compass—a tool to help navigate an attack surface to find gaps in security testing coverage. Top-tier security teams leverage bounty programs as a performance monitoring system for their internal security strategy and a safety net that automatically deploys when other security testing systems and processes fail.

Bugs that slip through to production can be used to identify and resolve underlying challenges in security programs. The output of a bug bounty program can help identify improvement opportunities in the SDLC to implement or bolster controls such as:

- Secure development training
- Static application testing
- Human code review
- Small pentests/security hygiene checks

A well-integrated bug bounty program pinpoints challenges across the full vulnerability management landscape, including remediation practices, SLAs, stakeholder relationships, and pentesting habits. By learning from the outputs, an organization can systematically tighten its security controls to the point where novel and elusive bugs—those that can only be identified by human expertise—become a more frequently reported class of vulnerability.



Find Mistakes Early With a Code Security Audit

In the past year, a specialized cohort of the HackerOne community, including a group of rigorously vetted, specialized software engineers and security experts, has performed over 30,000 code reviews. Each review takes a median of 88 minutes to complete and surfaces an average of 1.2 vulnerabilities.

18% of security fixes are incomplete, making them one of the most essential types of code changes to audit.

Vulnerabilities that are most likely to be discovered in a code security audit:

Design flaws and logic errors

Code audits can uncover design flaws and logic errors that might not be immediately apparent during production testing.

Insecure coding practices

Input validation and output encoding issues, lack of proper error handling, inadequate access controls, and other insecure coding practices can lead to various attacks, including injection attacks, cross-site scripting (XSS), and privilege escalation.

Hidden backdoors and malicious code

These are sometimes intentionally or unintentionally inserted into the codebase, and are often difficult to detect through traditional production testing methods alone.

Sensitive data leakage

Data such as hard-coded credentials, API keys, or encryption keys are often stored insecurely within the code.

Cryptographic vulnerabilities

Security vulnerabilities related to cryptography—such as weak encryption algorithms, improper key management, and insecure random number generation—are more likely to be found during a code audit due to their code-centric nature.

Application and Infrastructure-as-Code misconfigurations

These might lead to security vulnerabilities such as incorrect and missing security settings, default configurations, or insecure cloud configurations.

Insecure dependencies

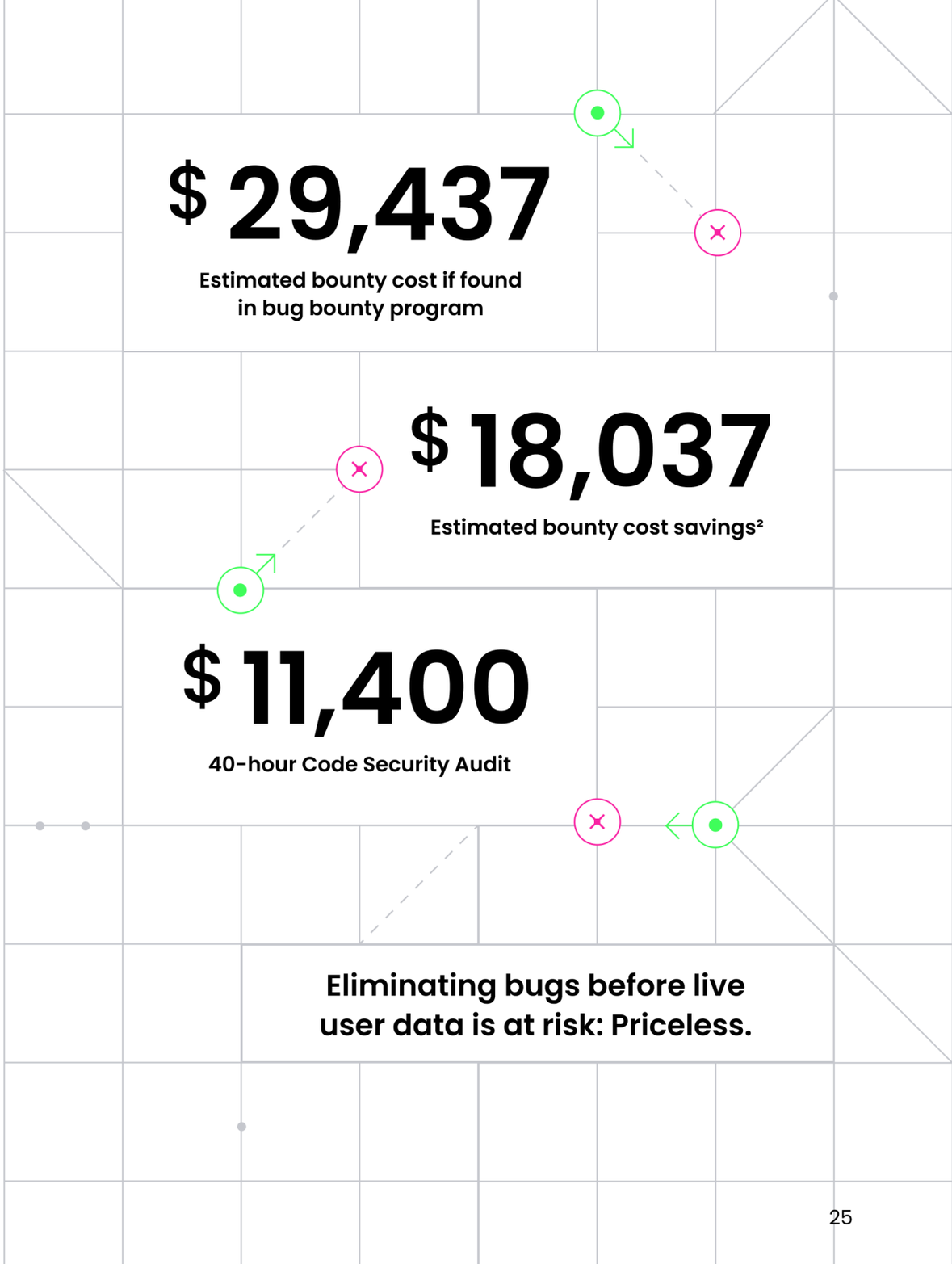
Code audits that include software composition analysis (SCA) can easily uncover vulnerabilities in third-party libraries and dependencies that the application might use.

Unintended information disclosure

Sensitive information—such as debug information, comments, or metadata—might unintentionally leak details about the application's internals and infrastructure.

Finding these vulnerabilities before a product has shipped delivers significant savings

[2] Calculations based off median bounty reward figures across a sample of 1,100+ active HackerOne programs



Ensure Compliance With Industry Standards via Pentest as a Service (PTaaS)

A penetration test (pentest) involves identifying and addressing vulnerabilities, similar to a bug bounty program, but a pentest often leans more toward ensuring an organization adheres to specific compliance and security standards. Pentests typically follow a structured methodology that encompasses a comprehensive, time-bound examination of the system, focusing on identifying vulnerabilities that adversaries could exploit.

Top Ten Vulnerabilities Surfaced in a Pentest

	Pentest top ten vulnerabilities	Bug bounty ranking
1	Misconfiguration	6
2	Cross-site scripting (XSS)	1
3	Information disclosure	3
4	Improper access control - generic	2
5	Using components with known vulnerabilities	8
6	Insecure direct object reference (IDOR)	4
7	Cryptographic	44
8	Insufficient session expiration	39
9	Violation of secure design principles	14
10	Exploiting incorrectly configured SSL/TLS	420

54%

increase in pentests since 2022

16%

increase in the number of vulnerabilities being surfaced by pentests

15%

of vulnerabilities found being rated as high or critical severity

Vulnerabilities such as insufficient session expiration or violation of secure design principles are more likely to be identified during a pentest. This is because pentests often aim to ensure compliance with security standards and help pass audits, focusing on revealing weaknesses stemming from a lack of secure development processes. Audits typically target weaknesses like issues with session expiration or secure design principle violations, making them more likely to be discovered during a pentest. However, since vulnerabilities like insufficient session expiration are not inherently exploitable because they require additional conditions to pose a real threat, they may not lead to payouts in a bug bounty program, where exploitable vulnerabilities are prioritized.

We've seen a 54% increase in pentests since 2022, and a 16% increase in the number of vulnerabilities being surfaced by pentests, with 15% of vulnerabilities found being rated as high or critical severity. On average, 11 valid vulnerabilities are reported per pentest.

"One thing people don't consider, including companies that want to sell us pentesting, is the advantage of running everything through one platform. Having one platform for a very wide range of offensive security testing avoids the need to onboard lots of different vendors, platforms, and so on. This creates a significant time and cost saving."

George Gerchow

CISO and SVP IT, Sumo Logic

sumo logic

Incentivize Novel and Elusive Vulnerabilities With a Bug Bounty

Once you have conducted a thorough code security audit or pentest to identify and address a range of vulnerabilities, it's crucial to continue this proactive security approach. A bug bounty program is a comprehensive and offensive strategy to further cover your bases. It incentivizes a broad spectrum of ethical hackers to apply their diverse skills and creativity in rooting out even the most novel and elusive vulnerabilities in your shipped products—ensuring robust, multi-layered security.

After launching a bug bounty, the median time to receive the first valid report is 20 days. Hackers are reporting 13% more critical bugs in 2023, and 15% more high-severity bugs. Critical or high-rated bugs make up 29% of valid bug bounty reports.

Top Ten Vulnerabilities Surfaced in a Bug Bounty

	Bug bounty top ten vulnerabilities	Pentest ranking
1	Cross-site scripting (XSS)	2
2	Improper access control	4
3	Information disclosure	3
4	Insecure direct object reference	6
5	Privilege escalation	23
6	Misconfiguration	1
7	Improper authentication - generic	16
8	Business logic errors	21
9	Open redirect	15
10	Improper authorization	13

How Does Your Industry Measure Up?

We've taken a look at the top ten vulnerabilities reported on the HackerOne platform across all HackerOne products and calculated what percentage of the total reports is attributable to each vulnerability type. And we've cross-referenced that by industry so you can see how your industry compares to the platform average when it comes to types of vulnerability reports received.

Cross-site scripting (XSS)—the largest category overall—is broken out into its different subtypes, so improper access control is the number-one vulnerability on the list, comprising 13% of all valid vulnerabilities reported through the HackerOne platform. Most industries are seeing fewer reports than average. We go into the reasons for that next, in the industry-specific sections.

Vulnerability Type by Industry Platform Average

13%	Improper access control - generic
11%	Information disclosure
10%	Cross-site scripting (XSS) - Reflected
7%	Insecure direct object reference (IDOR)
5%	Privilege escalation
5%	Cross-site scripting (XSS) - stored
5%	Misconfiguration
3%	Improper authentication - generic
3%	Business logic errors
3%	Cross-site scripting (XSS) - DOM

Vulnerability Type by Industry

Above average performance | Below average performance | Average performance

Most common platform vulnerability	Platform Average	Financial Services	Government	Telecoms	Retail & E-commerce	Automotive	Media & Entertainment	Computer Software	Internet & Online Services	Cryptocurrency & Blockchain	Travel & Hospitality
Improper access control - generic	*13%*	12%	13%	28%	10%	10%	10%	13%	12%	9%	8%
Information disclosure	*11%*	13%	5%	9%	13%	11%	10%	14%	10%	7%	13%
Cross-site scripting (XSS) - Reflected	*10%*	10%	15%	8%	13%	19%	11%	5%	9%	4%	16%
Insecure direct object reference (IDOR)	*7%*	7%	15%	7%	10%	11%	8%	6%	7%	3%	8%
Privilege escalation	*5%*	6%	4%	3%	3%	4%	5%	6%	5%	5%	5%
Cross-site scripting (XSS) - stored	*5%*	2%	6%	1%	3%	3%	5%	6%	7%	4%	3%
Misconfiguration	*5%*	4%	2%	6%	3%	3%	7%	4%	5%	6%	4%
Improper authentication - generic	*3%*	3%	2%	4%	3%	10%	5%	2%	3%	4%	4%
Business logic errors	*3%*	3%	2%	1%	4%	1%	3%	3%	3%	8%	2%
Cross-site scripting (XSS) - DOM	*3%*	3%	2%	3%	4%	3%	4%	2%	2%	1%	3%

High and Critical Vulnerabilities

When we look at the high and critical vulnerabilities, we see a high ranking for insecure direct object references (IDOR), for example, because these are not vulnerabilities you can scan for. This highlights the importance of human intelligence in seeking out these weaknesses. Similarly, SQL injection appears more often in the high/critical category because these vulnerabilities by their nature will have a significant impact because they would give an attacker access to the backend of your systems.

High and Critical Vulnerabilities Platform Average

12 %	Information disclosure
11 %	Improper access control - generic
9 %	Insecure direct object reference (IDOR)
8 %	Cross-site scripting (XSS) - stored
7 %	Privilege escalation
7 %	Misconfiguration
5 %	Improper authentication - generic
4 %	SQL injection
3 %	Cross-site scripting (XSS) - reflected
3 %	Server-side request forgery (SSRF)

High and Critical Vulnerabilities by Industry

Above average performance | Below average performance | Average performance

Most common platform vulnerability	Platform Average	Financial Services	Government	Telecoms	Retail & E-commerce	Automotive	Media & Entertainment	Computer Software	Internet & Online Services	Cryptocurrency & Blockchain	Travel & Hospitality
Information disclosure	*12%*	9%	5%	8%	13%	11%	8%	24%	7%	7%	12%
Improper access control - generic	*11%*	16%	16%	11%	12%	12%	9%	8%	10%	3%	10%
Insecure direct object reference (IDOR)	*9%*	13%	13%	9%	11%	12%	9%	6%	9%	4%	13%
Cross-site scripting (XSS) - stored	*8%*	3%	8%	2%	4%	4%	8%	5%	15%	12%	4%
Privilege escalation	*7%*	5%	8%	8%	4%	5%	7%	8%	6%	7%	5%
Misconfiguration	*7%*	6%	2%	8%	4%	4%	13%	4%	5%	9%	5%
Improper authentication - generic	*5%*	5%	4%	8%	3%	5%	5%	4%	5%	3%	8%
SQL injection	*4%*	4%	4%	4%	6%	11%	2%	2%	3%	1%	4%
Cross-site scripting (XSS) - reflected	*3%*	2%	6%	2%	3%	4%	3%	2%	5%	2%	2%
Server-side request forgery (SSRF)	*3%*	4%	1%	3%	4%	3%	2%	2%	3%	5%	3%

Financial Services

Financial Services stand out as being particularly security-mature because the industry requires stringent compliance with regulations, meaning easy-to-fix vulnerabilities are going to be identified and remediated before products go live.

Government

Government agencies are performing poorly when it comes to the low-hanging fruit. This is likely due to these organizations relying on older systems that get overlooked for reasons of budget, breadth, and forgotten assets. Government agencies are seeing fewer reports for more complex vulnerabilities like business logic errors because hackers exhaust the plentiful low-hanging fruit before delving deeper.

Telecoms

Telecoms also rely on legacy systems, which are hard to make changes to. When those systems were implemented, there was less of a focus on security, so a lot of vulnerabilities would have been introduced—meaning high volumes of improper authentication and misconfigurations. Implementing authentication mechanisms on older systems is challenging and there is an incredibly large telecom user base to authenticate. It may be, therefore, that telecom companies want access control to be a point of focus and are incentivizing hackers to find these vulnerabilities.

Retail and E-commerce

Retail and e-commerce businesses, on the other hand, are typically using newer systems and are constantly refreshing. We see fewer improper access control vulnerabilities because there is less nuance in their authentication mechanisms: a straightforward log-in to an account. Information disclosure and cross-site scripting are in higher volumes, and the overall numbers for vulnerabilities are fairly high because there are a lot of parallels between e-commerce sites, so testing for one will be very similar to testing for the next—meaning it's easy to replicate testing methods across hundreds of sites.

Automotive

It's not surprising that the automotive industry receives the greatest quantity of cross-site scripting vulnerabilities. Historically, websites haven't been their main focus when it comes to security software and they likely have a lot of third-party and franchise websites that have these vulnerabilities within them. The volume of high percentages in the high/critical category is because the automotive industry is relatively new to bug bounty programs, so there's more clean-up to do.

Media and Entertainment

The media and entertainment industry aligns closely with the average. While these organizations will have a lot of websites (including those largely forgotten for old releases), because they are often static pages, they are not hugely exploitable.

Computer Software

Because the computer software industry's products are largely delivered by desktop applications, fewer web vulnerabilities like cross-site scripting affect these businesses.

Internet and Online Services

We see a high level of security maturity in the internet and online services industry because security has always been a key focus for them. This industry sees a particularly high percentage of high and critical cross-site scripting (stored) vulnerabilities. This is because those vulnerabilities will have a particularly significant impact on this industry, allowing an attacker to deface websites and degrade customer trust, meaning that Internet and Online Services organizations incentivize hackers to report cross-site scripting vulnerabilities.

Crypto and Blockchain

The results for crypto and blockchain diverge most significantly from the average. This is in part because this young industry has no reliance on legacy software and their developers have strong insight into security. Crypto and blockchain companies are more likely to incentivize hackers to find vulnerabilities that could result in the stealing or draining of cryptocurrency wallets, which is why we're seeing a higher portion of reports for misconfiguration and business logic errors.

Travel and Tourism

The higher-than-average volume of cross-site scripting reports for travel and tourism businesses is attributable to their huge attack surfaces. Frequent mergers and acquisitions in this industry add to an existing attack surface, and it's not uncommon for each hotel property to have its own web presence. Findings for information disclosure and IDOR are also higher because this industry has a strong customer loyalty focus, so ensuring customer data is secure is a particular priority.

Fixing Bugs and Measuring Success

This year we've seen a significant 28% improvement in the time it takes to remediate a vulnerability once reported—from an average of 35.5 days down to 25.5 days. Automotive, media and entertainment, and government customers have seen the biggest improvements in time to remediate, each with at least 50% improvement since 2022.

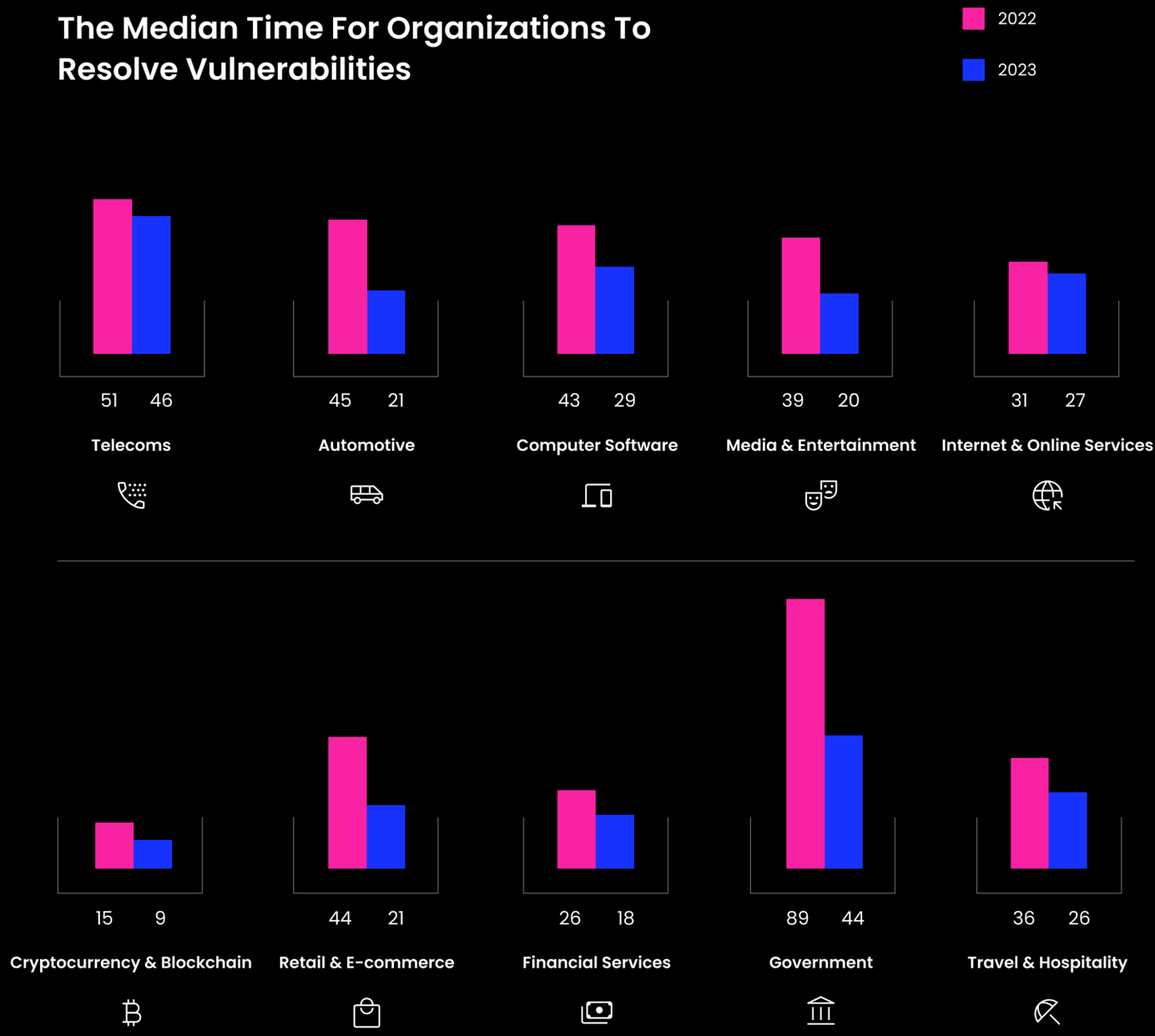
35.5

2022 average days to remediation

25.5

2023 average days to remediation

The Median Time For Organizations To Resolve Vulnerabilities

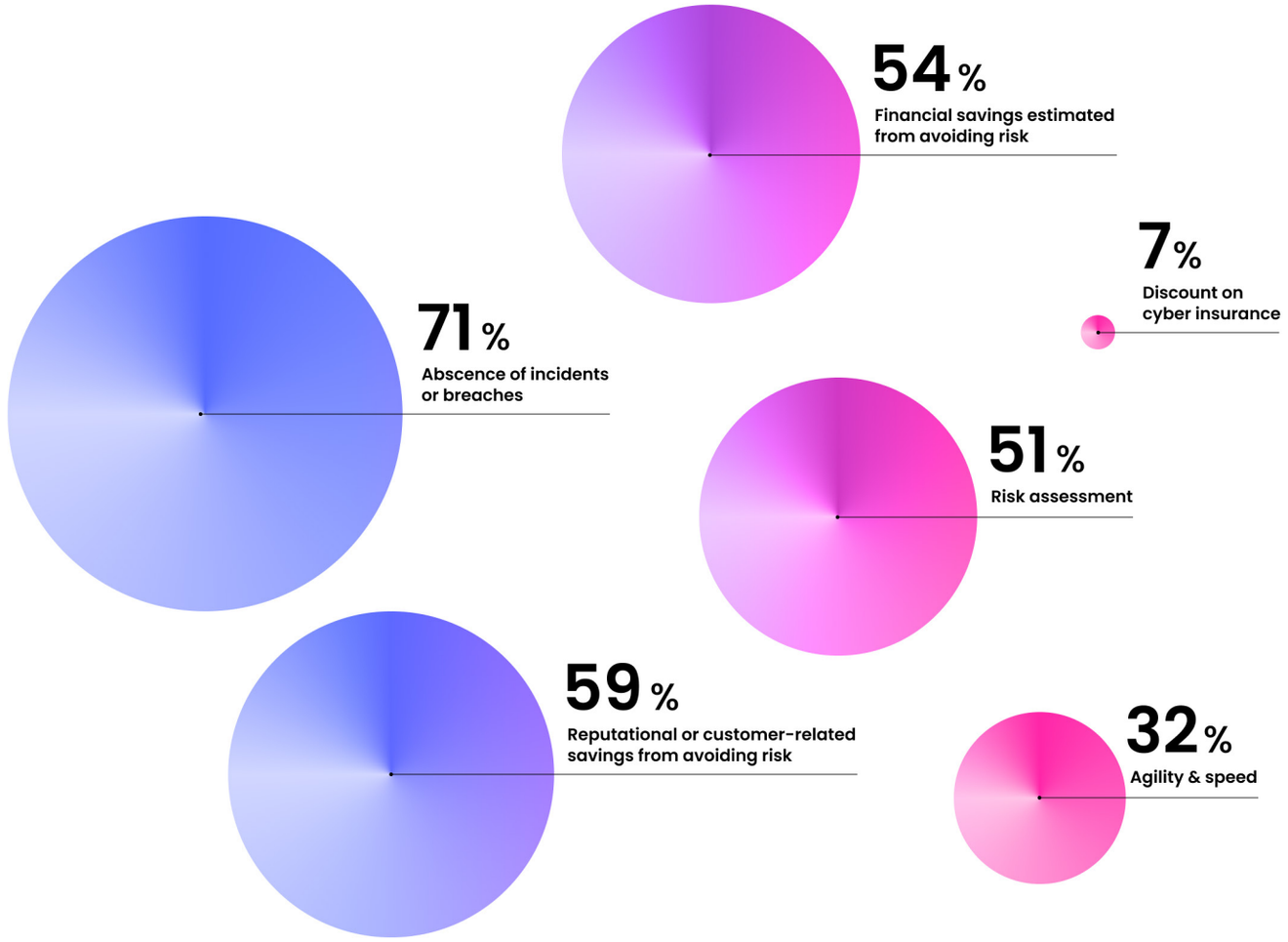


Fixing Bugs and Measuring Success

Time to remediate vulnerabilities is a good metric to show that your security teams are becoming more adept and efficient at resolving bugs. We also asked our customers how they measure success. The majority (71%) measure the absence of incidents or breaches, and many (59%) combine this with the estimated savings of reputational or customer-related incidents.

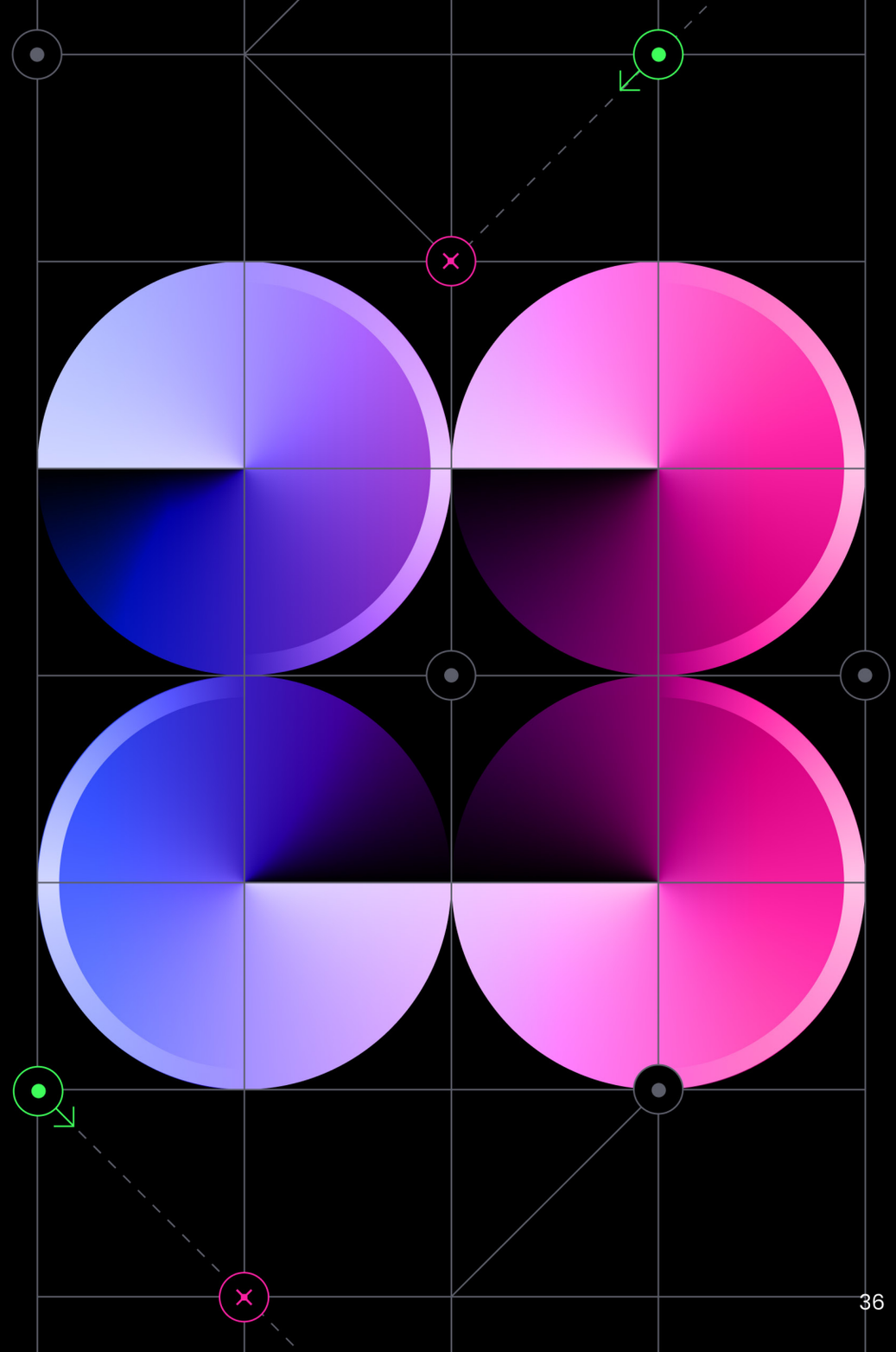
How does your organization measure the ROI of its HackerOne security program?

71%	Absence of incidents or breaches
59%	Estimated savings of reputational or customer-related impacts as a result of a security program
54%	Financial savings estimated from avoiding risk
51%	Risk assessment (internal or external)
32%	Agility and speed of security teams' responsiveness
7%	Discount on cyber insurance



Conclusion

The 7th annual Hacker-Powered Security Report makes it clear that the use cases for ethical hacking will continue to expand and diversify—from securing GenAI applications to finding bugs even earlier in the SDLC. Organizations that partner with this innovative community benefit from the cutting-edge research and techniques that hackers, with their outsider mindset, add to the organizations' talent pool. The partnership means organizations can outpace cybercriminal efforts and concentrate on building new, ever-more-secure products as exploitable vulnerabilities are discovered and fixed faster than ever before.



Methodology

HackerOne's annual hacker survey surveyed 2384 hackers that were active on the platform in the 30 days prior to the survey. The survey took place between July 25 and August 17, 2023.

The data collected from HackerOne's platform is from the period between June 2022 and June 2023.

HackerOne's customer survey was conducted via UserEvidence and surveyed 46 HackerOne customers between August 23 and September 14, 2023.

hackerone

HackerOne pinpoints the most critical security flaws across an organization's attack surface with continual offensive testing to outmatch cybercriminals. HackerOne's Attack Resistance Platform blends the security expertise of ethical hackers with asset discovery, continuous assessment, and process enhancement to reduce threat exposure and empower organizations to transform their businesses with confidence. Customers include Coinbase, Costa Coffee, General Motors, GitHub, Goldman Sachs, Hyatt, PayPal, Singapore's Ministry of Defense, Slack, and the U.S. Department of Defense. In 2023, HackerOne was named a Best Workplace for Innovators by Fast Company.

Trusted by

coinbase COSTA gm GitHub Goldman Sachs

HYATT PayPal MINDEF SINGAPORE slack U.S. Department of Defense

Book a meeting with a security expert and scope your pentest today.

Contact Us