hackerone

Hacker-Powered Security Report

2022

Introduction

Security automation cannot replace the creativity of humans. In fact, 92% of ethical hackers say they can find vulnerabilities scanners can't. For the past six years, we've been surveying hackers to learn more about how they see the evolving security testing industry. We combine these insights with the world's largest dataset of vulnerabilities to identify trends that inform our customers how to build an impactful security strategy.

This year, HackerOne introduced its Attack Resistance Management (ARM) approach that combines attack surface knowledge with the power of ethical hackers to give organizations a true security advantage and target the root causes of the attack resistance gap.

The attack resistance gap is the gap between what organizations are able to protect and what they need to protect. The main factors contributing to this gap are incomplete knowledge of digital assets, insufficient testing, and a shortage of the right skills.

In the past year, the hacking community has found over 65,000 customer vulnerabilities. Reports for vulnerability types typically introduced by digital transformation have seen the most significant growth with misconfigurations growing by 150% and improper authorization by 45%.

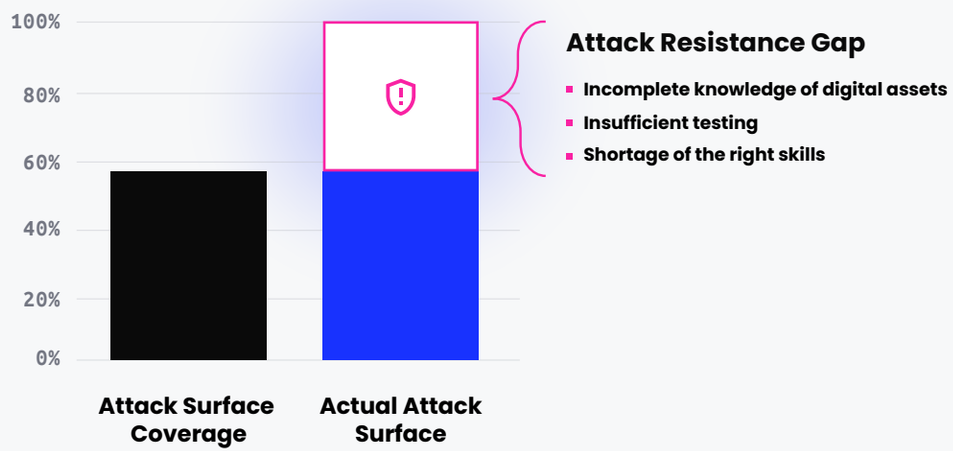
In this year's Hacker-Powered Security Report, we look at what drives the hacking community, what their focus is, and what they're doing to secure customers.

92%

OF ETHICAL HACKERS SAY THEY CAN FIND VULNERABILITIES SCANNERS CAN'T

65,000

VULNERABILITIES FOUND IN 2022



Hackers Are Motivated By Learning, Money, And The Mission To Build A Safer Internet

Forty-six percent of hackers say they are motivated to hack to protect businesses and their users. Despite the majority of hackers (70%) doing it part time, 47% say they are hacking more this year than they did in 2021. Sixty-eight percent says that the money earned from hacking makes up less than half of their income. Seventy-nine percent of hackers say they hack to learn, more than those that say they're in it for the money (72%).

79%
OF HACKERS ARE MOTIVATED TO LEARN

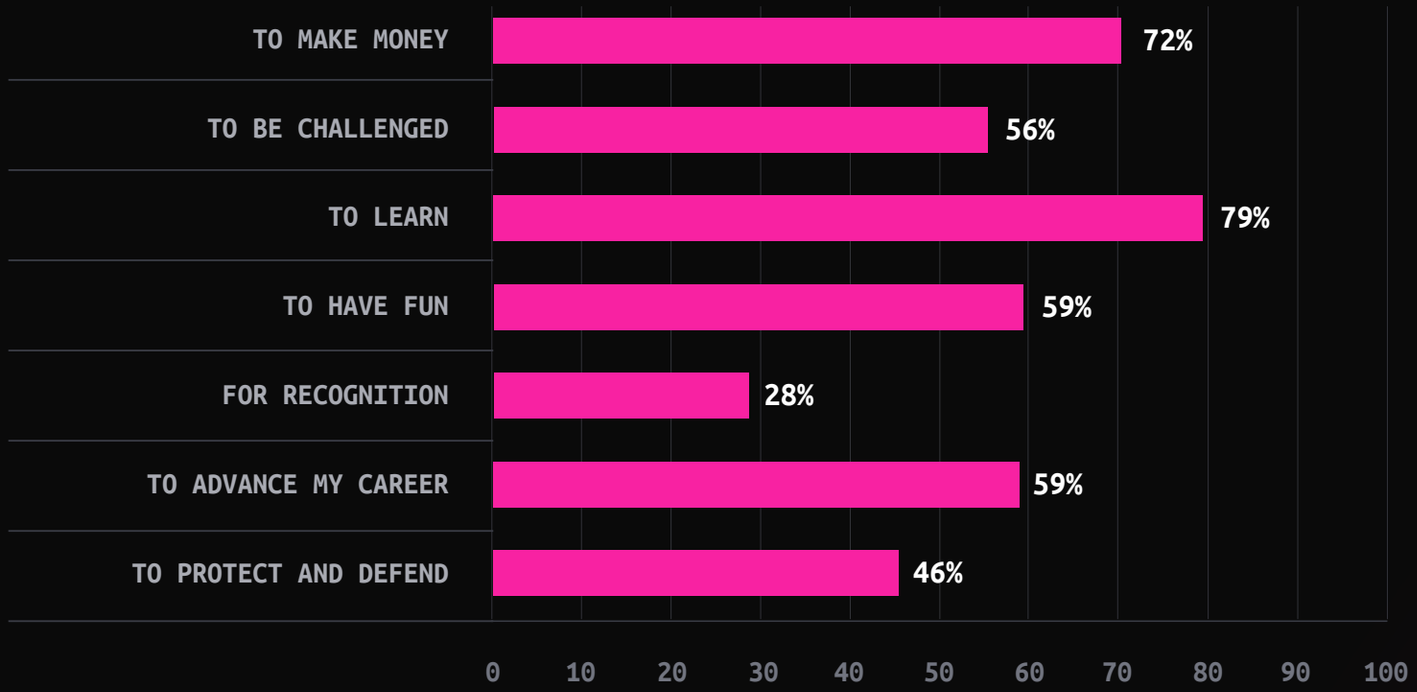
72%
OF HACKERS ARE MOTIVATED BY MONEY

59%
OF HACKERS ARE MOTIVATED TO HAVE FUN

"I'm a doctor when I'm not hacking and am motivated by the desire to do good in the world. There are many similarities between medicine and hacking; as a doctor, you're trained to do threat modeling on humans, and sharing knowledge is what leads us to detect new diseases or discover new treatments. I bring this curiosity and collaborative approach to bug hunting."

JONATHAN BOUMAN, HACKER, NETHERLANDS

Hackers Are Motivated By Learning, Money, And The Mission To Build A Safer Internet



$230M

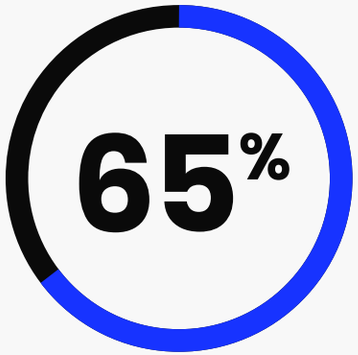
EARNED ON THE
HACKERONE PLATFORM

Hackers have now earned more than $230 million on the HackerOne platform.

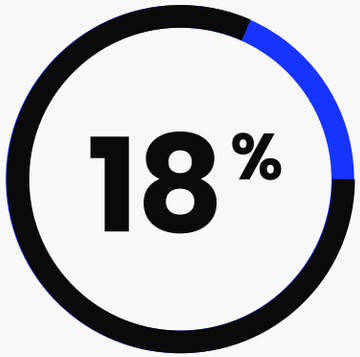
Twenty two hackers have earned over $1 million in bounties, up from 9 hackers since last year's Hacker Report.

The Most Security Mature Organizations Attract The Most Skilled Hackers

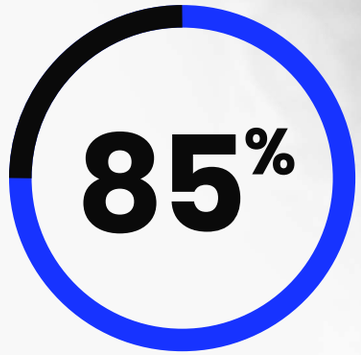
We asked hackers what attracts them to the programs they hack on. Bounties are the biggest attraction with 65% saying they choose a program based on the rewards offered. Having the opportunity to publicly disclose how they found the vulnerabilities and details of those vulnerabilities is important for 18% of hackers. Eighty five percent also say they believe companies should be more transparent about vulnerability disclosure.



OF HACKERS SAY THEY CHOOSE A PROGRAM BASED ON THE REWARD OFFERED

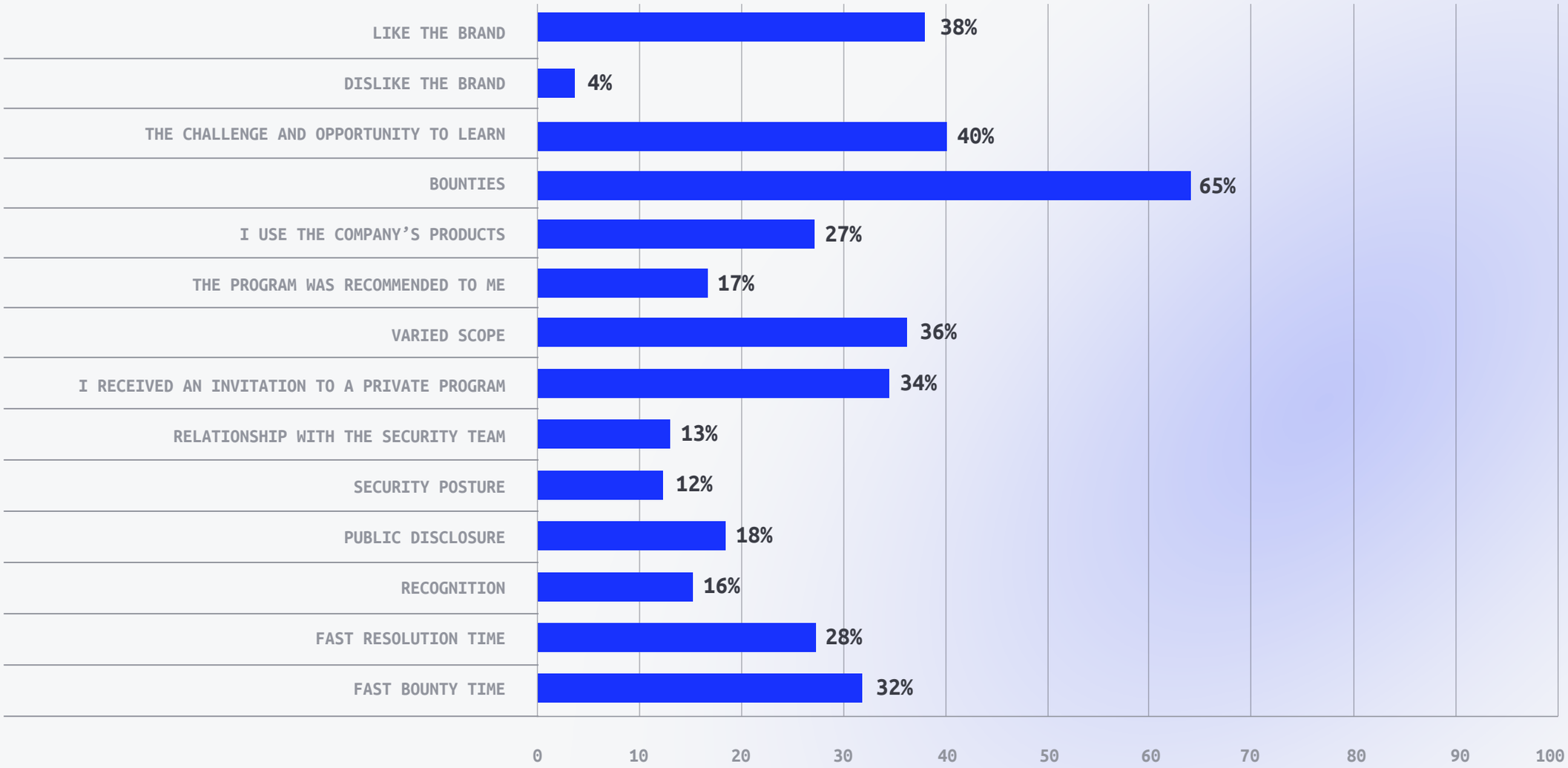


OF HACKERS SAY THEY CHOOSE A PROGRAM BASED ON PUBLIC DISCLOSURE

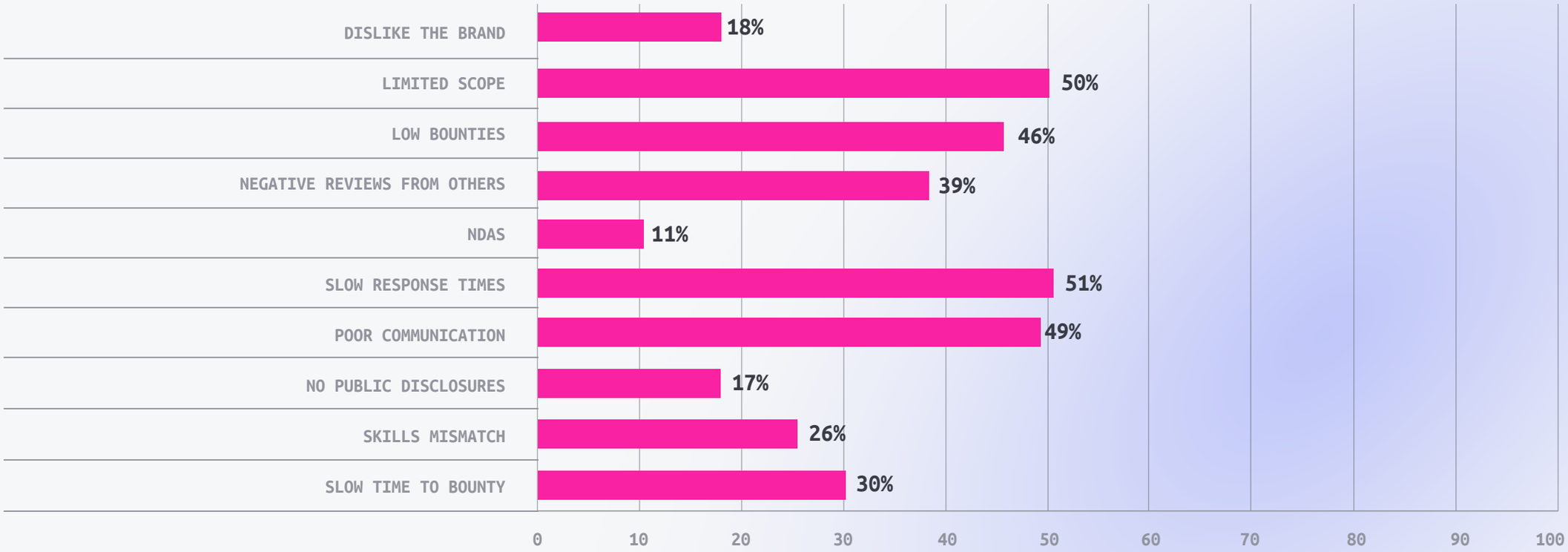


OF HACKERS BELIEVE COMPANIES SHOULD BE MORE TRANSPARENT ABOUT VULNERABILITY DISCLOSURE

How Hackers Choose Their Targets



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



Liking a brand plays a part for 38% of hackers. However, programs with less recognizable brands can make their program more attractive by following program best practices like regular communications, paying on triage, and resolving bugs quickly.

A limited scope puts off 50% of hackers, but slow response time and poor communication are the issues that are most likely to prevent a hacker reporting a vulnerability.

Overall time to remediation increased last year from 35 days to 37 days. Time to remediation is how long it takes the organization to fix the vulnerability from having received the report. Industries that are typically in early stages of the security maturity model, such as automotive and pharmaceuticals, have seen high levels of program adoption in 2022, which contributes to the average increase in remediation time.

Industries that decreased their time to remediation include cryptocurrency and blockchain (11.6 days down from 19.5), media and entertainment (28.9 days down from 36.7), and retail and ecommerce (42.2 days down from 53.4).

Cryptocurrency & Blockchain

19.5 ↓

11.6

DAYS TO REMEDIATION

Media & Entertainment

36.7 ↓

28.9

DAYS TO REMEDIATION

Retail & Ecommerce

53.4 ↓

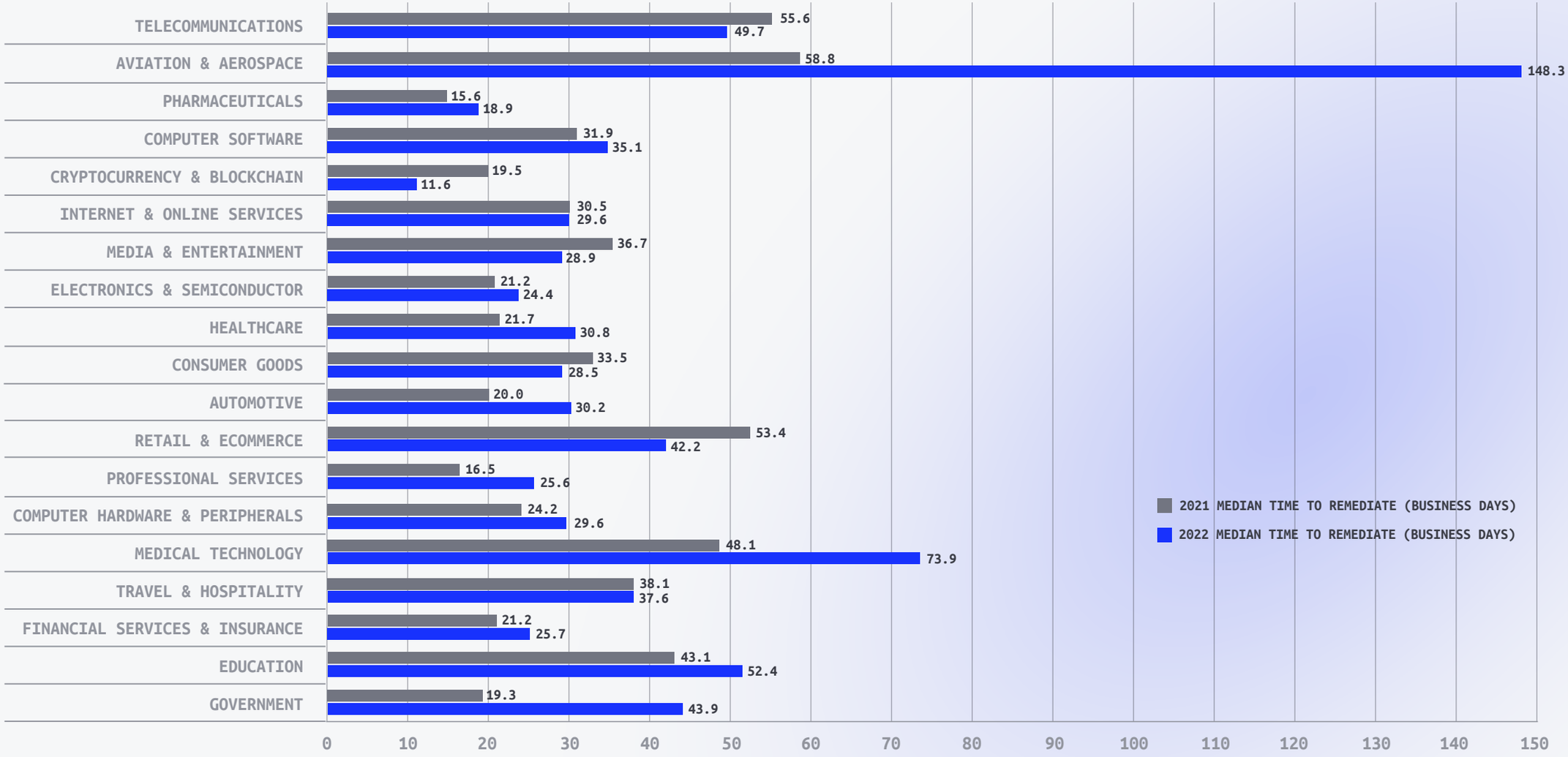
42.2

DAYS TO REMEDIATION

"Disclosure helps us all learn. By disclosing security vulnerabilities, organizations can help increase overall security. Public disclosure demonstrates that an organization has a high level of security maturity and will be a program worth hacking on."

ALEX CHAPMAN, HACKER, UK

Median Time To Vulnerability Resolution By Industry



Organizations Rely On Hackers To Help Close Their Security Gaps

Vulnerabilities can't be found without hackers. 69% of organizations have had a security incident in the past year. However, 50% of hackers chose not to disclose a vulnerability they have found. The biggest reason (42%) preventing disclosure is the most obvious one: organizations and websites do not have a vulnerability disclosure program.

Twelve percent of hackers also cite threatening legal language on program pages as something that has led them to hold onto a bug. However, two-thirds of hackers said that recent changes to the U.S. Department of Justice's to Computer Fraud and Abuse Act (CFAA) will increase hacking protections.

HackerOne launches the Gold Standard Safe Harbor statement

The Gold Standard Safe Harbor (GSSH) statement supports the protection of ethical hackers from liability when hacking in good faith. While many programs already include safe harbor in their policies, the GSSH is a short, broad, easily-understood safe harbor statement that's simple for customers to adopt. This standardization also reduces the burden on hackers for parsing numerous different program statements. HackerOne customers can now further demonstrate their commitment to protecting good faith security research with GSSH.

READ THE PRESS RELEASE

"We know that the best way to protect our community and stay ahead of the evolving threat landscape is to collaborate with industry-leading experts, researchers, and academics, inviting them to disclose potential security vulnerabilities so we can quickly address them."

SUHANA HYDER, VULNERABILITY MANAGEMENT LEADER, TIKTOK.

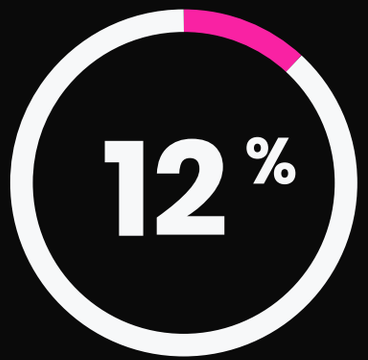
READ ABOUT TIKTOK'S TWO-YEAR ANNIVERSARY WITH HACKERONE HERE

ORGANIZATIONS RELY ON HACKERS TO HELP CLOSE THEIR SECURITY GAPS

Data from those vulnerability reports is also crucial to closing security gaps and preventing the same vulnerabilities from being introduced at development.

The HackerOne Top Ten leverages our unique dataset giving customers insight into the most impactful weaknesses from a hacker perspective. Knowing what attackers are most likely to prioritize helps customers understand where to incentivize hackers. These vulnerabilities are based on what hackers discover and are rewarded for on the platform.

OF HACKERS CHOSE NOT TO DISCLOSE A VULNERABILITY THEY HAVE FOUND

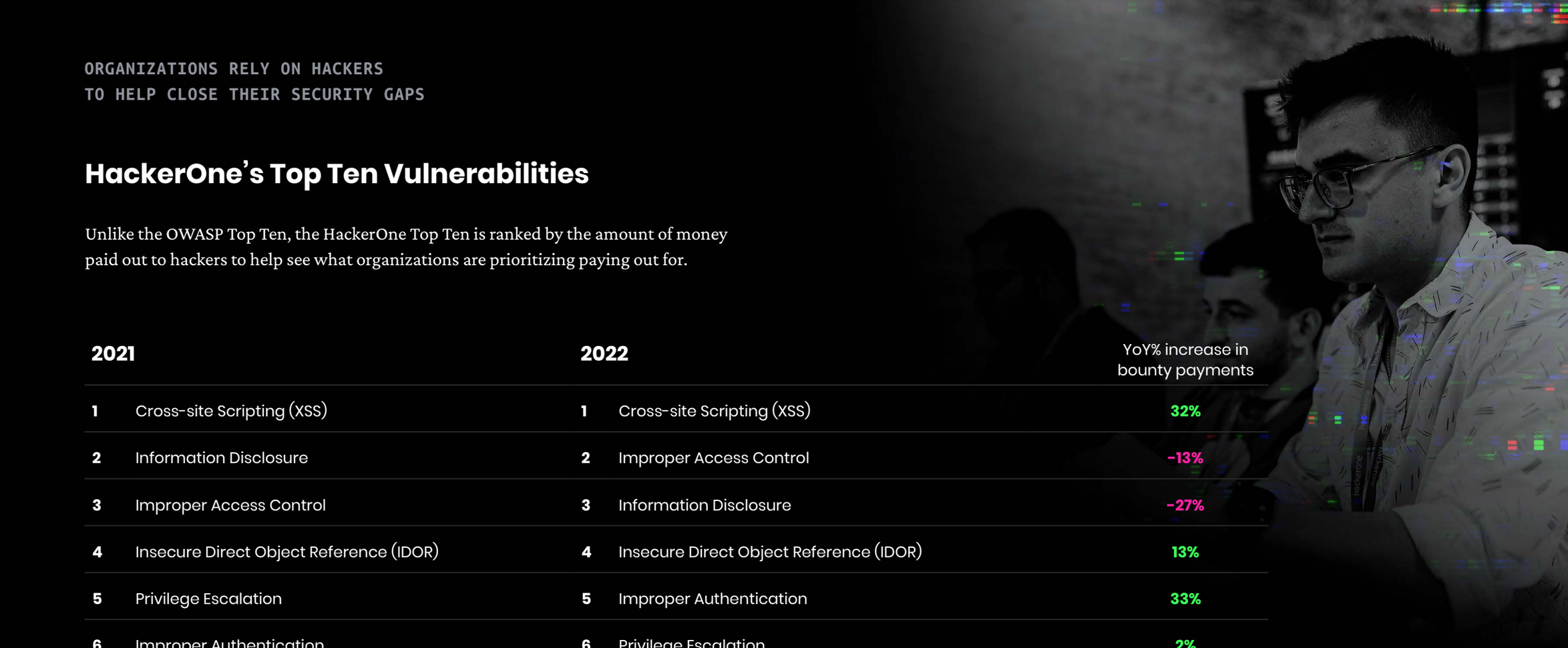


OF HACKERS CITE THREATENING LEGAL LANGUAGE AS A REASON NOT TO DISCLOSE A VULNERABILITY

"You can't argue with data. The more you have, the better position you'll be in to make clear decisions about what to prioritize. The data becomes even more valuable than the individual vulnerability reports, including trends of what vulnerability categories are submitted, how often they're occurring, what product or functionality they're found in, and what the root cause is."

ROY DAVIS, SECURITY MANAGER, ZOOM

WATCH ROY TALK THROUGH ZOOM'S APPROACH



HackerOne's Top Ten Vulnerabilities

Unlike the OWASP Top Ten, the HackerOne Top Ten is ranked by the amount of money paid out to hackers to help see what organizations are prioritizing paying out for.

2021		2022		YoY% increase in bounty payments
1	Cross-site Scripting (XSS)	1	Cross-site Scripting (XSS)	32%
2	Information Disclosure	2	Improper Access Control	-13%
3	Improper Access Control	3	Information Disclosure	-27%
4	Insecure Direct Object Reference (IDOR)	4	Insecure Direct Object Reference (IDOR)	13%
5	Privilege Escalation	5	Improper Authentication	33%
6	Improper Authentication	6	Privilege Escalation	2%
7	Code Injection	7	Code Injection	26%
8	SQL Injection	8	Improper Authorization	76%
9	Server-Side Request Forgery (SSRF)	9	SQL Injection	-15%
10	Business Logic Errors	10	Server-Side Request Forgery	-18%

ORGANIZATIONS RELY ON HACKERS TO HELP CLOSE THEIR SECURITY GAPS

In the past year, Cross Site Scripting has seen a 7% increase in reports and a 32% increase in the amount paid out. Because it's a simple bug to fix, we will continue to see reports for Cross Site Scripting trend downwards with organizations developing better filters to avoid the introduction of these bugs and potential for exploitation.

Digital transformation, caused by cloud migration and remote work, continues to impact vulnerability report data. Improper Authentication and Improper Authorization have both seen significant growth in payouts. More apps and tools are introducing ever more granular permissions and, as security maturity increases, there is more segmentation of user types based on what they should have access to. This increase in complexity introduces more opportunities to exploit access control.

Cross Site Scripting

7%

INCREASE IN REPORTS

32%

INCREASE IN AMOUNT PAID OUT

Websites Remain Organizations' Biggest Attack Vector

Ninety-five percent of hackers focus their efforts on websites. However, other technologies are also becoming of increasing interest to hackers. Twenty-four percent of hackers focus on cloud platforms. Reports for misconfigurations have also increased by 151% in the past year, along with other vulnerabilities common in cloud infrastructure like improper access control and authorization.

Despite a huge increase in decentralized finance (DeFi) attacks over the past year, blockchain is still a niche speciality with only 8% of hackers focusing on the technology, however, this is up from 5% in 2021.

> **"Having hackers test on our cloud is crucial to our overall security strategy. The scope we provide our researchers allows them to focus on the most critical aspects of security on our platform. Any report that gives us insights into exploiting issues or bypassing current implementations helps us align to industry best practices."**
>
> IFAT KOOPERLI, VULNERABILITY MANAGEMENT LEAD, WIX

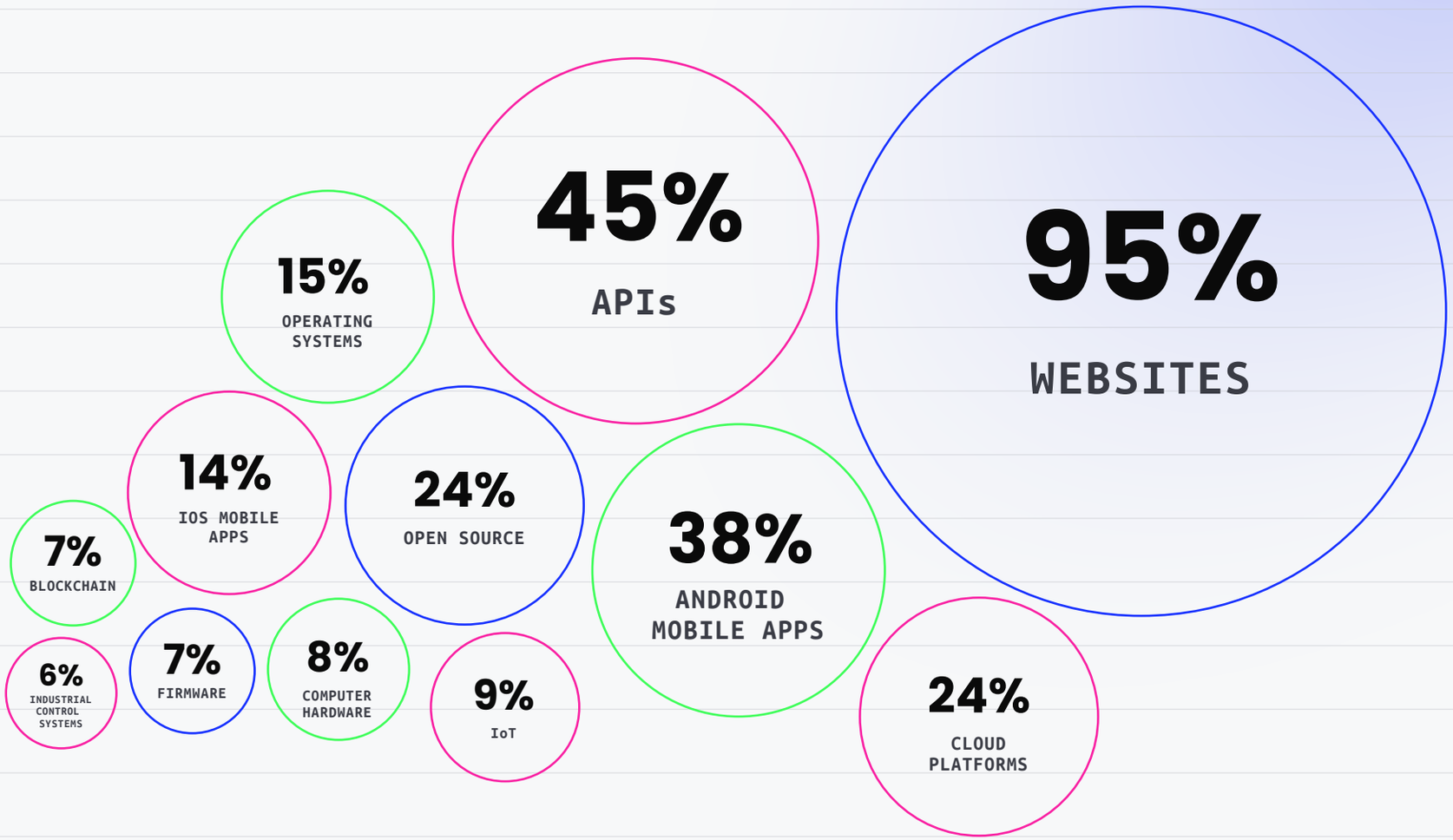
95%

OF HACKERS FOCUS THEIR EFFORTS ON WEBSITE

151%

INCREASE IN MISCONFIGURATION REPORTS

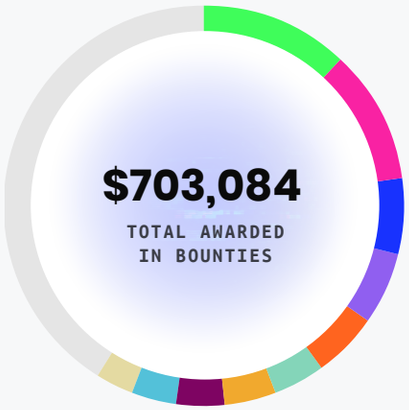
Where Hackers Spend Their Time



Check Out What The Top 10 Vulnerabilities Are In Your Industry

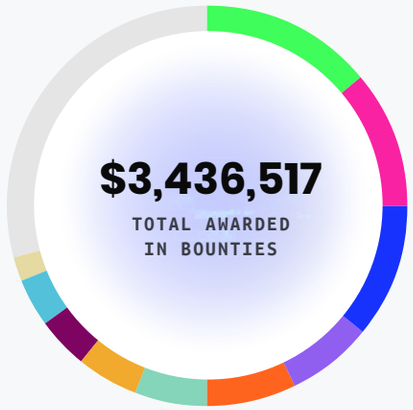
Government

1. Improper Access Control - Generic — **$88,261**
2. XSS — **$80,107**
3. Insecure Direct Object Reference (IDOR) — **$43,932**
4. Misconfiguration — **$42,771**
5. Improper Authentication - Generic — **$39,866**
6. Information Disclosure — **$30,701**
7. Code Injection — **$30,500**
8. Command Injection - Generic — **$27,000**
9. OS Command Injection — **$26,700**
10. Path Traversal — **$23,700**



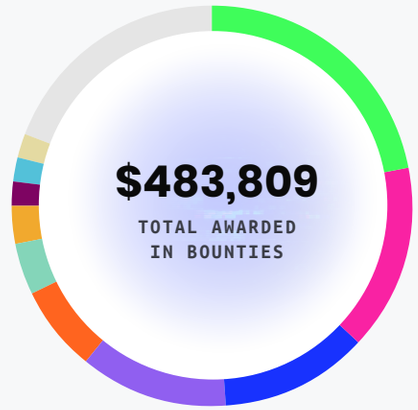
Financial Services

1. Insecure Direct Object Reference (IDOR) — **$481,975**
2. Improper Access Control - Generic — **$392,751**
3. XSS — **$381,305**
4. Information Disclosure — **$248,663**
5. Privilege Escalation — **$232,952**
6. Improper Authentication - Generic — **$198,137**
7. Server-Side Request Forgery (SSRF) — **$160,403**
8. SQL Injection — **$133,800**
9. Code Injection — **$125,325**
10. Path Traversal — **$64,400**



Automotive

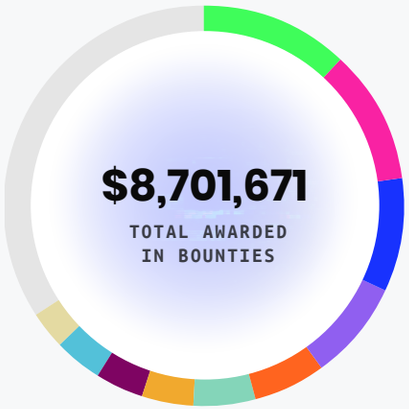
1. Insecure Direct Object Reference (IDOR) — **$107,665**
2. Information Disclosure — **$73,620**
3. XSS — **$60,028**
4. Improper Access Control - Generic — **$57,746**
5. Privilege Escalation — **$33,500**
6. Code Injection — **$17,250**
7. Improper Authentication - Generic — **$13,550**
8. Exposed Dangerous Method or Function — **$10,400**
9. Improper Input Validation — **$8,700**
10. SQL Injection — **$8,700**



Check Out What The Top 10 Vulnerabilities Are In Your Industry

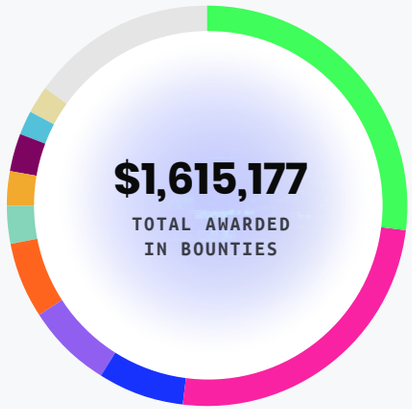
Computer Software

1. XSS — **$1,082,258**
2. Improper Access Control - Generic — **$946,814**
3. Information Disclosure — **$750,863**
4. Improper Authorization — **$711,453**
5. Privilege Escalation — **$564,417**
6. Insecure Direct Object Reference (IDOR) — **$462,114**
7. Improper Authentication - Generic — **$384,452**
8. Insecure Configuration of Network Infrastructure — **$333,000**
9. Other — **$310,500**
10. Code Injection — **$294,600**



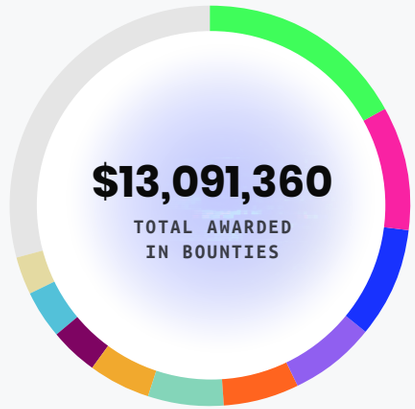
Crypto and Blockchain

1. XSS — **$439,044**
2. Business Logic Errors — **$408,713**
3. Information Disclosure — **$121,115**
4. Insecure Direct Object Reference (IDOR) — **$110,213**
5. Missing Authorization — **$100,000**
6. Denial of Service — **$49,996**
7. Improper Access Control - Generic — **$43,136**
8. Improper Authorization — **$42,750**
9. Use of Hard-coded Credentials — **$40,100**
10. Memory Corruption - Generic — **$30,000**



Internet and Online Services

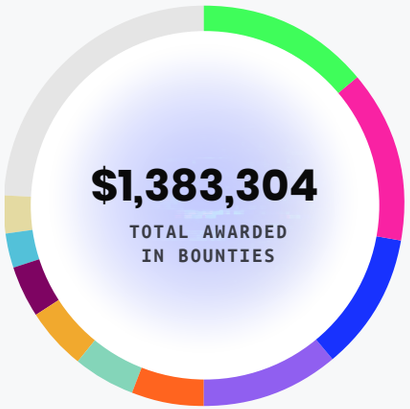
1. XSS — **$2,281,588**
2. Improper Access Control - Generic — **$1,277,983**
3. Improper Authentication - Generic — **$1,211,035**
4. Information Disclosure — **$947,082**
5. Insecure Direct Object Reference (IDOR) — **$775,218**
6. Privilege Escalation — **$742,010**
7. Code Injection — **$632,735**
8. Improper Authorization — **$523,896**
9. SQL Injection — **$505,955**
10. Server-Side Request Forgery (SSRF) — **$455,315**



Check Out What The Top 10 Vulnerabilities Are In Your Industry

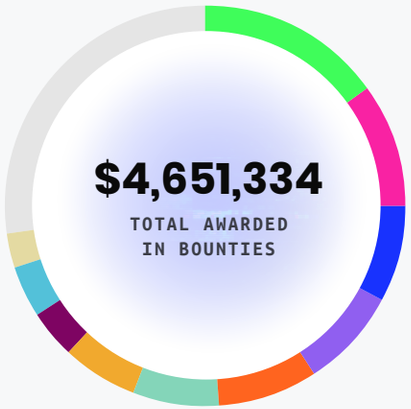
Retail and Ecommerce

1. Information Disclosure — **$197,190**
2. XSS — **$193,313**
3. Improper Access Control - Generic — **$146,710**
4. Insecure Direct Object Reference (IDOR) — **$145,362**
5. Privilege Escalation — **$82,200**
6. Code Injection — **$73,450**
7. Improper Authentication - Generic — **$64,910**
8. SQL Injection — **$60,700**
9. Business Logic Errors — **$43,425**
10. Path Traversal — **$36,420**



Telecoms

1. XSS — **$712,062**
2. Insecure Direct Object Reference (IDOR) — **$446,230**
3. Misconfiguration — **$382,101**
4. OS Command Injection — **$375,900**
5. Information Disclosure — **$354,050**
6. Incorrect Authorization — **$348,150**
7. Code Injection — **$293,325**
8. Improper Authentication - Generic — **$179,354**
9. Improper Access Control - Generic — **$177,257**
10. Authentication Bypass Using an Alternate Path or Channel — **$140,371**



Financial Services, Software, And Retail Are Most Common Targets For Hackers

Despite hackers focusing on financial services, software, and retail, growth in these areas remained steady and we saw the highest growth in newer sectors to adopt hacking solutions, including automotive and pharmaceuticals.

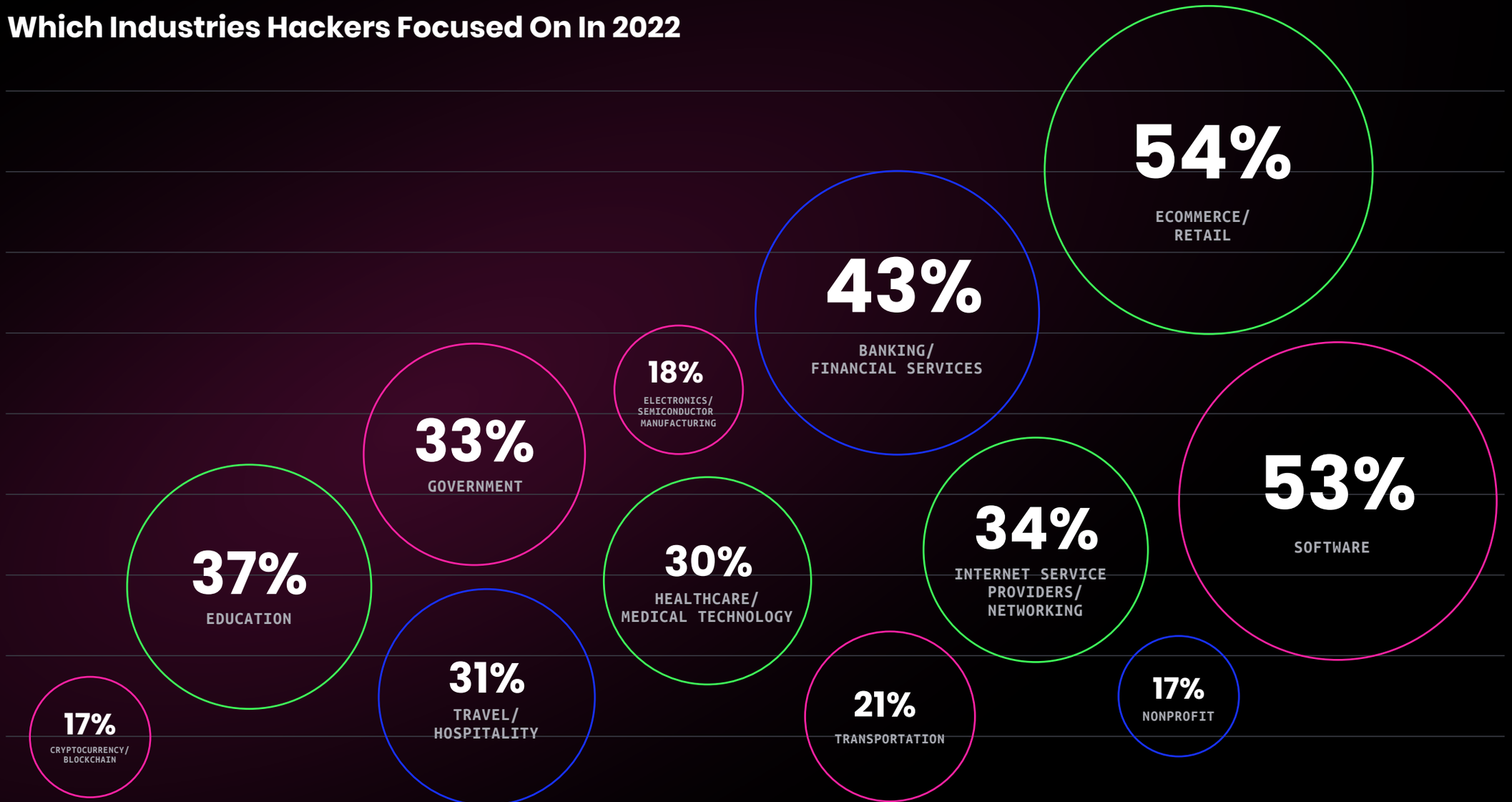
Highest Growth

400%
AUTOMOTIVE

700%
PHARMACEUTICALS

FINANCIAL SERVICES, SOFTWARE, AND RETAIL
ARE MOST COMMON TARGETS FOR HACKERS

Which Industries Hackers Focused On In 2022



2022 saw a 45% increase in program adoption. The automotive industry saw a 400% increase in program adoption, cryptocurrency and blockchain saw 143% growth, and telecommunications saw 156% growth.

Program Adoption

45%

INCREASE

Program Growth

143%

CRYPTOCURRENCY & BLOCKCHAIN

156%

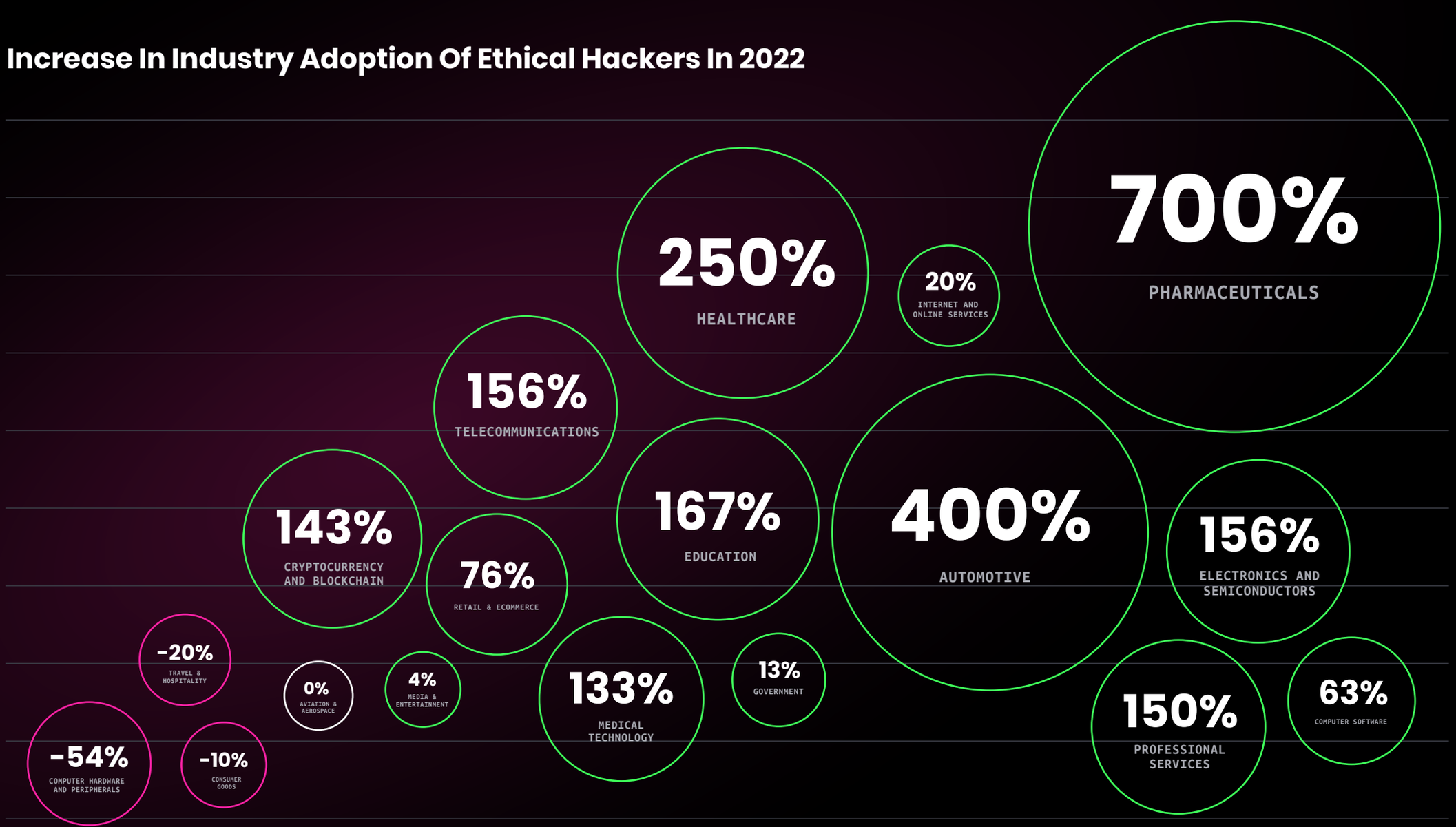
TELECOMMUNICATIONS

"Users of Web3 applications are beginning to expect to see a bug bounty program associated with the application, as it signals a more mature security posture. However, In the Web3 world, bug bounty programs often serve a different function than in the more traditional Web2 space — for example: if a smart contract that has $100M of cryptocurrency locked in it has a critical vulnerability, then that means an attacker could steal or destroy all $100M ... but, if a program offers a $1M bug bounty, it may encourage the attacker to just report the issue and collect the bounty legally and cleanly."

DANE SHERRETS, SENIOR SECURITY ARCHITECT, HACKERONE

FINANCIAL SERVICES, SOFTWARE, AND RETAIL
ARE MOST COMMON TARGETS FOR HACKERS

Increase In Industry Adoption Of Ethical Hackers In 2022



FINANCIAL SERVICES, SOFTWARE, AND RETAIL ARE MOST COMMON TARGETS FOR HACKERS

Overall, in 2021 median bounty prices fell slightly, while average bounties increased across many industries. Average bounties for financial services continue to increase; whereas, average payouts for critical bugs in retail have fallen by 15% and software by 30%. The cryptocurrency and blockchain industry saw the most dramatic increase in bounty spend; the median spend for a critical bug rose from $2,000 to $3,000 but the average payout increased by 315%, from $6,443 in 2021 to $26,728 in 2022. Governments have also upped the bounties for their programs, with the value of the average critical bug rising by 82%.

Cryptocurrency and Blockchain

2021

$2,000

AVERAGE SPEND

2022

$3,000

AVERAGE SPEND

2021

$6,443

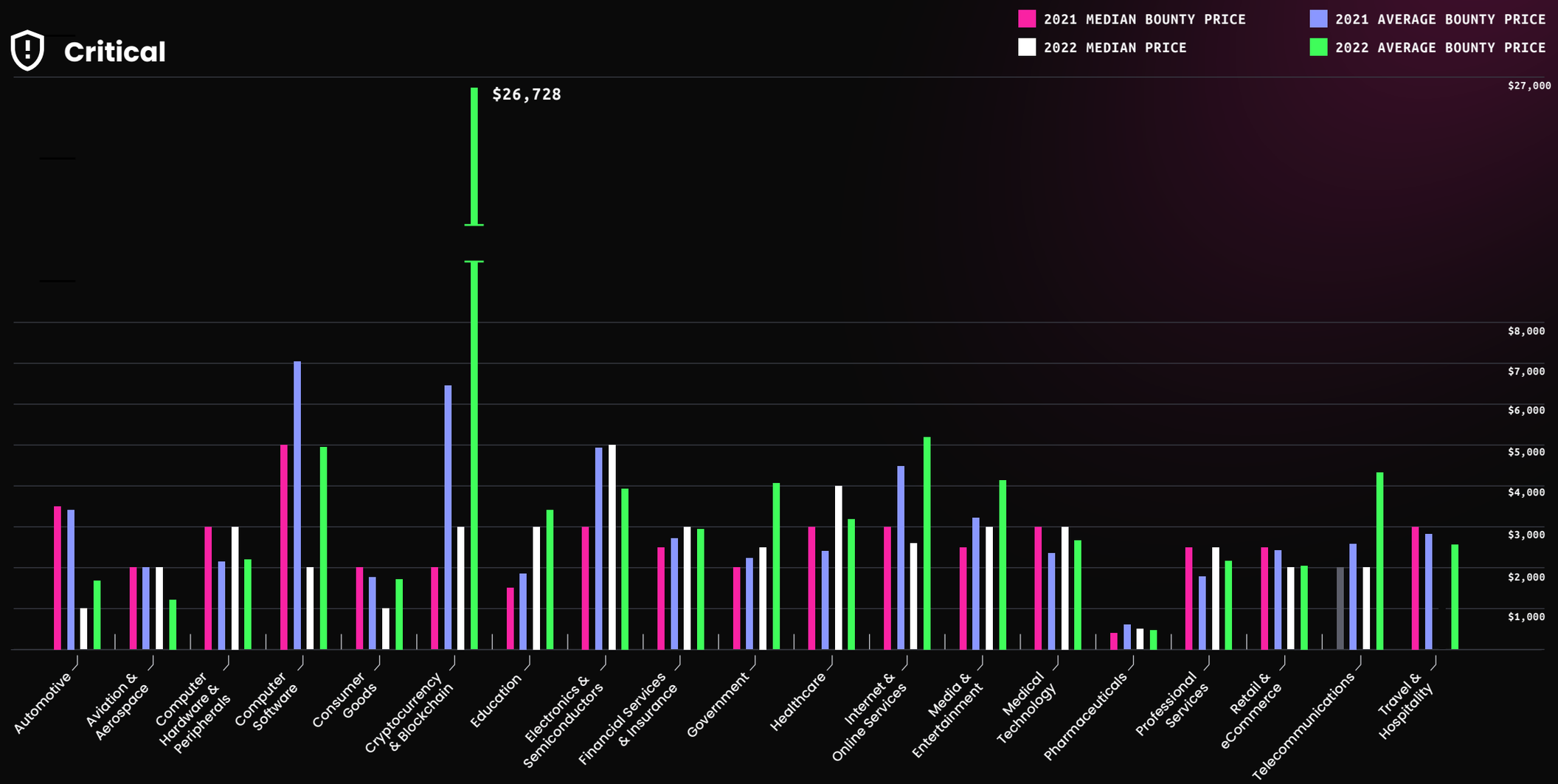
AVERAGE PAYOUT

2022

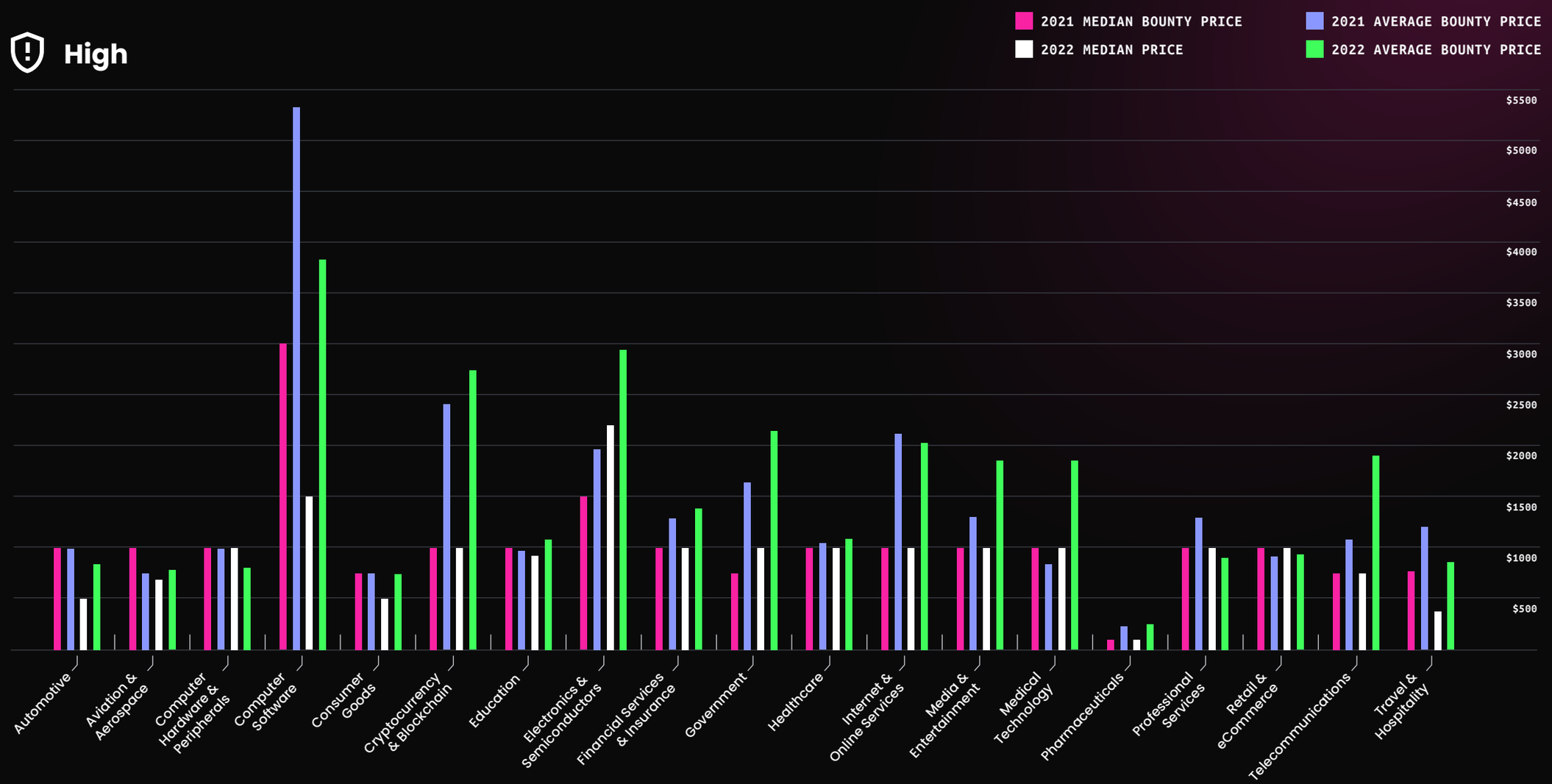
$26,728

AVERAGE PAYOUT

Median and Average Bounty Prices in 2022

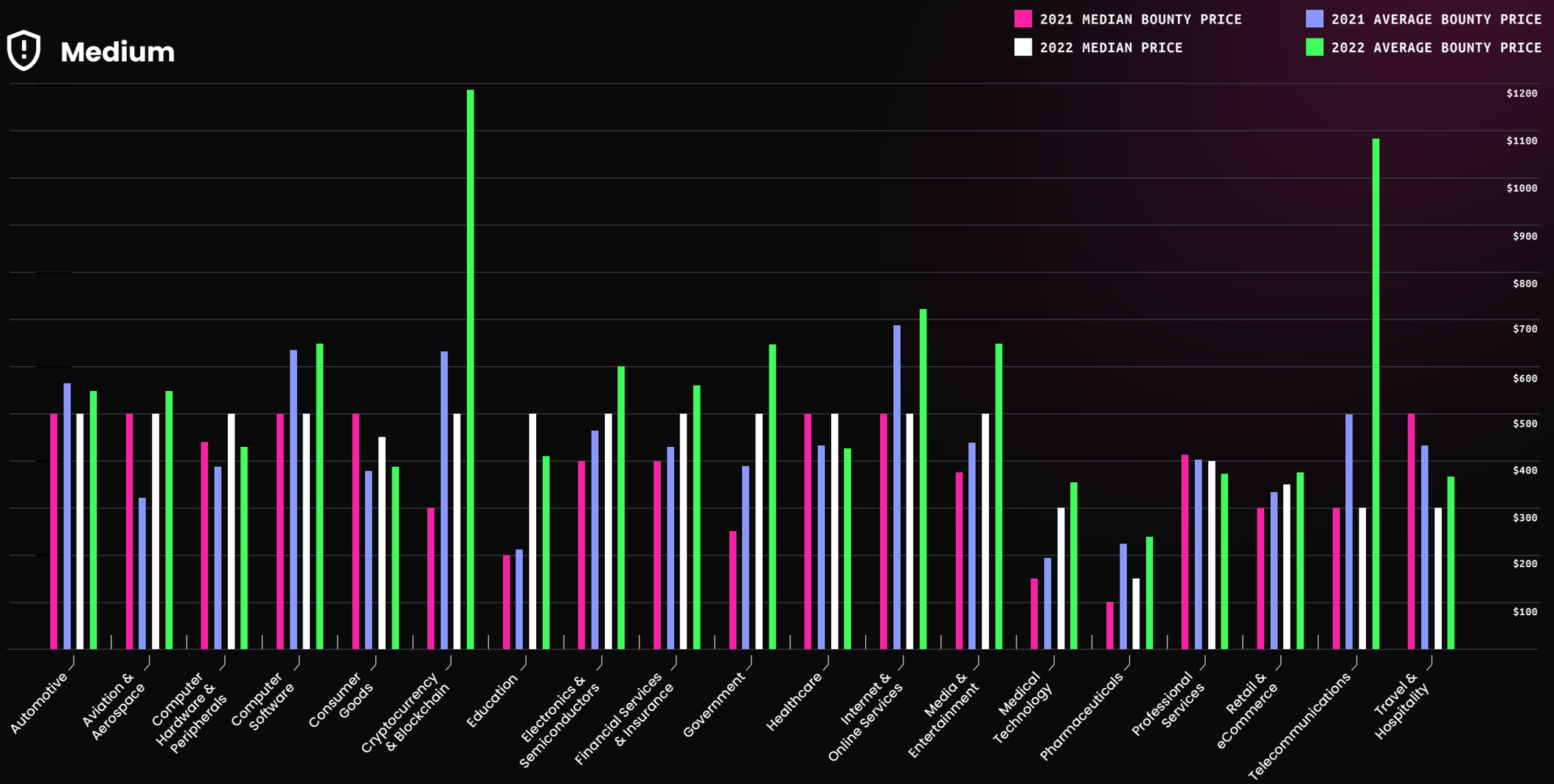


Median and Average Bounty Prices in 2022



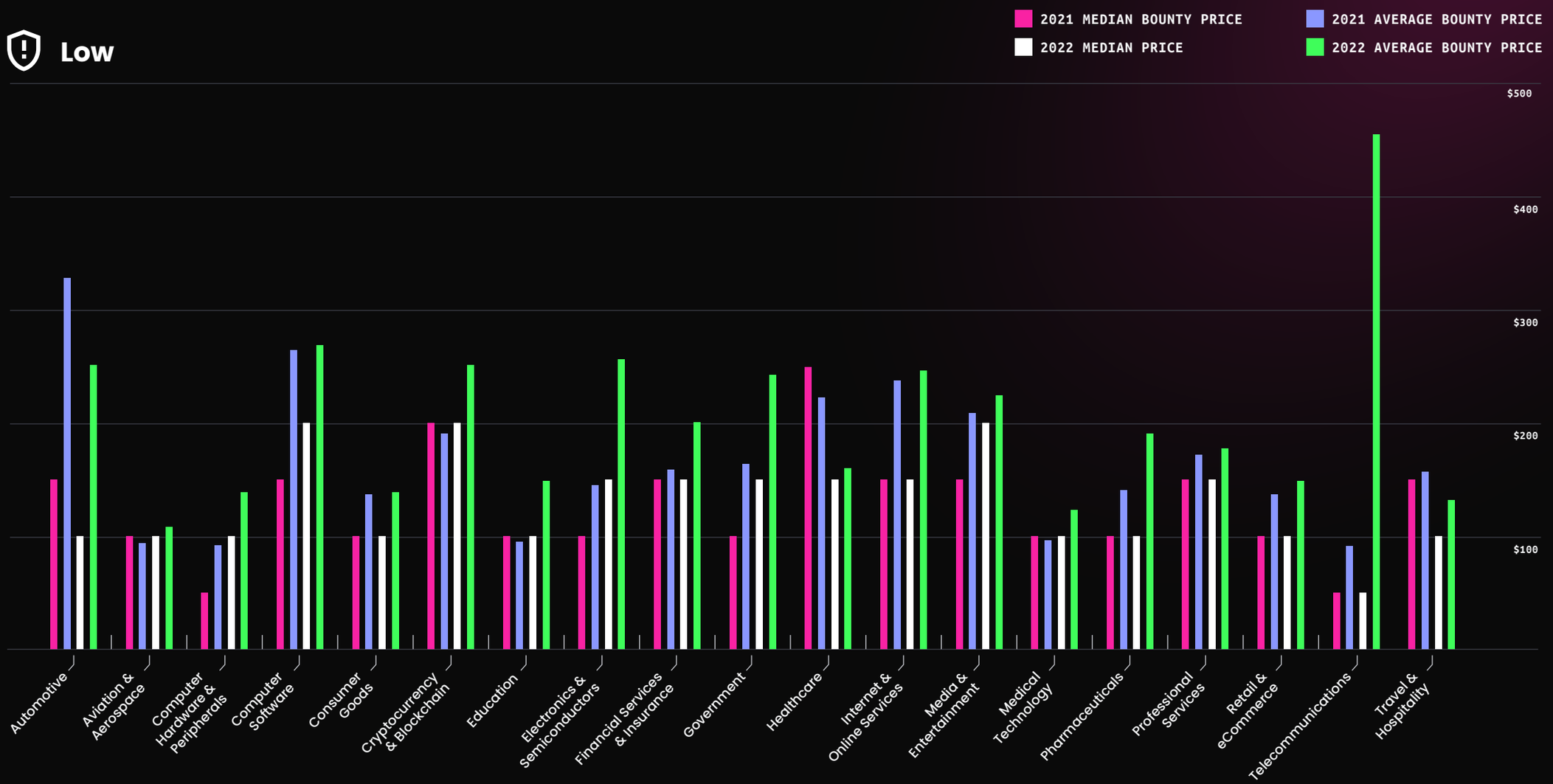
Median and Average Bounty Prices in 2022

Medium



Median and Average Bounty Prices in 2022

Low



Hackers' Reconnaissance Skills Augment Attack Surface Management Tools

Eighty eight percent of hackers say they see attack surfaces growing and 32% say they don't think organizations are running a sufficient number of security tests.

Thirty eight percent of hackers say organizations' biggest challenge is a lack of in-house skills and expertise, followed by a lack of visibility into the attack surface (28%).

Hackers use a variety of tools, including scanning tools. Eighty seven percent use Burp Suite, and 38% use web proxies/scanners. However, 92% of hackers believe hackers can find vulnerabilities scanners can't.

88%

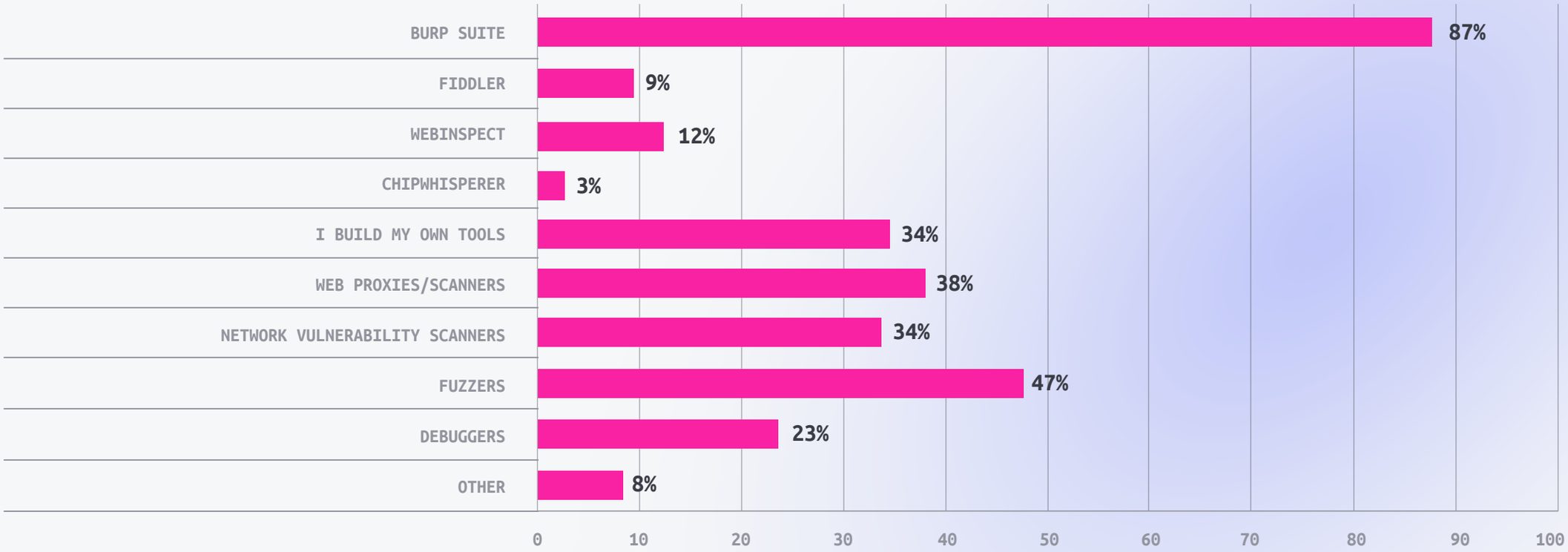
OF HACKERS SEE ATTACK SURFACES GROWING

32%

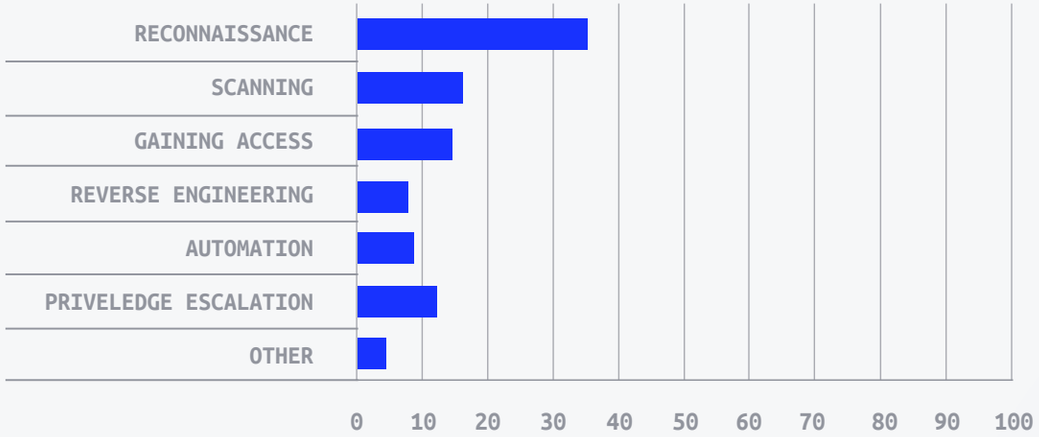
OF HACKERS SAY THEY DON'T THINK ORGANIZATIONS ARE RUNNING ENOUGH SECURITY TESTS

The Tools Hackers Use

When it comes to specialized skills, 35% of hackers say they are most skilled in reconnaissance, the information-gathering stage of hacking with the goal of identifying as many potential attack vectors as possible. With the recent launch of HackerOne Assets, the product harnesses this skill and combines with automated testing to effectively map an organization's attack surface.



The Skills Hackers Specialize In



Introducing HackerOne Assets

HackerOne Assets combines the core capabilities of Attack Surface Management (ASM) with the expertise and reconnaissance skills of ethical hackers to bring visibility, tracking, and risk prioritization to an organization's digital asset landscape. With Assets, customers can manage both the discovery and testing of assets in a single platform. The solution blends security expertise with asset discovery, continuous assessment, and process improvements to reduce risk. HackerOne's community of ethical hackers enrich the asset and scan data and analyze it themselves, ensuring that newly found assets are tested for risk and mapped according to their metadata. Once the assets have been identified and ranked for risk, security teams can use these insights to initiate pentests on newly discovered assets and add assets to their bug bounty scope.

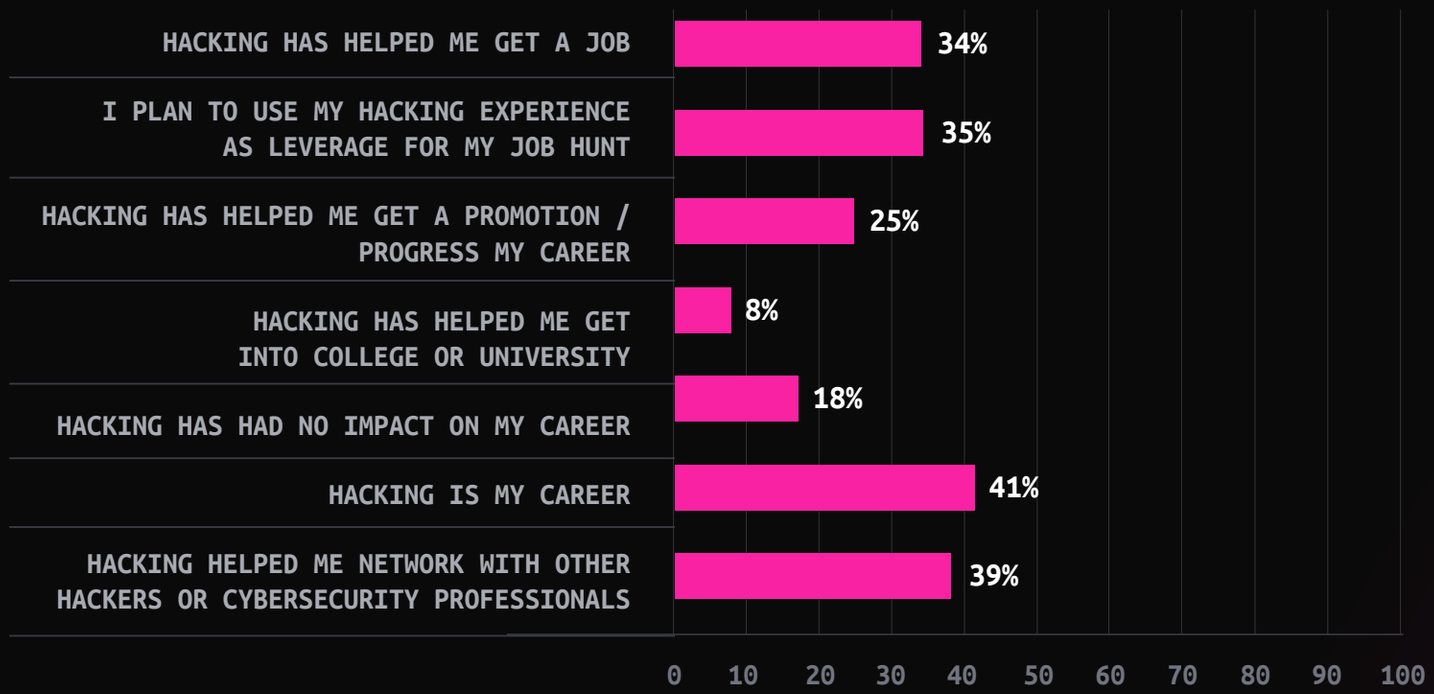
"I use automated tools in my reconnaissance flow to find opportunities where to focus my efforts. While it can send immediate notification of a quick win, I'm more interested in collecting as much information as possible from various data repositories to analyze trends. Specifically, I'm identifying where an organization will likely store specific files or documentation which I can leverage into more advanced attacks. Performing recon with a purpose helps me develop a better picture of the landscape and quickly narrow down my list of targets from 5000 to 500."

JON COLSTON, HACKER, USA

Hacking Is A Stepping Stone To A Great Infosec Career

Thirty five percent of hackers have secured a job based off their hacking experience and 26% say it's helped them get a promotion or progress in their career.

How Hacking Has Developed Infosec Careers



"Hacking gave me a career because I dropped out of school, so my HackerOne profile was my resume. I now work as a senior security engineer at European DIY, Gardening and Housing Marketplace, ManoMano, and I wouldn't have got that job without my hacking experience. I now run the bug bounty program and encourage other young hackers to develop their skills."

RONI CARTA, HACKER, FRANCE

Conclusion

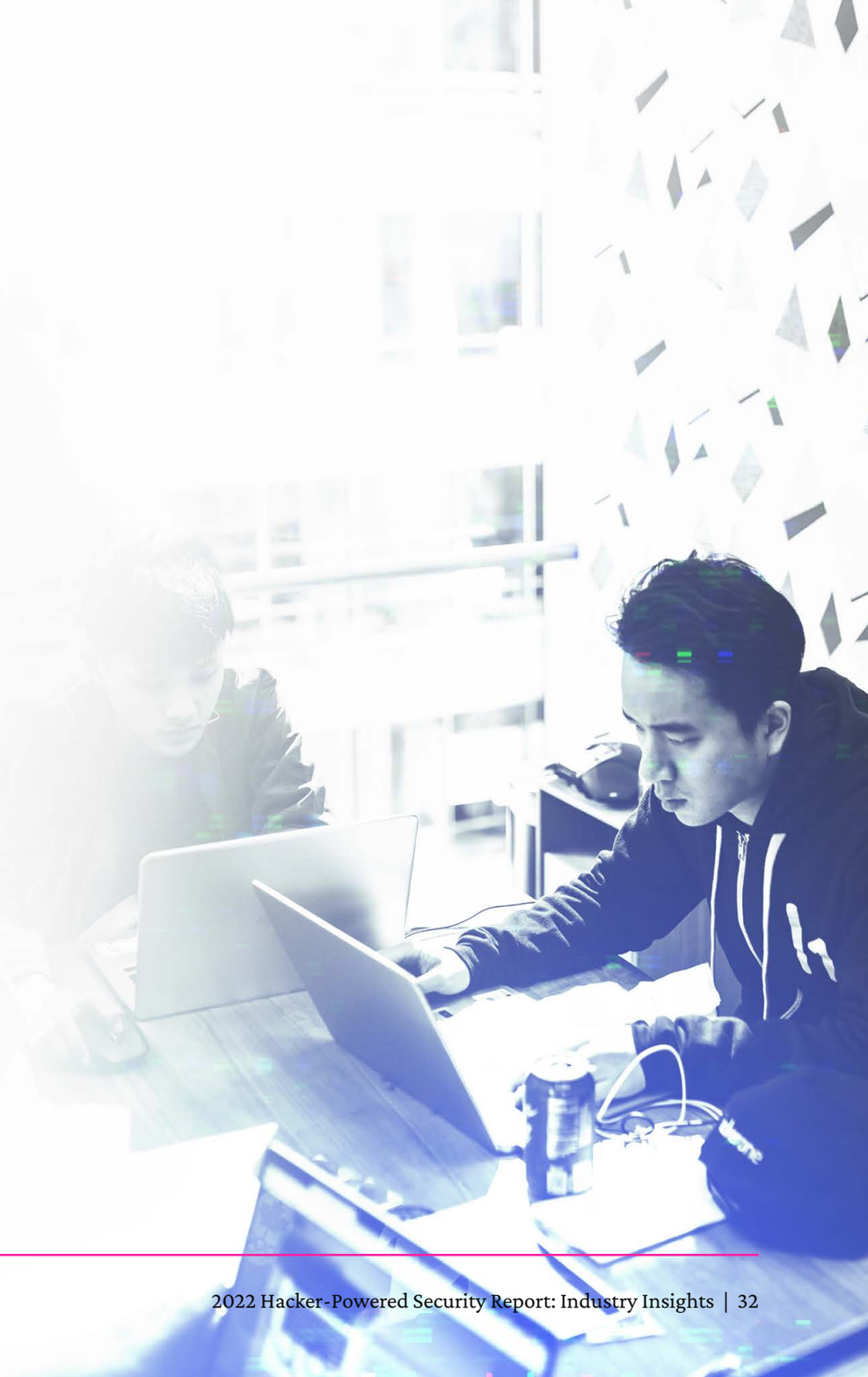
The 2022 Hacker-Powered Security Report has shown that hackers are more dedicated than ever before, and have increasingly diverse skillsets and specialities. The vulnerability data demonstrates the vulnerabilities that are the most impactful for HackerOne customers and what hackers are being incentivized to discover. It's this unique approach that combines the human insight of hackers and the dataset of collective vulnerabilities that sets Attack Resistance Management approach to closing security gaps apart.

Interested in finding out more about how hackers can help close your attack resistance gap? Read more.

Research

The Hacker Survey was conducted in September 2022 and surveyed 5,738 hackers worldwide

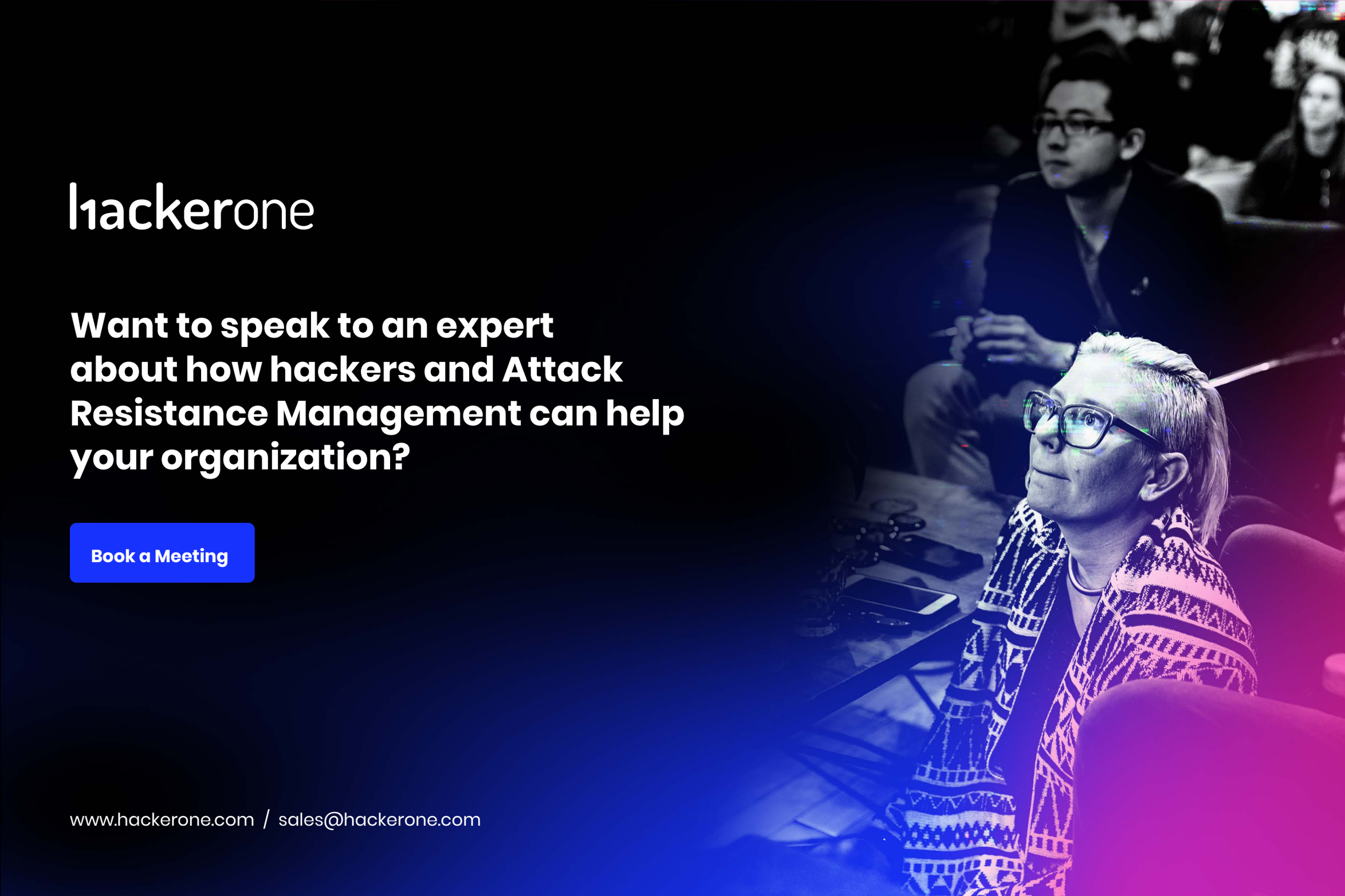
The data from the HackerOne platform covers the period June 2021 – June 2022



hackerone

Want to speak to an expert about how hackers and Attack Resistance Management can help your organization?

Book a Meeting



www.hackerone.com / sales@hackerone.com