hackerone

THE
2021

HACKER REPORT

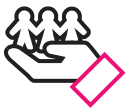
UNDERSTANDING HACKER MOTIVATIONS,
DEVELOPMENT AND OUTLOOK

Executive Summary

In the last year, the world has shifted to be digital-first, requiring security teams to rapidly adjust. At the same time, evolving attack surfaces and complex digital ecosystems introduce new challenges for cybersecurity teams. Cybersecurity too has become increasingly automated to keep up with new threats, but security teams still face an uphill battle when it comes to scaling expertise and covering shifting digital landscapes. Automated scanners help organizations defend against known threats, but it takes human creativity to link several low-severity vulnerabilities together to help a customer avoid a breach, or find a unique bypass to a software patch.

Hackers have risen to the challenges presented by the past year, from supporting businesses through rushed digital transformations to committing more time to protecting healthcare providers. The 2021 Hacker Report celebrates the diverse and robust expertise within the largest global hacker community and their symbiotic partnership with the security teams they work with.

Key Findings



63%

increase in the number of hackers submitting vulnerabilities over the past 12 months.

20

the average number of vulnerability categories top hackers report across.

53%

rise in submissions for Improper Access Control and Privilege Escalation.

310%

increase in reports for Misconfiguration.

50%

of hackers have not reported a bug because of a lack of a clear reporting process or a previous negative experience.

85%

of hackers hack to learn and **62% do it to advance their career.**

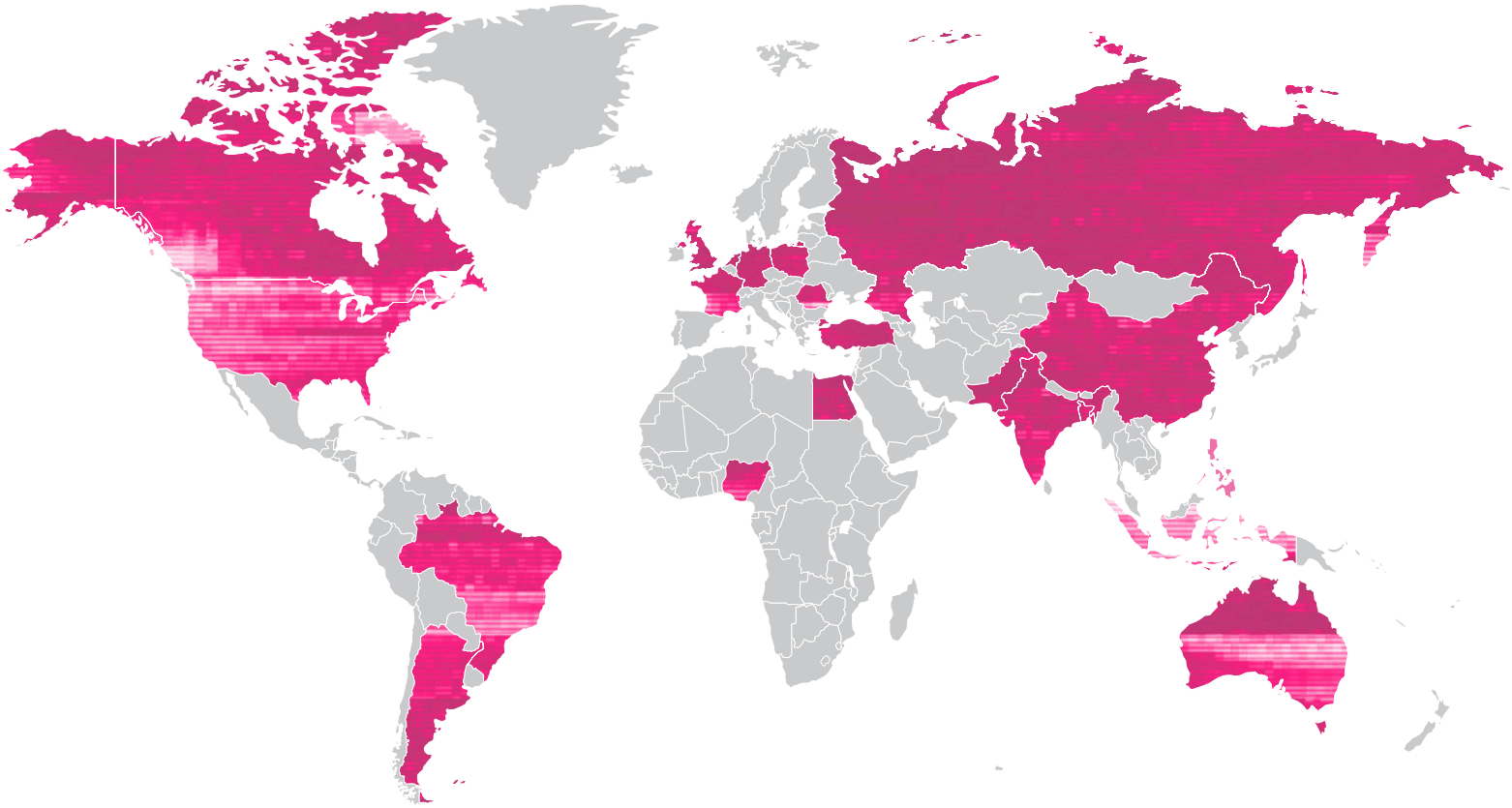
The Hacker Community

Since the release of the 2019 Hacker Report two years ago, the HackerOne community has doubled in size to over one million registered hackers. While much of the community is still exploring and learning, there has been a 63% increase in the number of hackers submitting reports in 2020. That's a 143% increase since 2018, demonstrating that hackers are growing their skills and expertise as organizations and industries across the globe invest in hacker-powered solutions.

Hackers earned $40 million in 2020 alone, contributing to reaching the milestone of $100 million paid out to hackers on the HackerOne platform. Nine hackers have earned over $1 million dollars on the platform since 2019, and one hacker passed the $2 million mark in 2020.

HACKERS AROUND THE GLOBE

TOP COUNTRIES REPRESENTED ON HACKERONE



82%
Of Hackers Hack Part-Time

55%
Are Under 25 Years of Age

The majority (82%) of the community define themselves as part-time hackers and 35% have a full time job. Despite the majority claiming to be self-taught, many have a technical background: 37% of hackers have studied computer science at a post graduate level and 20% hold post graduate qualifications in computer science.

Hacking remains a popular pursuit for Generation Z, with 55% of the community under 25 years old. Hacking is paving the way for their future; 33% have leveraged their skills to secure a job and 23% plan to continue their career in information security within an internal security team. Hackers are both enhancing an organization's security capabilities with bug hunting efforts and starting to bring their skills the hacker mindset to internal security functions.

SPOTLIGHT:

I AM A PENTESTER

LEANDRO BARRAGAN

@none_of_the_above

ARGENTINA

6 YEARS HACKING

"As a pentester, I have a broad range of knowledge and I'm a quick learner, adapting to new ventures and fields. Technology develops so fast that you can't know every detail of every new development, but either having a background in computer science or being self motivated to learn really helps to understand how to attack a new product in a short time frame. Sometimes it's not so much a matter of skill, but of tenacity, mindset, and persistence."

Hacker Motivations

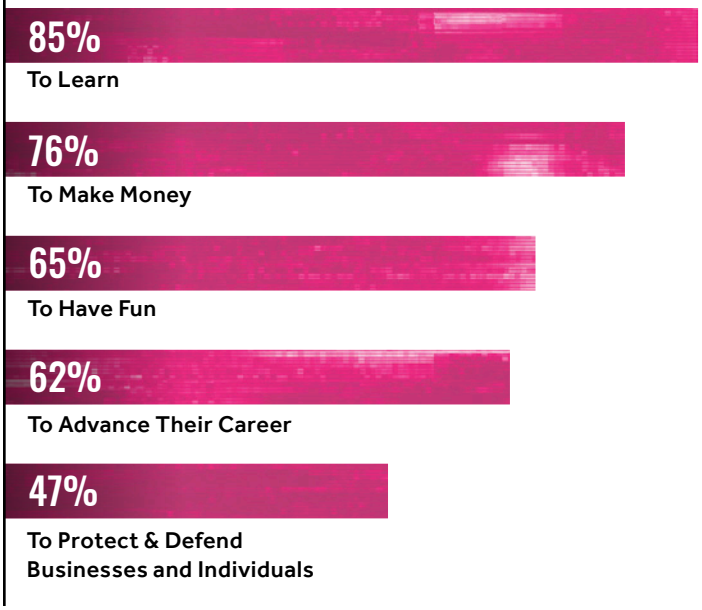
From part-time hackers to full-time pentesters, the hacking community brings a diversity of approaches, skill sets, and philosophies to organizations they are invited to test.

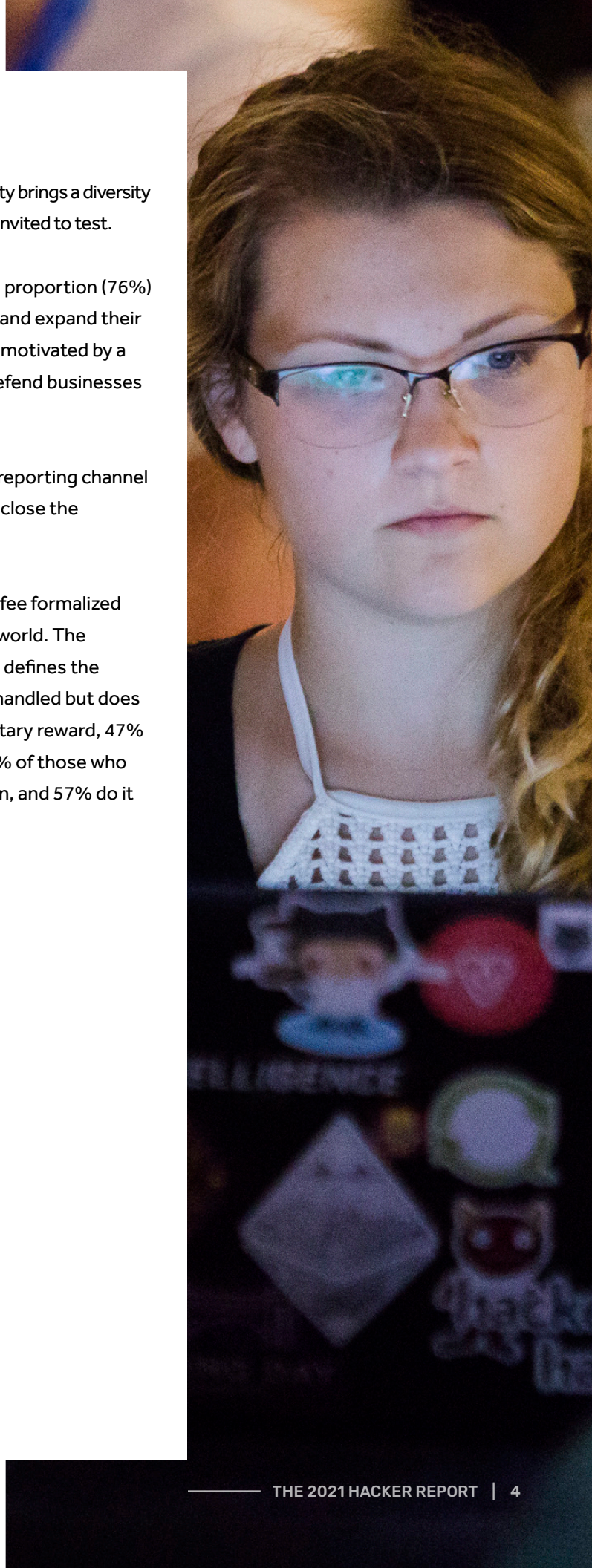
Keeping hackers motivated isn't all about the money. While a high proportion (76%) are motivated by bounties, 85% of them are also doing it to learn and expand their skill sets and 62% do it to advance their careers. Hackers are also motivated by a desire to do good in the world with 47% hacking to protect and defend businesses and individuals from cyber threats.

When hackers find a bug they want to report it. But, if an obvious reporting channel is unavailable, hackers are faced with a choice to do nothing or disclose the vulnerability publicly.

A vulnerability disclosure program (VDPs) is an organization's no-fee formalized method for receiving vulnerability submissions from the outside world. The VDP instructs hackers on how to submit vulnerability reports and defines the organization's commitment to the hacker on how reports will be handled but does not incentivize research with bounties. Despite offering no monetary reward, 47% of the community actively participates in VDPs. Furthermore, 51% of those who hack VDPs do so out of a sense of responsibility, 79% do it to learn, and 57% do it to build up their reputation on the platform.

WHY DO HACKERS HACK?





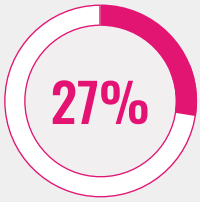
SPOTLIGHT:

I HACK EXCLUSIVELY ON VDPs

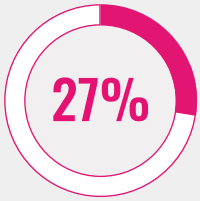
ALFIE NJERU
@emenalf
KENYA
8 YEARS HACKING

"I understand that money is a big motivation when it comes to bug bounty but, on the flip side, I have gained a lot of skills and exposure from hacking on VDP programs, especially those with wide scope. VDPs provide an opportunity to test out my skills, and tools without fear of litigation."

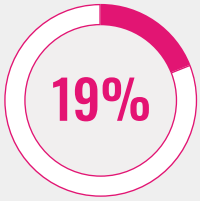
50% OF HACKERS HAVE NOT DISCLOSED A BUG THEY FOUND.



Failed to report a bug because there was no channel through which to disclose it.



Failed to report a bug because the company had previously been unresponsive or difficult to work with.



Failed to report a bug because no bounty was offered.

Despite their commitment to reporting bugs when they find them, 50% of hackers have, at one time or another, chosen not to disclose a bug they have found. Of those, 27% said this was because there was no channel through which to disclose it and another 27% said it was because the company had previously been unresponsive.

Money remains a key motivator for hackers with 76% doing the job to make money so it's perhaps not surprising that 19% have chosen not to disclose a bug they've found if a bounty isn't offered for their efforts.

Having a VDP that clearly outlines how your organization wants vulnerabilities to be reported gives hackers a clear, safe channel for reporting and provides a single stream for vulnerability intake from third parties for security teams.

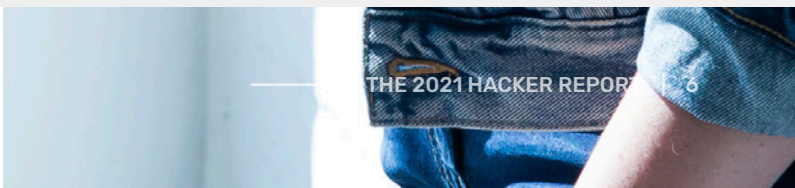
WHICH INDUSTRIES ARE HACKERS WORKING WITH?

59% Internet and Online Services
47% Fincancial Services Orgs
43% Computer Software Orgs
41% Retail & Ecommerce
37% Media & Entertainment
32% Educational Institutions
31% Government Programs
26% Leisure & Hospitality
25% Telecommunications
25% Professional Services
23% Healthcare Orgs
20% Consumer Goods Firms
16% Medical Technology
14% Semiconductors
14% Crypto and Blockchain Tech
14% Automotive
13% Computer Hardware
10% Aerospace
10% Non-Profit

Hacker Expertise & Impact

Hackers bring specialized skills and domain expertise to help security teams scale testing across agile attack surfaces. With an outsider's perspective, different approaches, experiences, and knowledge, hackers can submit impactful vulnerabilities, which means your attack surface is better protected.

Hackers are represented across all industries, with 59% of hackers focusing on internet and online services and 47% on financial services. 41% of hackers hack on retail & ecommerce programs, and 43% hack on computer software programs.

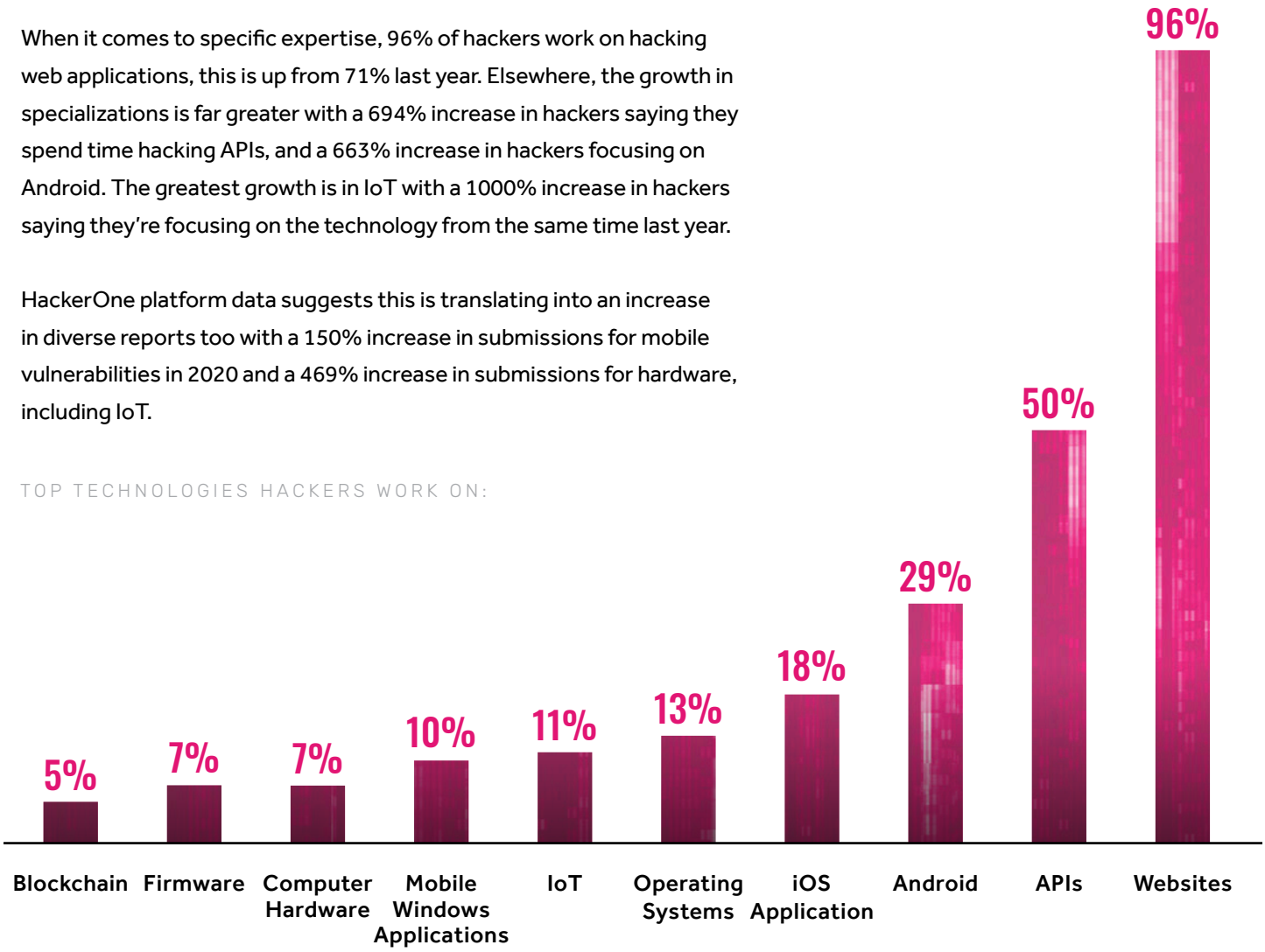


WHAT TECHNOLOGIES ARE HACKERS WORKING ON?

When it comes to specific expertise, 96% of hackers work on hacking web applications, this is up from 71% last year. Elsewhere, the growth in specializations is far greater with a 694% increase in hackers saying they spend time hacking APIs, and a 663% increase in hackers focusing on Android. The greatest growth is in IoT with a 1000% increase in hackers saying they're focusing on the technology from the same time last year.

HackerOne platform data suggests this is translating into an increase in diverse reports too with a 150% increase in submissions for mobile vulnerabilities in 2020 and a 469% increase in submissions for hardware, including IoT.

TOP TECHNOLOGIES HACKERS WORK ON:



+694%
Hacking APIs
compared to last year

+663%
Hacking Android
compared to last year

+1000%
Hacking Internet of Things
compared to last year

As attack surfaces expand and organizations shift to the cloud, hackers will continue shoring up vulnerabilities and providing the valuable insights that lead to more securely designed products.

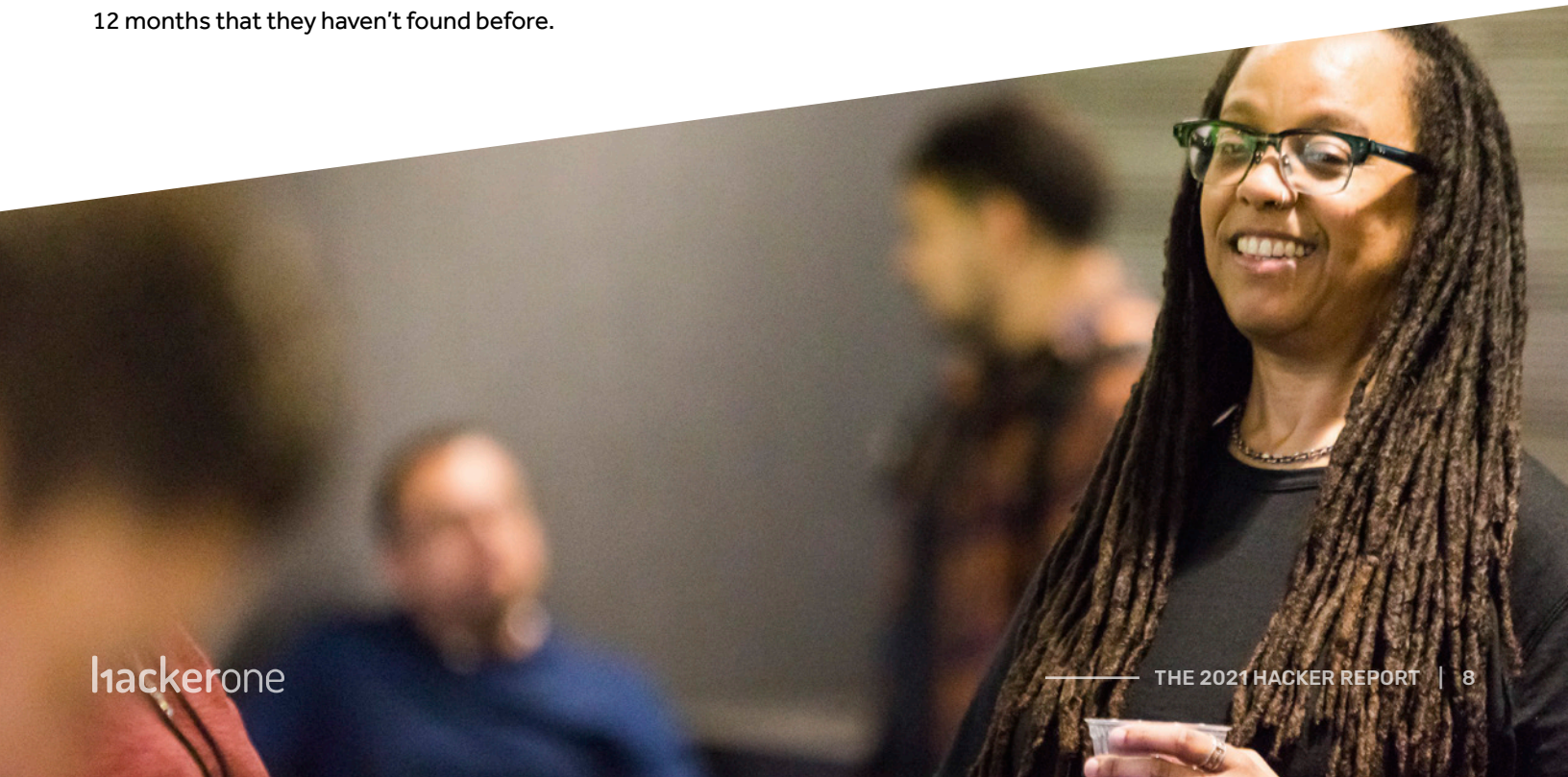
Data from the HackerOne platform also shows growth in most vulnerability categories year-over-year. Of the Top 10 Vulnerabilities, Information Disclosure has seen the biggest increase in valid submissions with 65% growth in the past year. While not yet one of the top ten reported vulnerabilities, reports for misconfiguration, no doubt driven by the pandemic-led shift to the cloud, grew by 310% in 2020.

The hacking community is also evolving to become more agile, more efficient and more sophisticated as hacker-powered security is widely adopted. In the past year, it took an average of just 16 days from the point a hacker joined the platform to reporting their first bug. This is down from 148 days in the previous year. Top hackers, on average, report bugs across 20 different vulnerabilities.

While hackers are finding new bugs and new ways of exploiting them, 49% of hackers believe attack surfaces are in fact hardening, as low hanging vulnerabilities are found and fixed. Although 26% of hackers say it's getting harder to find bugs, 45% of hackers do say they've found bugs over the last 12 months that they haven't found before.

YoY Growth of the Top Ten Vulnerabilities

1	Cross Site Scripting	+23%
2	Information Disclosure	+65%
3	Improper Access Control	+53%
4	Improper Authentication	+44%
5	Privilege Escalation	+54%
6	Insecure Direct Object Reference	+49%
7	Cross Site Request Forgery	+7%
8	Server Side Request Forgery	+18%
9	SQL Injection	+48%
10	Code Injection	+19%



SPOTLIGHT:

HTTP REQUEST SMUGGLING

HTTP REQUEST SMUGGLING REPORTS OVER TIME

Before 2017 there was not a single report of the long forgotten HTTP request smuggling vulnerability on the HackerOne platform. But, by 2019, hacker and security professional James Kettle had sent the community into a flurry of action when he disclosed his research on this old vulnerability, made relevant with new techniques. In the research, Kettle showed that request smuggling is a major threat to the web, that HTTP request parsing is a security-critical function, and that tolerating ambiguous messages is dangerous. Since then, hackers have used his research to identify the vulnerability on systems around the world, helping companies secure themselves against a previously under valued threat. From seeing just 127 reports in 2018, by 2019 this had increased to 438. HTTP request smuggling reports doubled again in 2020 with 848 reports submitted for the vulnerability.

SPOTLIGHT:

I STARTED ON HACKERONE WITH A CTF

ROBERT VULPE
@nytr0gen
ROMANIA
10 YEARS HACKING

"The first CTF I participated in from HackerOne was in 2019—it was so hard for me at that time. I got stuck somewhere in the middle and was not able to continue. After seeing the writeups and realizing my mistake, I committed to finishing the next CTF with a great writeup. Fast forward to the last H1 CTF, many hackers sent me messages about how much they've learned from my writeup. It's fantastic to help out the community and grow together!"

The Future of the Community

In a little over two years, HackerOne's community of potential hackers has doubled in size to over one million registered on the platform, and will continue to grow in skill and size through education and collaboration.

Since 2012, HackerOne has invested heavily in building resources and creating opportunities for the hacker community to learn and grow their skill sets. In fact, a quarter of hackers surveyed are learning from online resources, including Hacker101 and Hacktivity. Hacker101 is HackerOne's dedicated resource for hackers that provides free online webinars and lessons for anyone who wants to learn how to hack for good. Hacker101 CTFs (capture the flags) empower learners to find bugs in a simulated environment. In the past year alone, over 66,000 hackers found 420,000 flags in CTF challenges, up from 49,000 hackers finding 317,000 flags in 2019.

Conclusion

With budgets and staff being cut for a quarter of security teams since the pandemic, organizations are being forced to secure more with less, at scale. Meanwhile hackers have been busier than ever. 38% have spent more time hacking since the start of the pandemic and 34% have earned more in bounties. 34% of hackers said they have seen more bugs as a result of pandemic led digital transformation and 50% said that, overall, attitudes towards hackers are becoming more positive.

Traditional solutions can no longer keep pace with the dual requirements of speed and security. Internal security teams struggle to scale their skills and expertise with the growing and agile attack surfaces brought on by rapid digital transformation and remote working. Inviting hackers to share their insights means security teams can extend their reach and expertise to be better prepared for emerging threats.

"As businesses recover from this pandemic and economies are rebuilt, I predict that there will be an uptick in application development and deployment. That means the rapid introduction of new assets, applications and networks; and therefore fresh attack surfaces. With the shift to the cloud, companies are adopting newer technologies like Kubernetes to orchestrate the deployment of critical applications and services. New technologies and methodologies mean there are usually misconfigurations along the way that lead to vulnerabilities. Fortunately, there has definitely been a shift in perspective when it comes to working with security researchers. Hackers are seeing large corporations embrace security vulnerabilities from researchers as a core part of their security processes."

—SHUBHAM SHAH
@notnaffy
AUSTRALIA

WITH INSIGHTS FROM OVER 2,000 HACKER-POWERED PROGRAMS, MORE COMPANIES TRUST HACKERONE THAN ANY OTHER VENDOR

HackerOne surfaces more vulnerabilities than any other vendor.

CONTACT US

hackerone

HACKER-POWERED SECURITY