

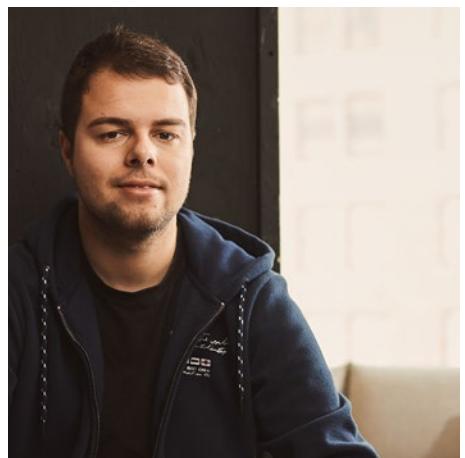


# HACK'ER

/'ha-ker/

noun

One who enjoys the intellectual challenge of creatively overcoming limitations.



# Executive Summary

Welcome to the age of the hacker. Hackers are heroes, they are in it for the good and there is more opportunity than ever before. We share some of their stories and celebrate their impact in this, the third annual Hacker Report.

The Hacker Report details the more than 300,000 individuals that represent our hacker community today. It highlights where hackers live, what motivates them, what their favorite hacking targets & tools are, where they learn, why they collaborate and much more.

In 2018 alone, Hackers earned over \$19 million in bounties, almost the entire amount awarded in the years prior combined. And while the most successful find it very lucrative, it's about so much more than money. Many are finding career building opportunities through bug bounties, with companies hiring from within the hacker community at a faster clip than ever before. Companies are utilizing bug bounty reports and hacker engagement as an enhanced resume of proven skills that will impact company goals and security efforts from day one.

The generosity and camaraderie of hackers continues to impress with more emphasis than ever before on education, collaboration, and giving back.

As hacking grows in popularity, training continues to be a focus. With more than 600 hackers registering to join the ranks any given day, in depth training modules such as [Hacker101](#) capture the flag challenges are in-demand.

This past year we saw incredible individual performances such as hackers earning \$100K for one vulnerability and the first hacker passing the \$1 million milestone. We also saw unmatched collaboration, like hackers acting as teams to report over 250 valid customer vulnerabilities.

Hackers represent a global force for good, coming together to help address the growing security needs of our increasingly interconnected society. The community welcomes all who enjoy the intellectual challenge to creatively overcome limitations. Their reasons for hacking may vary, but the results are consistently impressing the growing ranks of organizations embracing hackers through hacker-powered security—leaving us all a lot safer than before.

**300K+**  
**TOTAL REGISTERED HACKERS**

**100K+**  
**TOTAL VALID VULNERABILITIES  
SUBMITTED**

**\$42M+**  
**TOTAL BOUNTIES PAID**

\*As of December 2018

# Table of Contents

Hacker Definition .....	2
Executive Summary .....	3
Key Findings .....	6
<b>Geography</b> .....	8
The International Flow of Bug Bounty Cash .....	10
The Economics of Bug Hunters .....	12
Hacker Spotlight: Jesse   @randomdeduction .....	14
<b>Demographics</b> .....	15
Age .....	16
Trends in Hacker Education .....	18
<i>Introducing Hackboxes and the Hacker101 Capture the Flag</i> .....	19
Profession .....	20
Hours Per Week Spent Hacking .....	21
<i>Blockchain Hacker Trends</i> .....	22
Hacker Spotlight: Ron   @ngalog .....	23
<b>Experience</b> .....	24
Hacker Spotlight: Tanner   @cache-money .....	26
<i>Vulnerability Spotlight 1: XSS in Stream React Chat Client</i> .....	27
<b>Targets &amp; Tools</b> .....	28
Favorite Tools .....	29

Hackers Love Researching Websites, APIs and Technology That Holds Their Own Data .....	30
Hacker Spotlight: Andre   @0xacb .....	31
<i>Vulnerability Spotlight 2: SSRF in Exchange Leads to ROOT Access in all Instances .....</i>	32
<b>Motivation .....</b>	<b>33</b>
Curiosity Means More Than Money .....	34
Governments Lead the Way in Hacker-Powered Security .....	35
Hackers Value Good Communication, a Challenge, and Recognition When Choosing a Bug Bounty Program to Focus On .....	36
More and More Hackers Name XSS Their Favorite Attack Vector .....	38
Hacker Spotlight: Joel   @teknogeek .....	40
<i>Bringing the Community Together for Global Live Hacking Events .....</i>	41
<b>Working Together &amp; Giving Back as a Community .....</b>	<b>42</b>
Hackers Frequently Work Alone, but Like Learning From Others .....	43
Do You Actively Participate in Any Hacker Oriented Community-Based Organizations? .....	44
Hacker Spotlight: Santiago   @try_to_hack .....	45
<i>Embracing Hacker-Powered Security: Organizations Across Sectors Increasingly See Value of Hacker Efforts .....</i>	46
<i>Vulnerability Spotlight 3: Bypass 2FA Requirement and Reporter Blacklist through Embedded Submission Form on HackerOne .....</i>	48
Hacker Spotlight: Mathias   @avlidienbrunn .....	49
<b>Conclusion .....</b>	<b>50</b>
<b>Methodology .....</b>	<b>52</b>
<b>About HackerOne .....</b>	<b>52</b>



## Key Findings

\$19 million in customer bounties earned in 2018 represent nearly **the bounty totals for all preceding years combined**. At the end of 2018, hackers had earned more than \$42 million for valid results.

---

Hacker globalization provides a literal meaning to "hack the planet." India and U.S. remains the top hacker locations, and **more than 6 African countries had first-time hacker participation in 2018.**

---

The interest and attraction of joining the hacker ranks continues to skyrocket, as **the community surpassed 300,000 registered, with monthly signups growing each month of 2018.**



## Key Findings

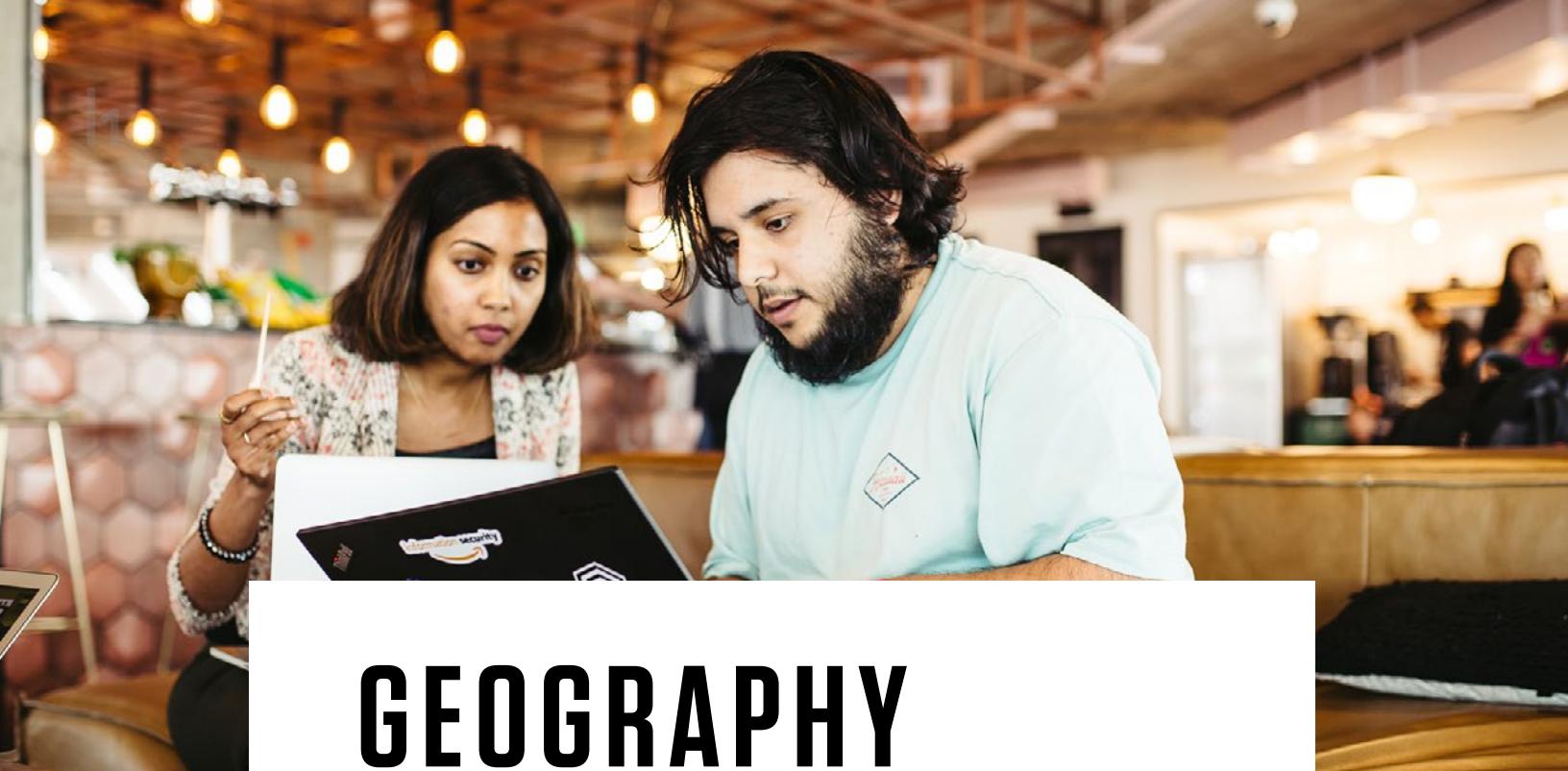
Hacker-powered security is creating opportunities across the entire globe. **Top earners can make up to 40x the median annual wage of a software engineer** in their home country respectively.

---

Hacker training continues to take place outside of the traditional classroom, as **81% say they learned their craft mostly through blogs and self-directed educational materials** like Hacker101 and [publicly disclosed reports](#). While just 6% have completed a formal class or certification on hacking.

---

Hacking for good is growing in popularity as nearly **two thirds of Americans (64%) today recognize that not all hackers act maliciously** according to recent Harris Poll data.



# GEOGRAPHY

Hackers participate from every corner of the globe.

Countries like Iceland, Ghana, Slovakia, Aruba, and Ecuador have hackers with as much determination, skill and success as those from India, the United States, Russia, Pakistan, and the United Kingdom. The latter, however, represent the top five countries contributing to hacker-powered security, with their participants comprising just over 51% of all hackers in the HackerOne community. Hackers from India and the U.S. alone account for 30% of the total, but that is a shift from 2018, when those two countries claimed 43% of the hacker community. We've seen great gains in community members and it is exciting to see the growth and hacking talent coming from outside the historically top regions.

Hacker globalization provides a literal meaning to "hack the planet". With the online nature of hacker-powered security programs, it's easy for hackers to find new and potentially lucrative opportunities from anywhere—all they need is an internet connection. On the other side of the relationship, companies and governments anywhere in the world can seamlessly work directly with leading hackers in Bangladesh and Namibia to find their most critical vulnerabilities fast. Every minute of every day, hackers and companies across the globe come together to make the internet safer for everyone.

# WHERE HACKERS ARE LOCATED IN THE WORLD



*Figure 1: Geographic representation of where hackers are located in the world.  
Remaining countries are each ≤5% of the HackerOne population.*

## KENYA

Hackers based in Kenya participated for the first time ever.

## ALGERIA

The number of hackers participating from Algeria more than doubled this year over last.

## INDIA

India remains the top hacker location for the second year.

## AFRICA

More than 6 African countries had first-time hacker participation this year.

## THE INTERNATIONAL FLOW OF BUG BOUNTY CASH

While today hackers are located in more than 150 countries, the most prolific paying organizations and highest earning hackers hail from just a few countries.

Of the \$42+ million awarded to hackers through 2018 on HackerOne, organizations in just 8 countries served as the primary source for more than half that amount. The U.S. and Canada based organizations comprise the lion share of bounties, followed by the U.K., Germany, Russia, and Singapore, all contributing significant bounty awards.

The chart below shows the collective outflow and inflow of bug bounty cash from organizations to hackers on the HackerOne platform. From when we published this graph a year ago, there has been some shuffling of the top 10 positions. Hackers from the U.S., India, and Russia continued to dominate in earnings again this year, collectively pulling in 36% of the total value of awarded bounties. Canadian hackers earned 3.3% of all bounties awarded, moving them into the top 10 this year with just under \$1.4 million earned. The Netherlands entered the top 10 as well, with Dutch hackers earning more than 3% of the total bounties awarded. Pakistan, Argentina, and Hong Kong fell out of the top 10, but hackers in each of those countries still earned at least 40% more in 2018 compared with 2017.



# GEOGRAPHIC MONEY FLOW

Where Hackers Are Located

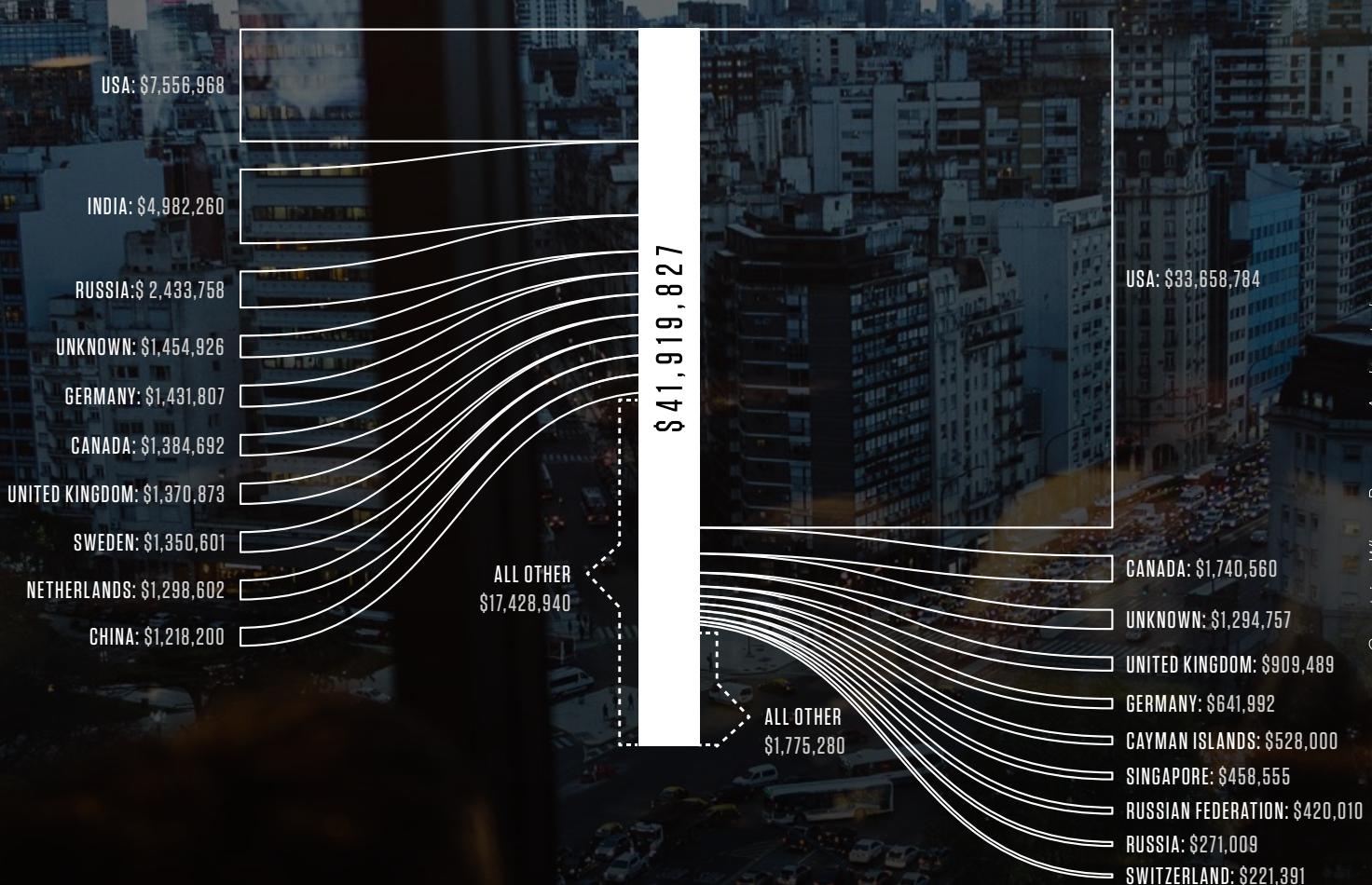
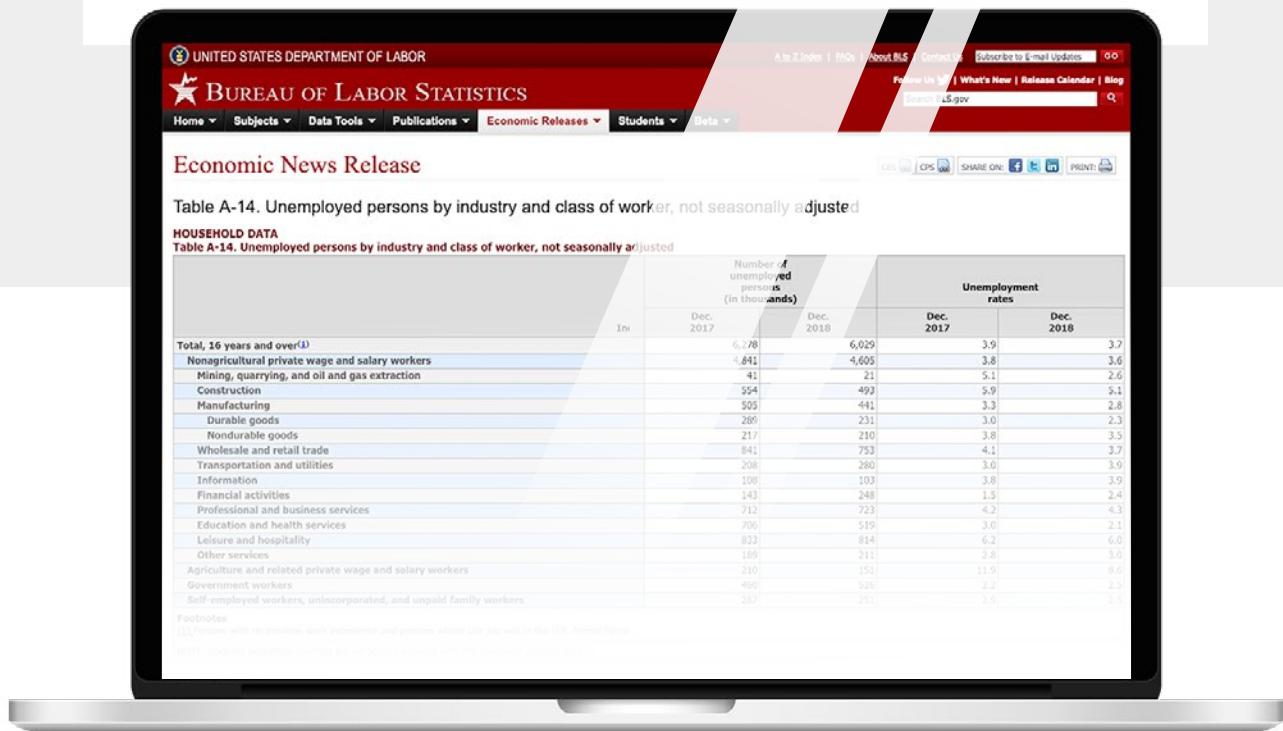


Figure 2: Visualization of the Bounties by Geography showing on the right where the organizations paying bounties are located and on the left where hackers receiving bounties are located.

# THE ECONOMICS OF BUG HUNTERS

Hacker-powered security is creating opportunities across the entire globe. Whether you're a trained professional looking for a side hustle, in search of an intellectual challenge, or pursuing hacking as a full time endeavor, there is no shortage of opportunity to earn and learn. Dozens of companies in the past year have hired from within the community, utilizing submitted bug reports, personal interactions and public HackerOne profile activity as a bellwether for hiring decisions—a practice encouraged and championed within HackerOne.

The unemployment rate for trained cybersecurity personnel is [infamously 0%](#). This fact makes the decision to work with hackers through methodical crowdsourced security efforts logical for both the individual hacker as well as the organization. Hackers get the opportunity to get well-rewarded for their efforts, and organizations can expand their security talent almost instantaneously in a results-driven compensation model.



The image shows a laptop screen displaying the Bureau of Labor Statistics (BLS) website. The page is titled "Economic News Release" and features a table titled "Table A-14. Unemployed persons by industry and class of worker, not seasonally adjusted". The table provides data for December 2017 and December 2018, comparing the number of unemployed persons (in thousands) and their unemployment rates across various industries. The industries listed include Nonagricultural private wage and salary workers, Mining, quarrying, and oil and gas extraction, Construction, Manufacturing, Durable goods, Non durable goods, Wholesale and retail trade, Transportation and utilities, Information, Financial activities, Professional and business services, Education and health services, Leisure and hospitality, Other services, Agriculture and related private wage and salary workers, Government workers, and Self-employed workers, unincorporated, and unpaid family workers.

	Ink	Number of unemployed persons (in thousands)		Unemployment rates	
		Dec. 2017	Dec. 2018	Dec. 2017	Dec. 2018
<b>Total, 16 years and over<sup>(1)</sup></b>		6,278	6,029	3.9	3.7
Nonagricultural private wage and salary workers		6,241	6,005	3.8	3.6
Mining, quarrying, and oil and gas extraction		41	21	5.1	2.6
Construction		554	493	5.9	5.1
Manufacturing		505	441	3.3	2.8
Durable goods		269	231	3.0	2.3
Non durable goods		217	210	3.8	3.5
Wholesale and retail trade		841	753	4.1	3.7
Transportation and utilities		208	260	3.0	3.9
Information		108	103	3.8	3.9
Financial activities		143	248	1.5	2.4
Professional and business services		712	723	4.2	4.3
Education and health services		706	519	3.0	2.1
Leisure and hospitality		832	814	6.2	6.0
Other services		189	211	2.8	3.0
Agriculture and related private wage and salary workers		210	151	11.9	8.6
Government workers		460	526	2.2	2.9
Self-employed workers, unincorporated, and unpaid family workers		287	251	3.9	3.9

Footnotes:  
(1) Persons with no previous work experience and persons whose last job was in the U.S. Armed Forces.

# BUG BOUNTIES VS. SALARY

MULTIPLIER OF MEDIAN ANNUAL WAGE

**40.6x**

**ARGENTINA**

**24.5x**

**THAILAND**

**24.2x**

**EGYPT**

**17.6x**

**INDIA**

**6.7x**

**HONG KONG**

6.4x	UNITED STATES OF AMERICA
6.3x	SWEDEN
6.2x	CHINA
6.2x	ALGERIA
4.8x	CANADA
3.9x	PAKISTAN
3.8x	MOROCCO
3.5x	LATVIA
3.1x	BELGIUM
3.0x	PHILIPPINES
3.0x	AUSTRALIA
2.9x	NEW ZEALAND
2.9x	GERMANY
2.9x	PORTUGAL
2.7x	HUNGARY
2.5x	ROMANIA
2.5x	CHILE
2.5x	ETHIOPIA
2.4x	INDONESIA
2.2x	NETHERLANDS

Figure 3: Median annual wage of a software engineer was derived from [PayScale](#) for each region. The multiplier is the top bounty salary divided by the median annual wage of a software engineer.

HACKER SPOTLIGHT

# JESSE

@randomdeduction

“I started doing bug bounties because I could do that on the side to really perfect my skills, and then I had a chance to legally hack against all these random third-party companies that encouraged it.”





# DEMOGRAPHICS

Youthful, hungry for knowledge, and creative.

That's the profile of the average hacker in the HackerOne community. Nine out of 10 hackers are under 35, eight out of 10 are self-taught, and more are coming from diverse industries outside of technology, which brings creative thinking to bug finding. They're also hacking more than 2018, with more than 40% spending 20-plus hours per week searching for vulnerabilities and making the internet safer for everyone.

# AGE

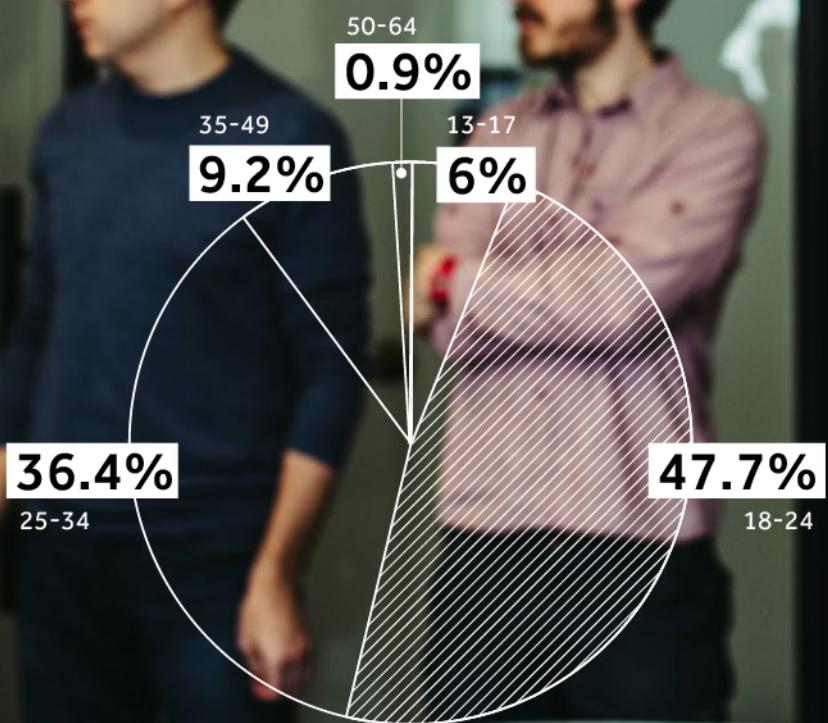


Figure 4: What's your age?

Most of the hackers on HackerOne are under the age of 35, which includes a slight increase in the 18-24 subgroup. Those younger adults now account for more than 47% of the HackerOne community, and were the only age group showing a year over year increase. Don't count the older folks out quite yet, however. The 35-49 year olds maintained their share at just over 9% again this year. And the percentage of 50-64 year olds nearly doubled this year, albeit they represent just a fraction of the overall community.

# HACKER PERCEPTIONS IN AMERICA

In January 2019, HackerOne commissioned a survey, conducted online by The Harris Poll among over 2,000 U.S. adults to gauge their perception of hackers, whether positively or negatively. The results, a portion of which are included below, should be seen as encouraging but also sobering as we consider the road ahead to retrain our collective psyche to see hackers as heroes, not criminals. It's part of an ongoing mission to [redefine the term hacker](#) in the likes of the Cambridge Dictionary, removing the unnecessary and incorrect association of criminality with hackers.

82% of Americans believe hackers can help expose system weaknesses to improve security in future versions

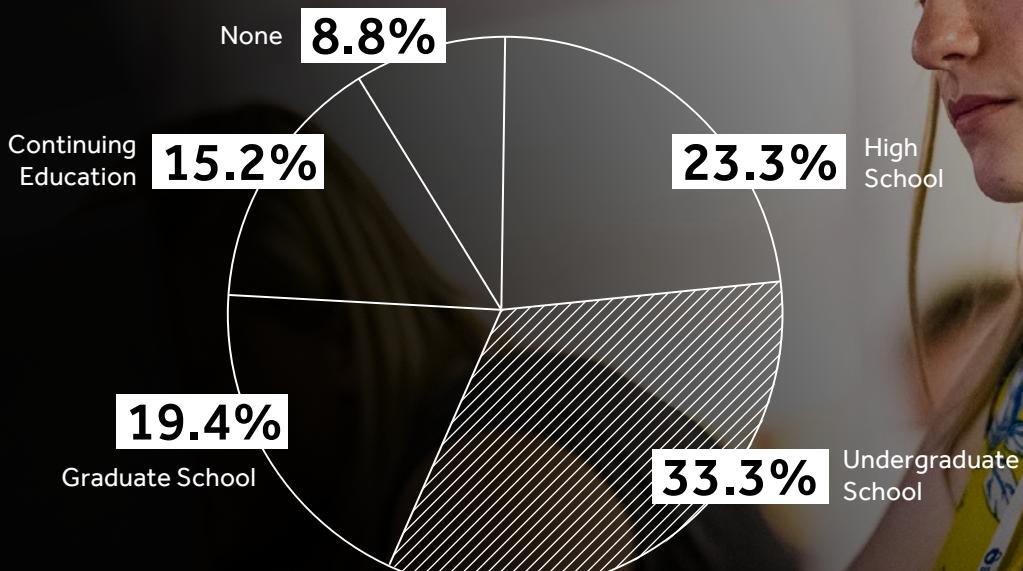
Millennials (ages 18-34) are most likely to believe that hacking is a legitimate profession (57% vs. 31% of those aged 35+)

Nearly two thirds of Americans (64%) think not all hackers act maliciously

More than 4 in 5 Americans (83%) believe hacking is an illegal activity



# TRENDS IN HACKER EDUCATION



*Figure 5: What best describes your education specifically related to computer science and/or programming?*

As hackers skew younger, the type and level of computer science and programming education have shifted as well. More than 80% are working off undergraduate or earlier training, up more than 25 points from last year and reflecting another shift as more hackers learn from experience and self-directed research rather than from a traditional educational setting. In fact, 81% of hackers point to online resources and blogs as their primary source for hacking education, while just 6% have completed a formal class or certification on hacking.

## INTERLUDE

# INTRODUCING HACKBOXES AND THE HACKER101 CAPTURE THE FLAG

In September 2018, HackerOne launched the [Hacker101 CTF](#), a perpetual 24/7 capture the flag (CTF) challenge. The Hacker101 CTF is available for learners to jump right in and find bugs in real-world simulated environments using the skills taught in our Hacker101 videos. Hacker101 CTF participants have grown to over 19,395 individuals, collectively discovering 61,576 flags.

In November 2018, we announced that finding flags in the CTF will now allow hackers to directly earn invitations to private bug bounty programs on HackerOne. Now, anyone can turn the hacking skills learned in the Hacker101 "classroom" into cash earned through established bug bounty programs. To date, hackers participating through the Hacker101 CTF earn 18% more per report than the platform average.

Hacker education got another boost with the introduction of [Hackboxes](#): Sandbox environments of disclosed vulnerability reports on HackerOne's [hacktivity](#) where learners can test their skills in real-world simulated bugs. The 5 Hackbox environments were launched with the help of HackEDU and are available for anyone to test their hacking skills and see if they can replicate the same bug that was discovered.

**hacker101**

**HackEDU**



# PROFESSION

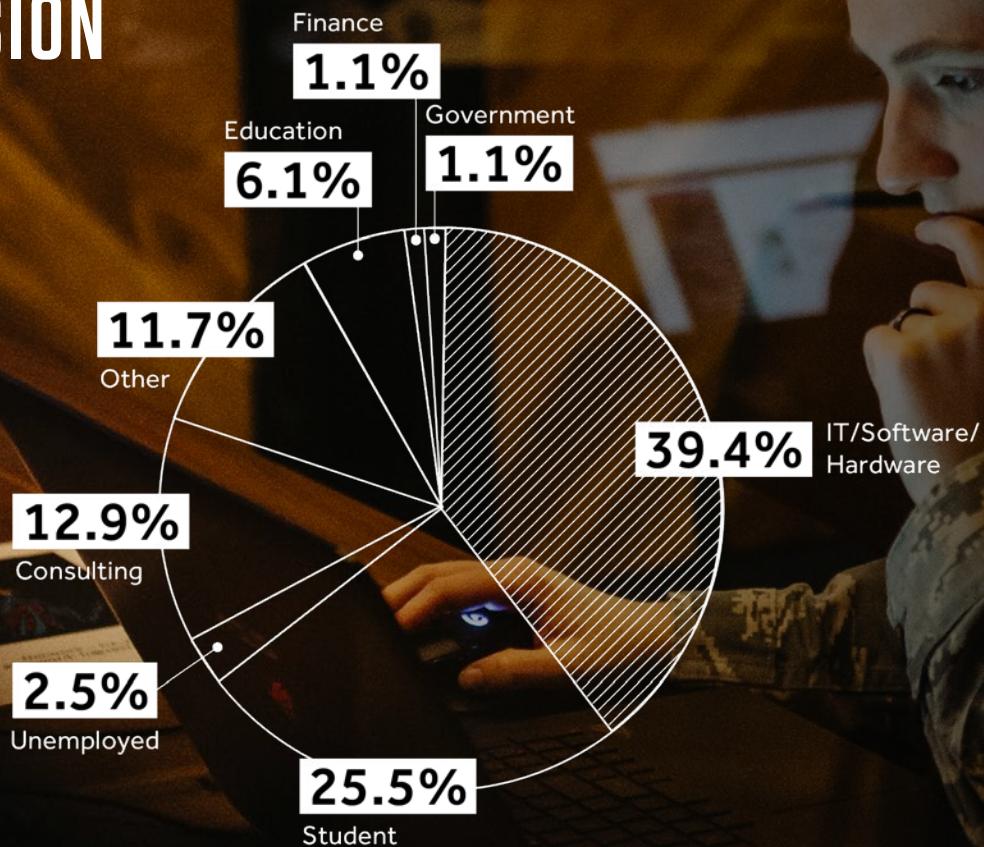


Figure 6: What best describes your professional title?

Hacking can be a lucrative hobby or full-time pursuit. A majority of the community fit in the first category, spending most of their days working a full time job or as students with a full class load. One-quarter fit that latter category, while just under 40% of those working do so in an IT or technology field. The biggest year over year shift was a drop in those working from the field of technology, from 47% last year, and an increase in those claiming "other" as their profession, from 4% last year to over 11% this year.

Regardless of what fills their days, hackers are spending more time hacking. One-third devote 10 or fewer hours per week, but that share is down from 44% last year. More telling is that over 25% of hackers spend 30 or more hours each week hacking, up from just 20% last year.

# HOURS PER WEEK SPENT HACKING

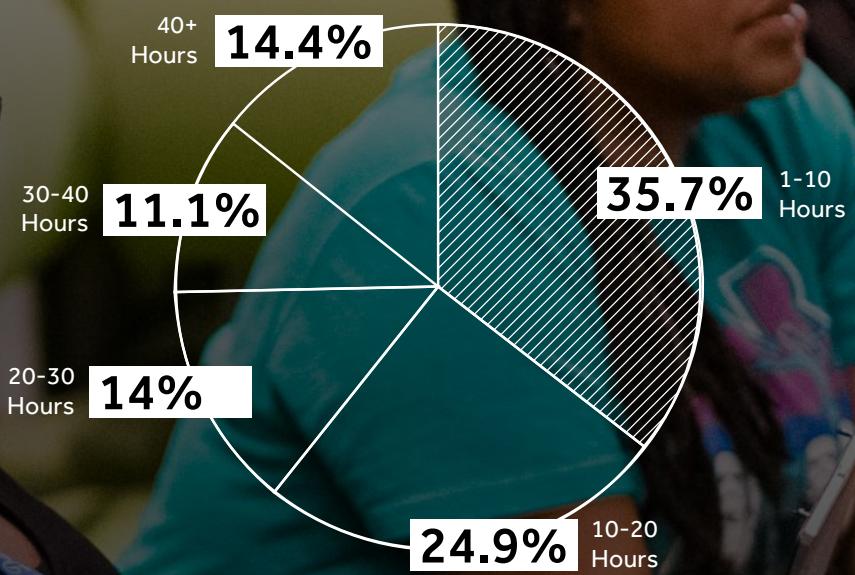


Figure 7: On average, approximately how many hours per week do you spend hacking?

**INTERLUDE**

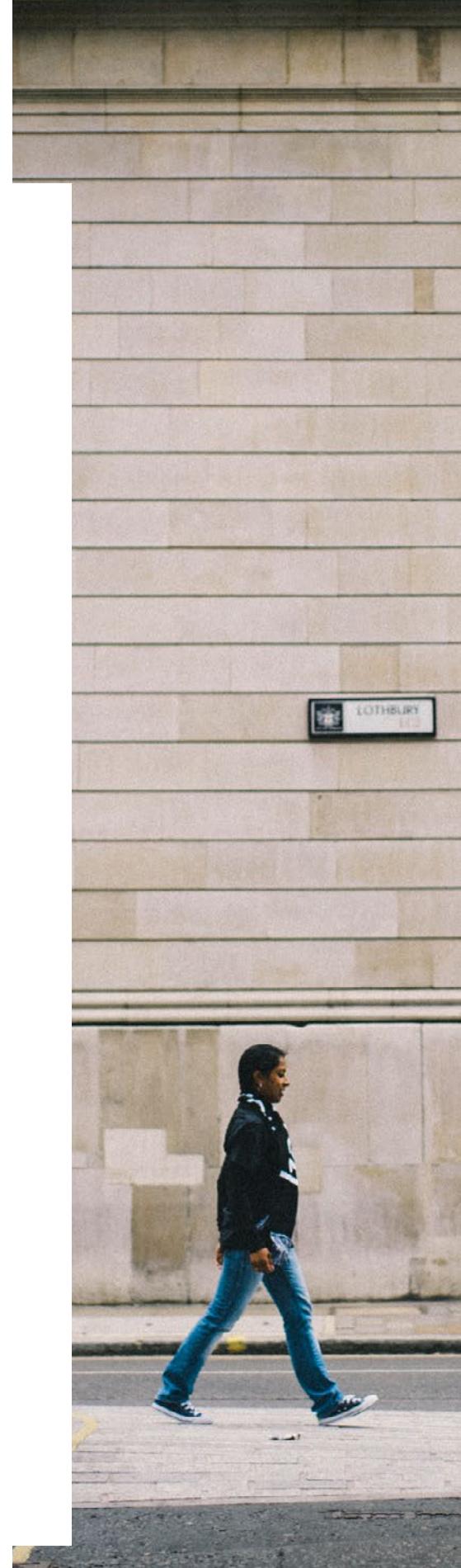
# BLOCKCHAIN HACKER TRENDS

Since blockchain first became a core component of bitcoin technology roughly ten years ago, the promise of the public ledger has exploded. Beyond just cryptocurrency, blockchain has seemingly endless applications, from tracking financial transactions to managing music distribution to monitoring supply chains and even voting.

As with any technology, security issues are still being explored and understood, and hackers are a critical part of that security equation. Today, nearly 70 blockchain and cryptocurrency companies utilize HackerOne's platform and community of hackers to help secure their technology. In 2018 alone, those organizations received nearly 3,000 vulnerability reports, which points to the interest hackers have in blockchain. Furthermore, nearly 4% of all bounties awarded on HackerOne in 2018 were from blockchain and cryptocurrency organizations.

Blockchain companies like [Coinbase](#), [Tron Foundation](#), [Block.One](#), [Voatz](#), and many more run public bug bounty programs on the HackerOne platform. [Brave](#), whose browser product features blockchain-based tokens, has paid out more than \$25,000 in bounties and resolved nearly 100 vulnerability reports.

In addition to the experience gained by working with such a popular technology, hackers also receive higher than average bounties from blockchain organizations. In 2018, the average bounty paid across all blockchain-related firms was just under \$1,500 which is about \$600 more than the 2018 platform average. What's more, the top earning blockchain and cryptocurrency hackers made seven times the median software engineer salary in their respective country!



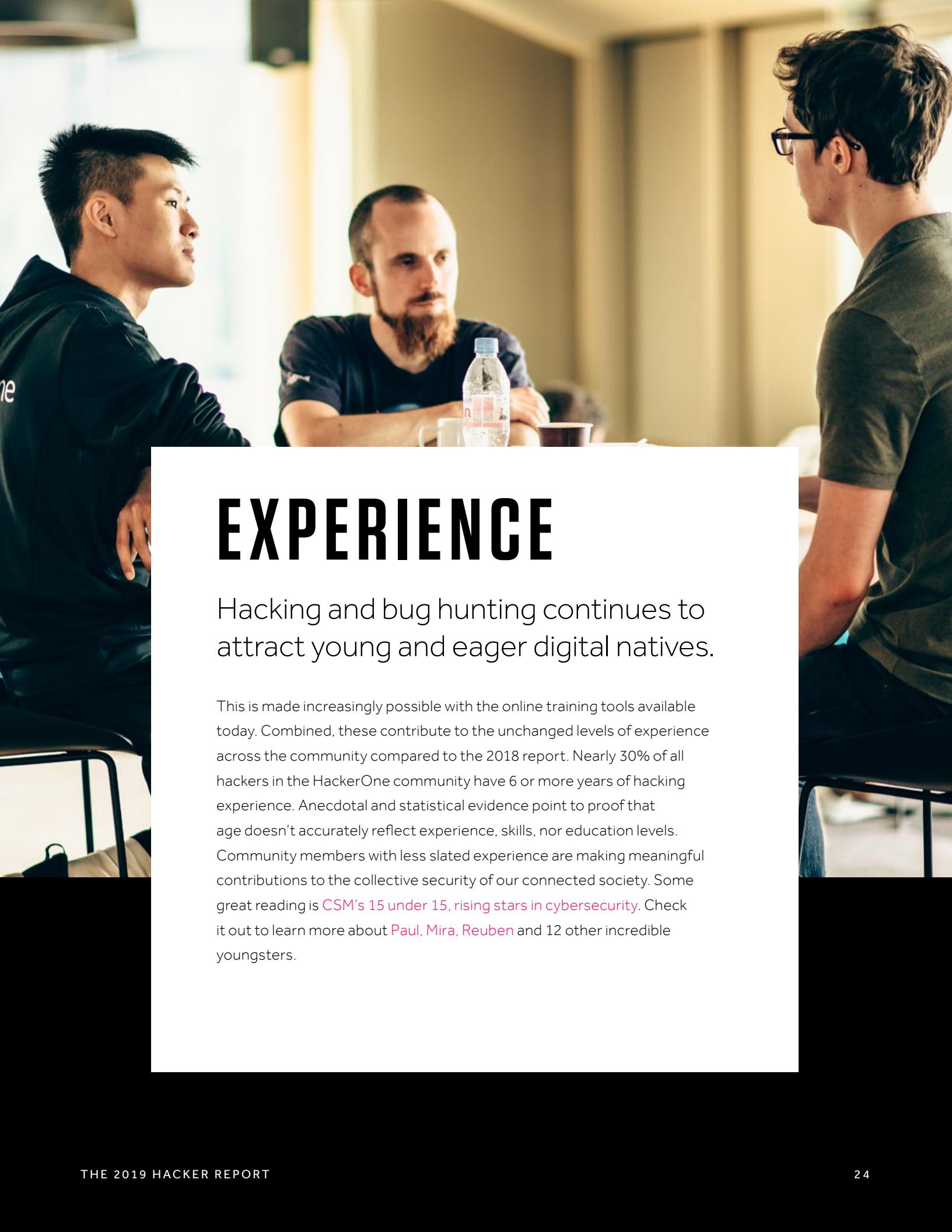


HACKER SPOTLIGHT

# RON

@ngalog

“The reason I hack is because I like the challenge. I think this is some kind of intellectual challenge for me because hacking is like finding something that others will not be able to find and thinking like how some others may not be able to think.”



# EXPERIENCE

Hacking and bug hunting continues to attract young and eager digital natives.

This is made increasingly possible with the online training tools available today. Combined, these contribute to the unchanged levels of experience across the community compared to the 2018 report. Nearly 30% of all hackers in the HackerOne community have 6 or more years of hacking experience. Anecdotal and statistical evidence point to proof that age doesn't accurately reflect experience, skills, nor education levels. Community members with less slated experience are making meaningful contributions to the collective security of our connected society. Some great reading is [CSM's 15 under 15, rising stars in cybersecurity](#). Check it out to learn more about [Paul](#), [Mira](#), [Reuben](#) and 12 other incredible youngsters.

# EXPERIENCE



Figure 8: Approximately how many years have you been hacking?

HACKER SPOTLIGHT

# TANNER

@cache-money

A medium shot of a young man with short brown hair, smiling slightly. He is wearing a dark grey t-shirt under a black zip-up hoodie. He is seated in a large, light-colored leather armchair. In the background, there's a lamp and some vertical blinds on a window.

“When you find a bug, your heart starts racing. You keep going back, chasing that feeling over and over again.”

# XSS in Steam React Chat Client

Reported by hacker [@zemnmez](#) to [Valve](#), this critical vulnerability earned a \$7,500 bounty.

*The Steam Chat client is a particularly interesting system to attack because it's built using a modern set of technologies with strong security characteristics. It's built on React, which has some of the strongest security characteristics of any modern Javascript application framework, and avoids use of the unsafe `dangerously family of functions` well...*

— [@zemnmez](#)

Read the fully disclosed report write-up [here](#).

The image shows a tablet displaying the HackerOne website. The profile picture of the reporter, Zemnmez, is highlighted with a pink circle. The main page shows the following details for the reported issue:

- Reputation:** 437
- Rank:** -
- Signal:** 4.06
- Percentile:** 84th
- Impact:** 24.09
- Percentile:** 96th

**#409850 XSS in steam react chat client**

**State:** Resolved (Closed)

**Disclosed:** January 7, 2019 3:00pm -0500

**Participants:** Valve

**Asset:** steamcommunity.com (Domain)

**Weakness:** Cross-site Scripting (XSS) - Stored

**Bounty:** \$7,500

**SUMMARY BY ZEMNMEZ**

**1. Background**

The Steam Chat client is a particularly interesting system to attack because it's built using a modern set of technologies with strong security characteristics. It's built on React, which has some of the strongest security characteristics of any modern Javascript application framework, and avoids use of the unsafe `dangerously family of functions` well...



# TARGETS & TOOLS

How do hackers decide which programs to hack?

What are their tools of choice? What attack surfaces do they prefer? Read on to find out.

# FAVORITE TOOLS

2018 saw a 67% increase in hackers embracing third party local proxy tools. Burp Suite is still the most used tool (32.7%), but Fiddler (14.7), Webinspect (11.1%), and ChipWhisperer (9.8%) have all seen increased usage by our hackers. As our community has grown, the number of hackers using network scanners and fuzzers has remained steady, falling to 5% and 4.9% of users respectively.

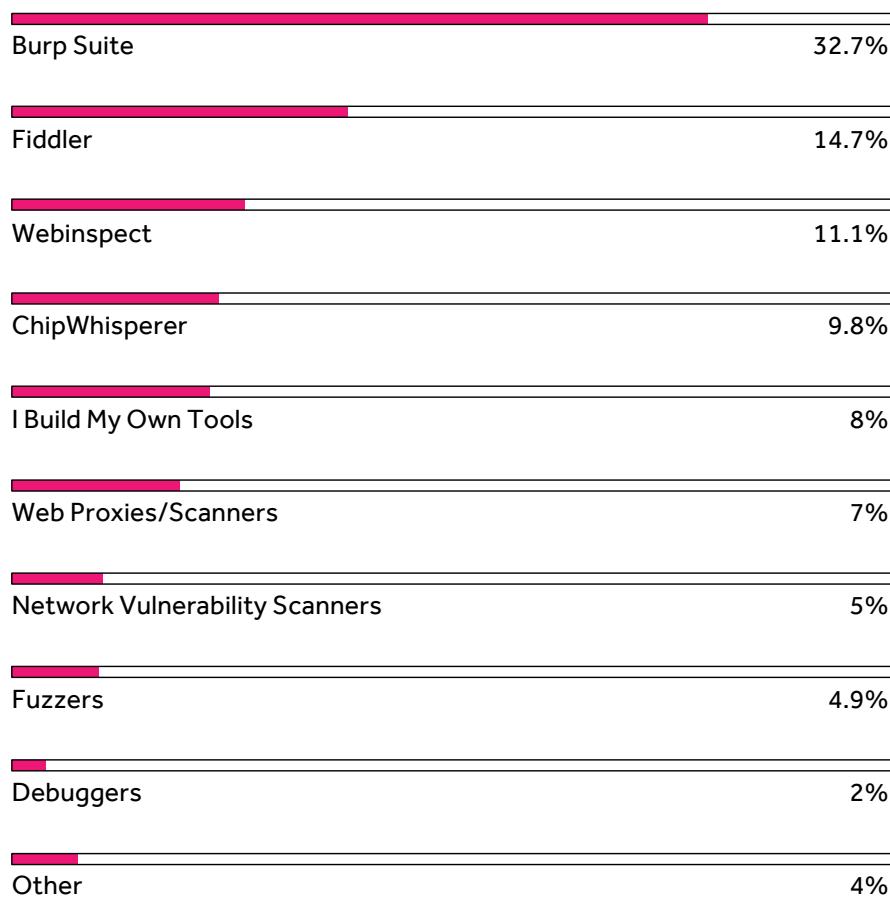


Figure 9

# WHAT DO YOU HACK?

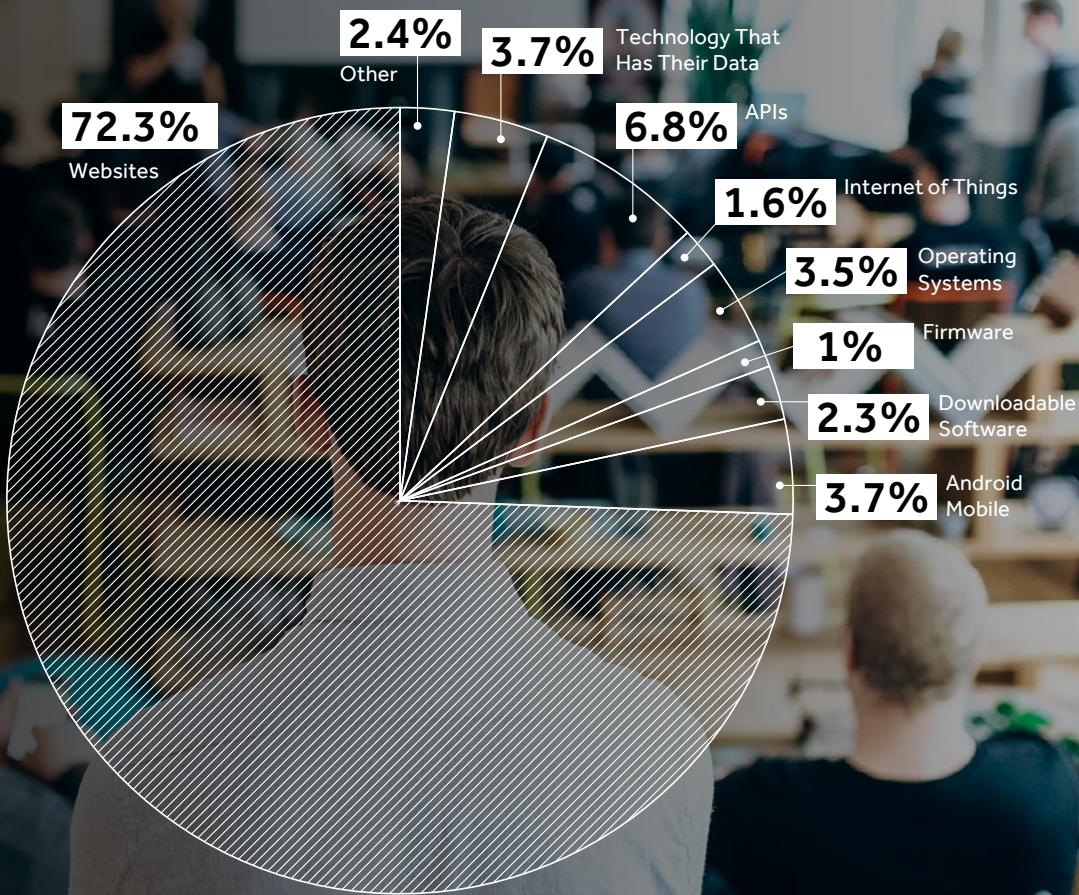


Figure 10

## HACKERS LOVE RESEARCHING WEBSITES, APIs AND TECHNOLOGY THAT HOLDS THEIR OWN DATA

Bug bounty hackers still love finding vulnerabilities in web applications. Over 70% of surveyed hackers said their favorite types of product or platform to hack is websites, followed by APIs (6.8%), technology that stores their data (3.7%), Android apps (3.7%), operating systems (3.5%) and downloadable software (2.3%).

## HACKER SPOTLIGHT

# ANDRE

@0xacb

"The hacker community is about knowledge-sharing. We can help each other to improve our skills and keep up to date with security."



# SSRF in Exchange Leads to ROOT Access in all Instances

Disclosed on May 23, 2018 this Server-Side Request Forgery vulnerability reported to Shopify earned hacker @0xacb \$25,000.

*Shopify infrastructure is isolated into subsets of infrastructure. @0xacb reported it was possible to gain root access to any container in one particular subset by exploiting a server side request forgery bug in the screenshotting functionality of Shopify Exchange. Within an hour of receiving the report, we disabled the vulnerable service, began auditing applications in all subsets and remediating across all our infrastructure. The vulnerable subset did not include Shopify core... — Shopify*

Read the full report [here](#).

The image shows a laptop screen displaying the HackerOne platform. The page is for a completed bounty titled "SSRF in Exchange leads to ROOT access in all instances" submitted by André Baptista (@Oxacb). The summary section includes details such as State: Resolved (Closed), Disclosed: May 23, 2018 5:09pm -0400, Reported To: Shopify, Asset: https://exchangemarketplace.com/ (Domain), Weakness: Server-Side Request Forgery (SSRF), and Bounty: \$25,000. The summary text from the bounty page reads: "Shopify infrastructure is isolated into subsets of infrastructure. @0xacb reported it was possible to gain root access to any container in one particular subset by exploiting a server side request forgery bug in the screenshotting functionality of Shopify Exchange. Within an hour of receiving the report, we disabled the vulnerable service, began auditing applications in all subsets and remediating across all our infrastructure. The vulnerable subset did not include Shopify core." Below the summary, there is a note about the fix: "After auditing all services, we fixed the bug by deploying a metadata concealment proxy to disable access to metadata information. We also disabled access to internal IPs on all infrastructure subsets. We awarded this \$25,000 as a Shopify Core RCE since some applications in this subset do have access to some Shopify core data and systems."



# MOTIVATION

Bug bounty hunters are motivated only by cash, right? **Wrong.**

Financial incentives are without question important. However, there's more to hacking than just the money. Curiosity is an enduring quality across the hacker community, as is an affinity for high profile vulnerability disclosure programs (such as the U.S. Department of Defense, General Motors, Alibaba, Goldman Sachs, Toyota, IBM, and more) and a genuine desire to help the internet become more secure.

## CURIOSITY MEANS MORE THAN MONEY

So what motivates hackers if it's not just money? Nearly three-times as many hackers do so to learn and contribute to their own growth. Unsurprisingly, nearly as many hack just "to have fun" as those who do it for the money. The generosity and altruism of hackers also shines through, with more than one-quarter hacking to protect, help others, and simply to do good in the world.

### WHY DO YOU HACK?

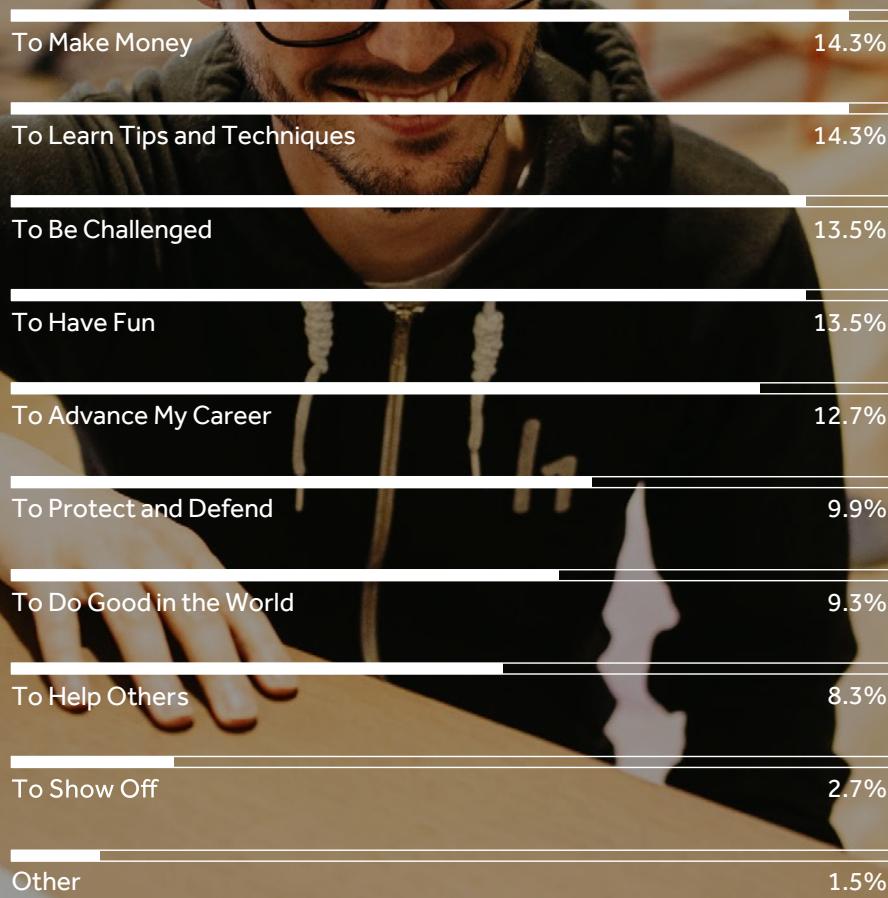


Figure 11

## GOVERNMENTS LEAD THE WAY IN HACKER-POWERED SECURITY

"Governments lead the way" isn't a phrase you often hear, especially in technology. But in the realm of hacker-powered security, governments and [government agencies](#) are decidedly progressive on their use and promotion of this proven approach to cybersecurity.

The U.S. Department of Defense has partnered with HackerOne for several years, running pioneering programs such as [Hack the Pentagon](#) and [Hack the Army](#) to great success. In late 2018, they [announced](#) the results of their seventh bug bounty program, which was their third [Hack the Air Force](#) event, and which resulted in hackers from across the globe submitting 120 valid vulnerabilities and earning over \$130,000 in just one month. This past year the U.S. General Services Administration became [the country's first civilian agency](#) to launch a public multi-year bug bounty program, awarding HackerOne its second contract with GSA.

Governments in other regions are also embracing hacker-powered security. The European Commission partners with HackerOne as part of a framework created by the EU-Free and Open Source Software Auditing (EU-FOSSA) project, which aims to help EU institutions better protect their critical software. FOSSA plans to launch more than two dozen additional bounty programs in 2019.

In Singapore, building on the success of the bounty program run by their Ministry of Defense (MINDEF), the Government Technology Agency of Singapore (GovTech) and the Cyber Security Agency of Singapore (CSA), are [working with HackerOne to launch](#) a government bug bounty initiative designed to protect Singapore's citizens and help secure public-facing government systems.

Governments continue to lead the way with their successful hacker-powered programs. This is further proven by the legislation recently proposed and passed in favor of hacker-powered programs, such as the Cyber Intelligence Sharing and Protection Act (CISPA) and the Cybersecurity Information Sharing Act (CISA) in the U.S. and new budget in Singapore. More and more, organizations across a spectrum of sectors realize the value these white-hat hackers add to their security apparatus.



## HACKERS VALUE GOOD COMMUNICATION, A CHALLENGE, AND RECOGNITION WHEN CHOOSING A BUG BOUNTY PROGRAM TO FOCUS ON

Hackers are motivated in a number of ways. This year, bounty amounts were knocked off the top spot for why hackers choose to participate in a program, dropping down to fourth place. Hackers favor education and experience, as the opportunity to learn was, by far, the number one motivator. The organization behind the program is also important, namely their likability and their responsiveness to the hackers trying to help them secure their technology.



# WHY DO YOU CHOOSE THE COMPANIES THAT YOU HACK?

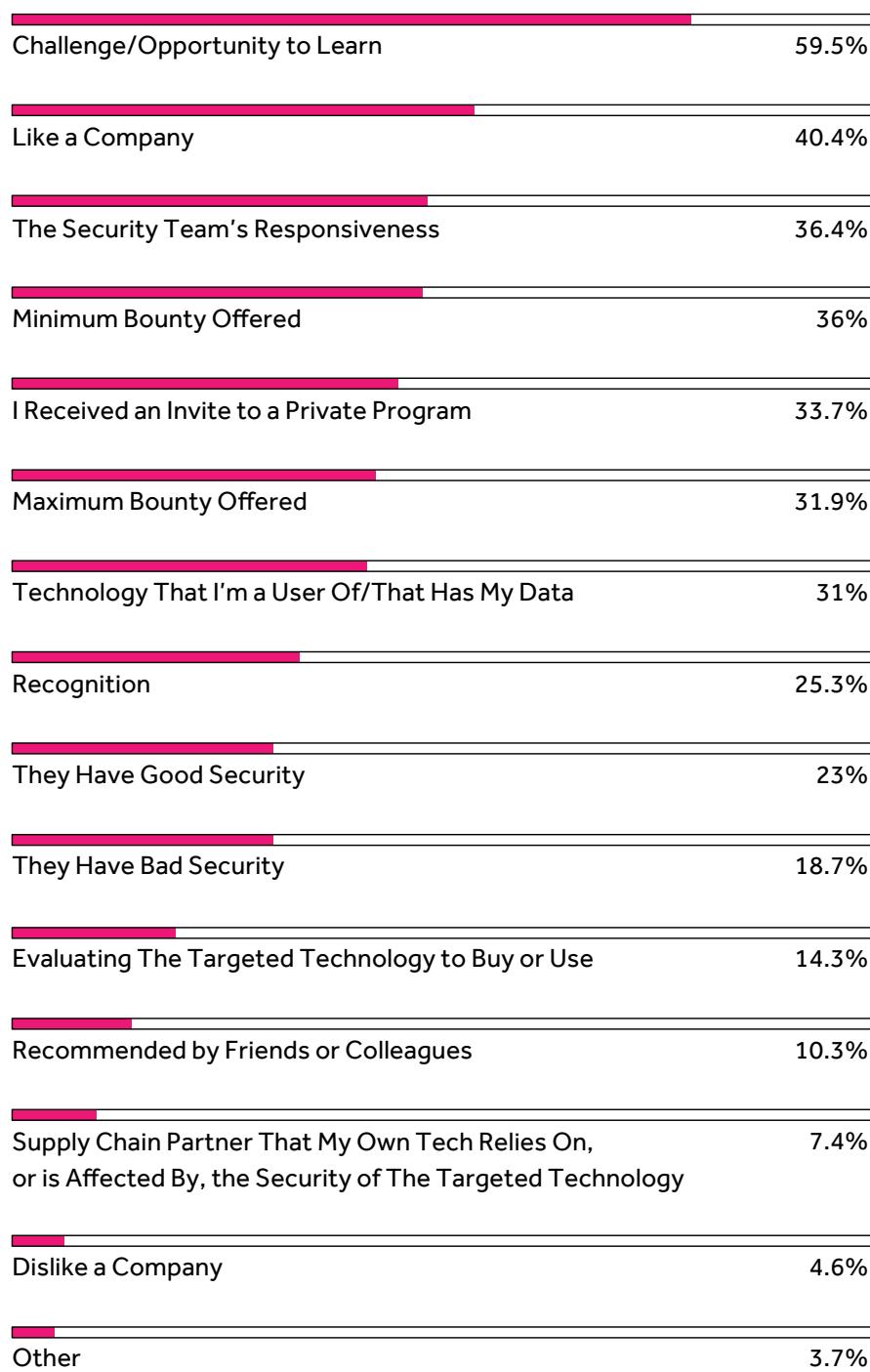


Figure 12

## MORE AND MORE HACKERS NAME XSS THEIR FAVORITE ATTACK VECTOR

When asked about their favorite attack vector, technique or method, over 38% of hackers surveyed said they prefer searching for cross-site scripting (XSS) vulnerabilities. That's up from just 28% last year, and puts XSS significantly ahead of all other attack vector preferences. SQL injection placed second at 13.5%, while fuzzing, business logic, and information gathering rounded out the top five. In 2017, neither business logic nor information gathering placed in the top 10 last year.



# WHAT IS YOUR PREFERRED TECHNIQUE, ATTACK VECTOR OR METHOD WHEN HACKING?

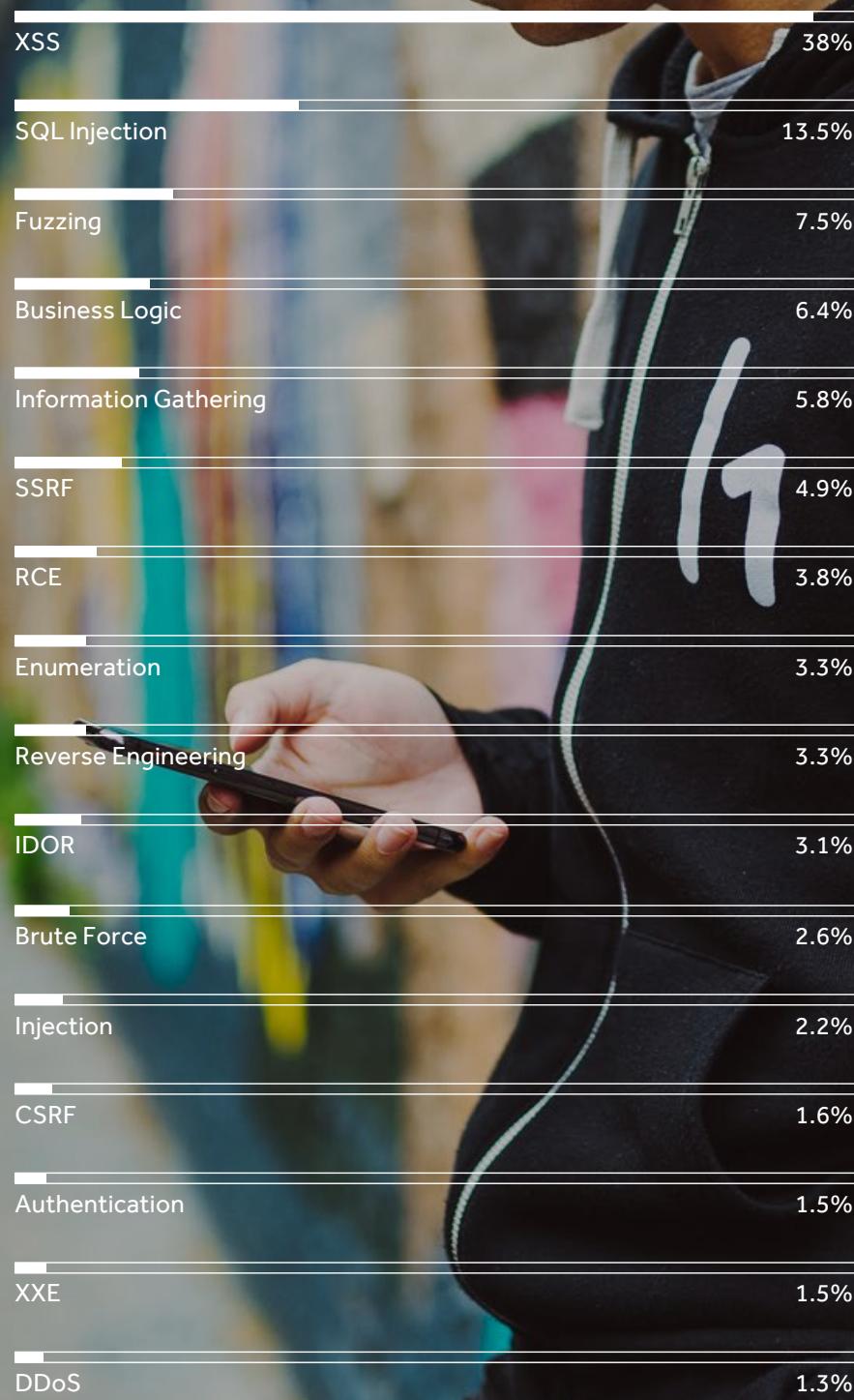


Figure 13

## HACKER SPOTLIGHT

# JOEL

@teknogeek

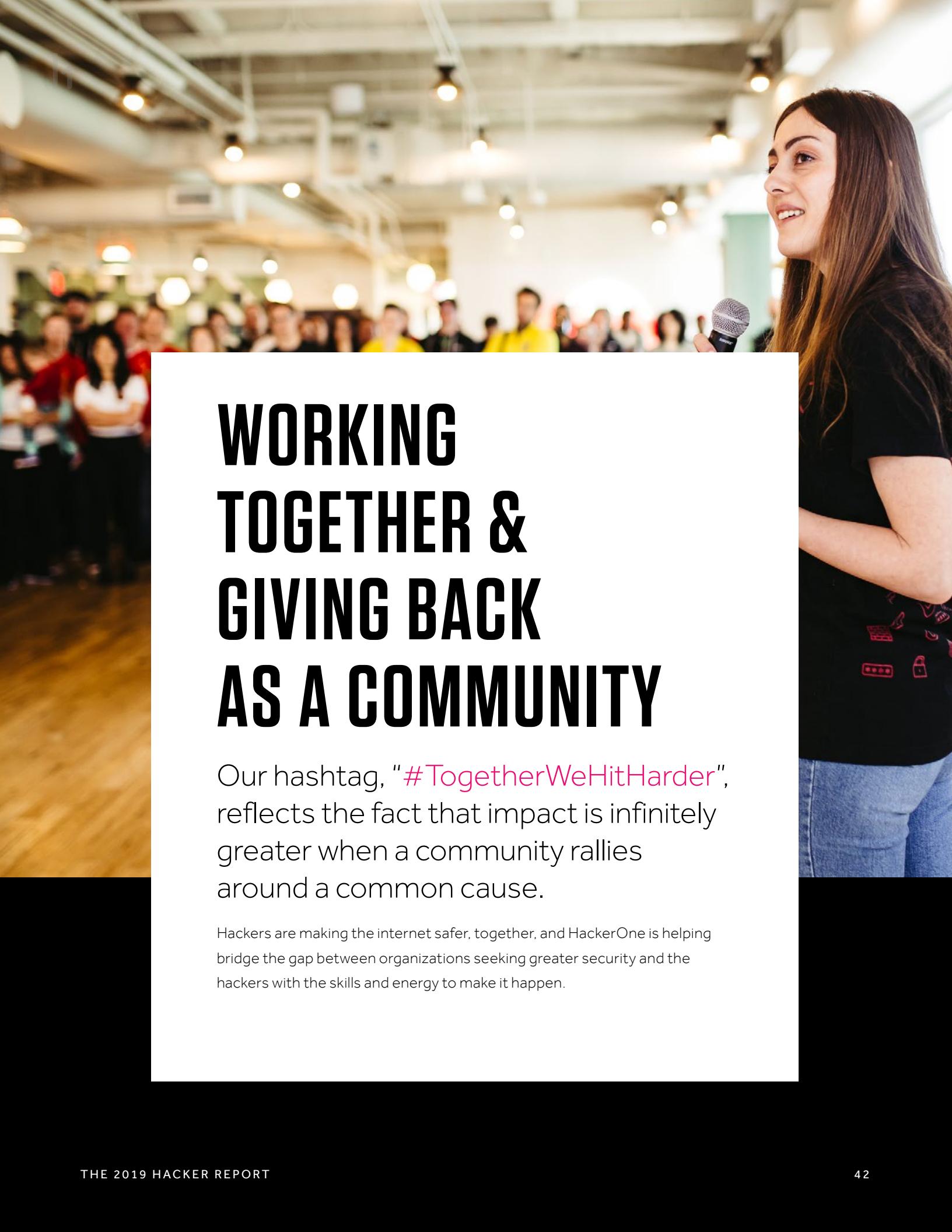
"I think it's really important to hack in order to preserve the security of everything around us. There are so many applications we put our personal information into it and we just leave it out there. If it's not secure, what's to stop a malicious person from taking it?"



## BRINGING THE COMMUNITY TOGETHER FOR GLOBAL LIVE HACKING EVENTS

HackerOne hosts live hacking events in cities around the world, connecting security teams with top hackers. In 2018 HackerOne hosted live hacking events in 9 cities: Las Vegas (h1-702), New York City (h1-212), Goa, India (h1- 91832), Washington DC (h1-202), San Francisco (h1-415), Amsterdam (h1-3120), London (h1-4420), Buenos Aires (h1-5411), and Montreal (h1-514). For each event, we partner with our customers to fly out 25 to 40 (sometimes over 50!) of the top members of our community from across the globe to participate.





# WORKING TOGETHER & GIVING BACK AS A COMMUNITY

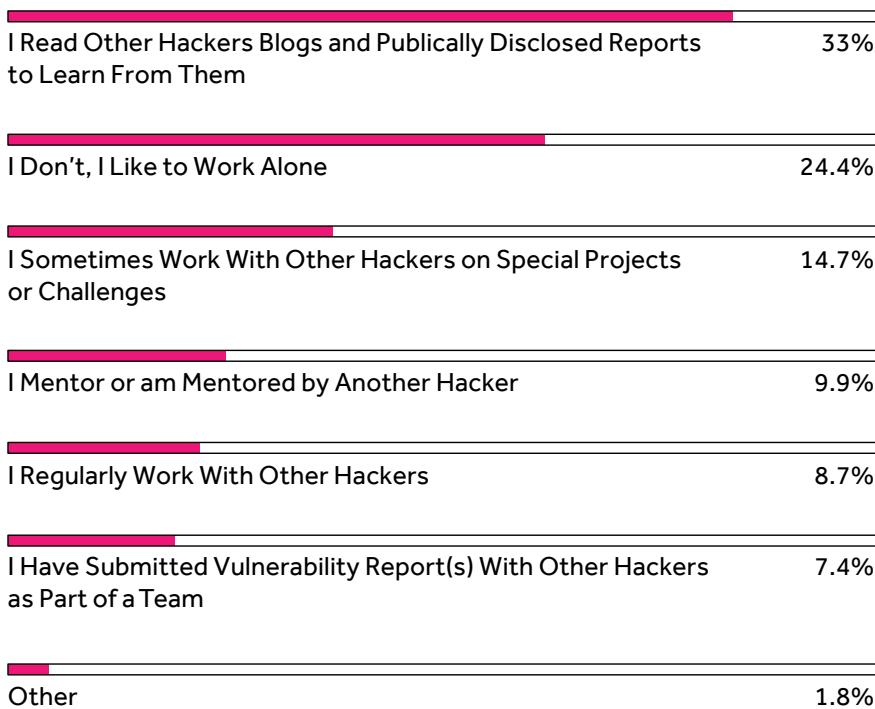
Our hashtag, "#TogetherWeHitHarder", reflects the fact that impact is infinitely greater when a community rallies around a common cause.

Hackers are making the internet safer, together, and HackerOne is helping bridge the gap between organizations seeking greater security and the hackers with the skills and energy to make it happen.

## HACKERS FREQUENTLY WORK ALONE BUT LIKE LEARNING FROM OTHERS

As hackers look to their community to learn and grow, they're also forming relationships that translate into knowledge sharing and direct collaboration. One-quarter of hackers still choose to work alone, but that number has fallen significantly from 31% last year. Today, more than one-third of hackers rely on the experiences shared by other hackers, and more than 40% collaborate with other hackers occasionally or more often.

## HOW DO YOU TYPICALLY WORK WITH OTHER MEMBERS OF THE HACKER COMMUNITY?



*Figure 14*



## DO YOU ACTIVELY PARTICIPATE IN ANY HACKER ORIENTED COMMUNITY-BASED ORGANIZATIONS?

Hackers are a giving bunch. They regularly contribute their time, talents, and treasures to support cybersecurity initiatives. **These are just a few of the organizations that our community wrote-in that they actively engage with.**



**OWASP**  
Open Web Application Security Project

**BSIDES**



WOMEN  
IN SECURITY  
AND PRIVACY

**BUG BOUNTY FORUM**

  
**Chaos  
Computer  
Club**





HACKER SPOTLIGHT

# SANTIAGO

@try\_to\_hack

"I really like to hack. It's fun. I like the challenges of hacking to break stuff."

## **EMBRACING HACKER-POWERED SECURITY: ORGANIZATIONS ACROSS SECTORS INCREASINGLY SEE VALUE OF HACKER EFFORTS**

In last year's Hacker Report, we noted that there had been over \$23 million in total bounties over 6 years. **In just the past year alone, hackers earned \$19 million on HackerOne.** To say that companies are merely embracing hacker-powered security seems like an understatement. Even the hackers themselves see the shift, with nearly 70% saying that organizations are somewhat or far more open to receiving vulnerability reports.

What remains shocking, however, is the gaping security hole reflected in the fact that 93% of the Forbes 2000 still don't have an easy means for anyone to report potential security issues. It's as if most companies still turn a blind eye to outside help on cybersecurity issues, better known as "security through obscurity." By ignoring any mention of potential cybersecurity risks, companies assume no one will find them.

The U.S. Postal Service, for example, reportedly ignored reports of a security vulnerability for more than a year. Eventually, hackers reported the bug to [Krebs On Security](#), who published detailed findings and prompting the Postal Service to finally address the vulnerability.

Responsiveness matters to hackers who have dedicated their time to finding and safely reporting vulnerabilities. More than two-thirds of hackers chose to work with companies based on their security team's responsiveness. As we've seen consistently over the years, data breaches [happen to some of the largest and most recognizable brands](#) across the globe.

# WHAT BEST DESCRIBES COMPANIES' REACTIONS TO RECEIVING VULNERABILITY REPORTS FROM SECURITY RESEARCHERS?

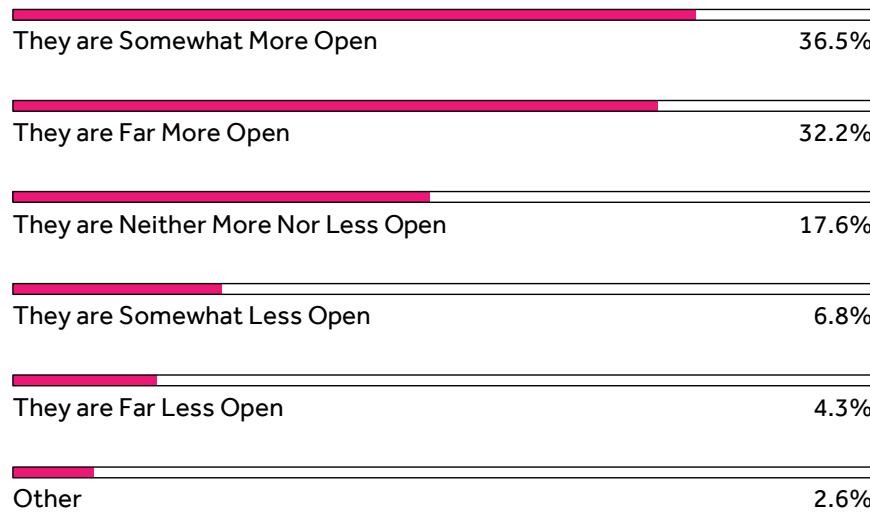


Figure 15



# Bypass 2FA Requirement and Reporter Blacklist through Embedded Submission Form on HackerOne

Disclosed on October 31, 2018 @japz and @mga\_bobo reported they were able to bypass 2FA requirements on HackerOne, earning them \$2,500 for this medium severity issue.

*The hacker submitted a vulnerability to us that allowed any user to bypass multiple program restrictions, such as the 2FA requirement, report rate limit, and internal abuse limits. The severity for this vulnerability was set to medium (CVSS 5.0). This vulnerability was awarded \$2,500... — HackerOne*

Read the full report [here](#).

The image shows a tablet displaying the HackerOne website. The user profile 'japz' is highlighted with a pink circle. The report details a vulnerability titled 'Hacker can bypass 2FA requirement and reporter blacklist through embedded submission form'. The report was resolved on October 31, 2018, at 1:24pm -0400, and was reported to 'HackerOne'. The asset is 'https://hackerone.com' (Domain). The weakness is 'Improper Authorization', and the bounty is \$10,000. The severity is Medium (5.0). The summary notes that the hacker submitted a vulnerability allowing any user to bypass multiple program restrictions, such as the 2FA requirement, report rate limit, and internal abuse limits. The severity for this vulnerability was set to medium (CVSS 5.0). This vulnerability was awarded \$2,500. A note states that when looking into the root cause, another vulnerability was found with a higher CVSS score (7.1), which allowed an attacker to gain access to other users' attachments who were writing a report at the same time. Because this second vulnerability was identified due to @japz's report, an additional \$7,500 was awarded. The report itself contains an in-depth explanation of where the vulnerability originated from.

HACKER SPOTLIGHT

# MATHIAS

@avlidienbrunn



"It's a lot of pride to be a part of a community with such great and smart people."





# CONCLUSION

The age of the hacker is here.

As hacking grows in popularity and acceptance, there is even more opportunity for the creative and talented to make the internet safer for us all. The world needs hackers like Jesse, Ron, Tanner, Andre, Santiago, Joel, and Mathias. HackerOne is proud to know thousands more like them within the community, keeping a watchful eye on the security of the internet. Here's to all the hackers out there, here's to [#TogetherWeHitHarder](#).

“There are so many friendly hackers out there that want to do the right thing. We have to create the pathways and the accessible on-ramps for these friendly hackers to converse with us, to let us know about their findings so we can all benefit.”

Keren Elazari, on stage at Security@San Francisco, October 24, 2018

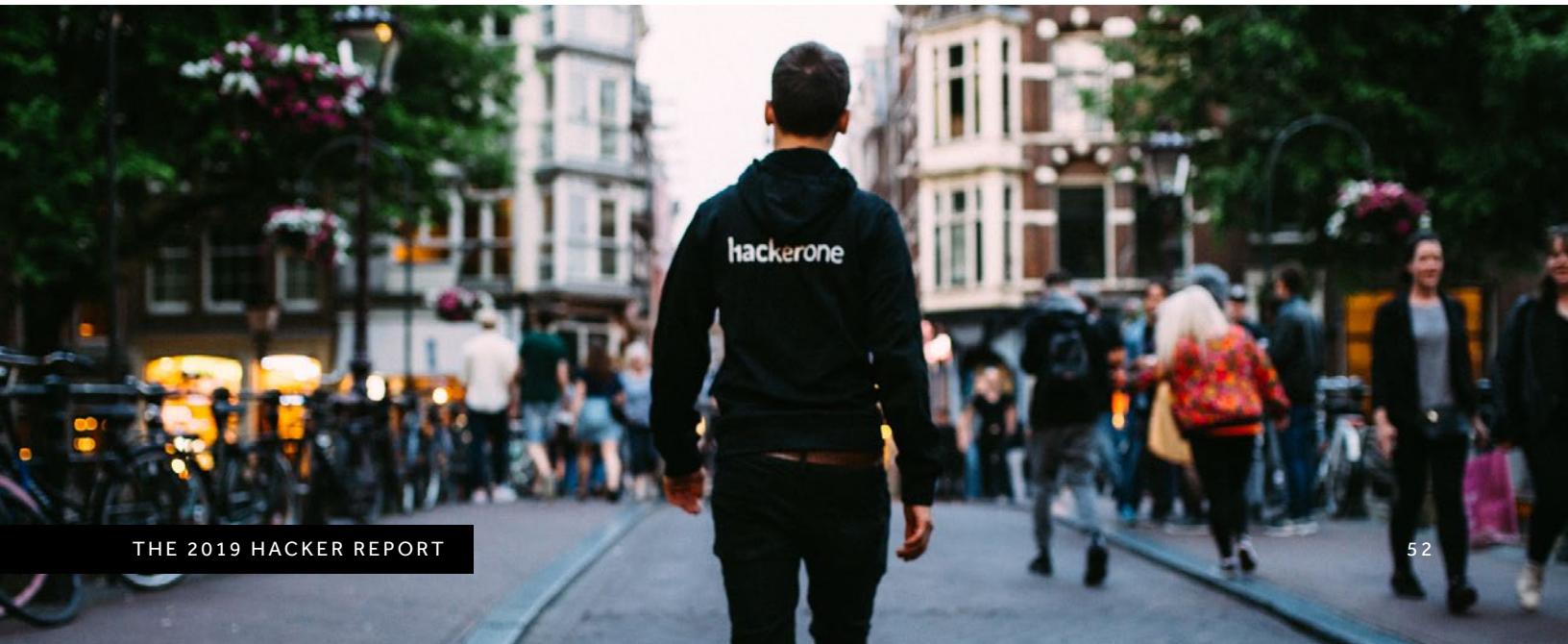


## METHODOLOGY

Data collected from HackerOne Platform survey data and Harris poll data in December 2018 and January 2019 totaling over 3,667 respondents from over 100 countries and territories. The HackerOne platform surveyed individuals have all successfully reported one or more valid security vulnerabilities on HackerOne, as indicated by the organization that received the vulnerability report. Additional findings were collected from the HackerOne platform using HackerOne's proprietary data based on over 1,200 collective bug bounty and vulnerability disclosure programs.

## ABOUT HACKERONE

HackerOne is the #1 [hacker-powered security platform](#), helping organizations find and fix critical vulnerabilities before they can be exploited. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security alternative. The U.S. Department of Defense, General Motors, Google, Twitter, GitHub, Nintendo, Lufthansa, Panasonic Avionics, Qualcomm, Starbucks, Dropbox, Intel, the CERT Coordination Center and over 1,200 other organizations have partnered with HackerOne to resolve over 95,000 vulnerabilities and award over \$46M in [bug bounties](#). HackerOne is headquartered in San Francisco with offices in London, New York, the Netherlands, and Singapore.



# TRUSTED BY

More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security alternative.



Lufthansa





MAKE THE  
INTERNET  
SAFER



[WWW.HACKERONE.COM](http://WWW.HACKERONE.COM) / [SALES@HACKERONE.COM](mailto:SALES@HACKERONE.COM) / +1 (415) 891-0777

hackerone