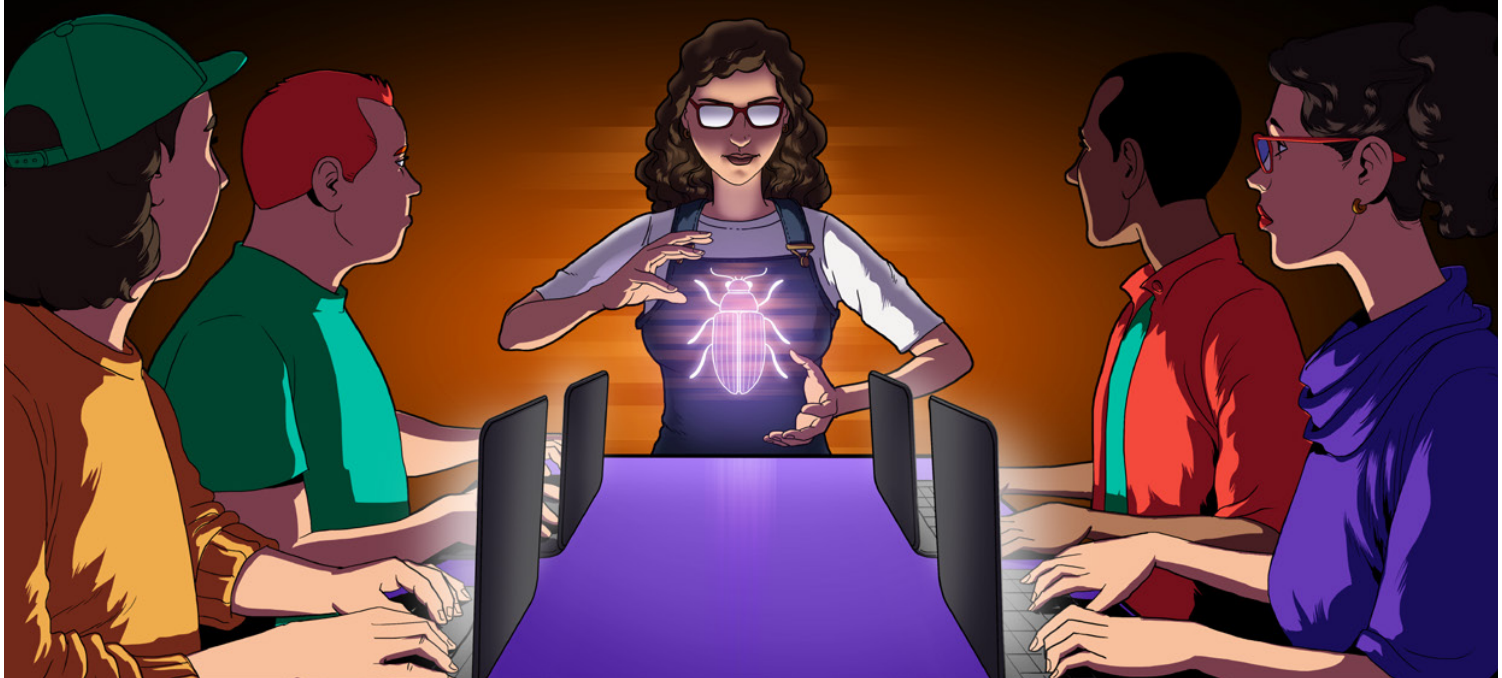
bugcrowd

INSIDE THE MIND OF A HACKER

The Ultimate Guide to Ethical Hackers and the Economics of Security Research

2021



Contents

Ashish Gupta
CEO and President

Foreword

The pandemic has challenged the world with far-reaching problems, but these challenges have also heralded a time of great digital transformation and opportunity.

Cybersecurity faces a parallel digital pandemic, plaguing organizations of all types and sizes across every industry, in the form of continually evolving cyberthreats. Software vulnerabilities or just plain user errors can result in successful malware attacks or phishing campaigns that lead to ransomware deals and reputational damage. Estimated global losses from cybercrimes were projected to reach nearly **$1 trillion in 2020**, as the pandemic spurred new ways for hackers to threaten consumers and businesses.

Yet the pandemic has also created a clear imperative for companies to rethink their security practices—and a chance to improve it. This *Inside the Mind of a Hacker '21* Report presents a captivating portrait of a globally distributed network of security researchers, also known as ethical hackers. These researchers help organizations to search for vulnerabilities and advance on our platform with every valid exploit they uncover. Customers using the Bugcrowd Platform benefit from this human intelligence, which provides expert insight into their attack surface and bolsters the strength of their security posture.

The stakes could not be higher. The report found that in the past year, 80% of security researchers identified a bug that they had never seen before. More alarmingly, 91% of ethical hackers believe that point-in-time testing is no longer adequate to keep companies secure year-round.

The initial disruption from the pandemic and the shift to a remote workforce resulted in new technologies to improve collaboration and productivity. However, running all those applications over home Wi-Fi networks and personal mobile devices introduced worrying levels of risk for many understaffed security teams.

At the same time, faced with the initial slowdown in business from COVID-19, many companies scaled back for a time or shut down completely. Such actions caused staffing shortages when growth resumed, sparking a talent war. Unsurprisingly, at the height of the pandemic, Bugcrowd observed an uptick in the use of our crowdsourcing-powered SaaS platform. In this hypercompetitive environment, on-demand crowdsourced security can help shore up the human resource shortfall. In addition, CISOs today are facing more pressure to measure and communicate their ROI to their stakeholders. To keep up in the new normal, security teams need to be agile and adaptive to fast-changing cyber-attacks. This is where the intelligence of the Crowd comes in.

To demystify common portrayals of crowdsourced security, this report introduces readers to several security experts who are active on the Bugcrowd Platform. Too often, hackers are unfairly maligned as shady criminal figures in hoodies who hole up in dark basements and conduct nefarious acts. In fact, most ethical hackers are curious, committed people who come from a broad range of backgrounds and viewpoints, which help drive innovation.

To broaden the reach of our researcher community, Bugcrowd has partnered with the federal Cybersecurity and Infrastructure Security Agency (CISA) to connect government security teams with ethical hackers. Through this partnership, we have launched the popular program **Hack the Homeland for Challenge Coins** to give our community of researchers chances to report the vulnerabilities they find across multiple federal agencies, including the Department of Homeland Security.

Despite the financial incentives, most ethical hackers' motivations are largely benevolent. In fact, hackers believe that reporting a vulnerability is more important than trying to make money from it. I would like to personally thank these dedicated researchers for their loyalty and expertise.

For example, our own Katie Paxton-Fear, who hacks as **InsiderPhD**, gives back to the hacker community by lecturing and creating online educational content. As a hacker and educator, Katie welcomes the wide diversity among her peers and adds that while a formal education can be helpful, it is not required to become a security researcher. Instead, Katie stresses the need for strong communication skills, attention to detail, and relentless curiosity.

As an ethical hacker from Jordan explained, "The work I do is good for all people—not just for me. It's about making an impact. I like that I'm securing online services used all around the world and helping people to trust their technology." Another ethical hacker from India commented, "I want people to look at security research as a creative art form rather than merely as a subject or skill."

Let's face it—our future will not be free of hackers, but it will be without the companies that remain complacent. Forward-looking organizations can unlock access to a formidable global network of expert ethical hackers working around the clock on their behalf. That is the power and wisdom of the Bugcrowd Platform. With this report, we are excited to introduce you to the committed members of our global researcher community.

Overview

This edition of *Inside the Mind of a Hacker* analyzes survey responses and security research on the Bugcrowd Platform from May 1, 2020 to August 31, 2021, in addition to millions of proprietary data points collected about vulnerabilities from 2,961 programs.

KEY TAKEAWAYS

- **Who** ethical hackers are, the skills they have, and the incentives that motivate them.
- **What** new survey findings can teach us about the next era of vulnerability disclosure.
- **When** ethical hackers do their best work and what gets in the way of their success.
- **Where** security researchers are focused and which industries leverage their expertise.
- **How** ethical hackers behave in high-stakes situations and when no one is looking.
- **Why** companies trust Bugcrowd to continuously secure innovation and mitigate risk.

REPORT HIGHLIGHTS

$27B[†]

of cybercrime prevented by ethical hackers working on the Bugcrowd Platform.

58%

of ethical hackers do not report a vulnerability if the company lacks a clear way to disclose it.

91%

of ethical hackers agree that point-in-time testing cannot secure companies year-round.

80%

of hackers encountered a vulnerability they had previously not seen before.

1 in 5

ethical hackers has extraordinary abilities in memory, creativity, and thinking.

213%

more companies used the Bugcrowd Platform to coordinate disclosure of a bug than last year.

47%

of ethical hackers earned more on Bugcrowd than they did in the previous period.

94%

of ethical hackers speak at least two languages and many are fluent in more than three.

←30min

time-to-payment for an ethical hacker who made a valid report on the Bugcrowd Platform.

[†]# of valid P1 findings made on the platform multiplied by the average cost of a breach, according to **IBM** in 2021.

Introduction

Digital transformation is no longer a race among security teams—it is a tug of war between old challenges and new opportunities.

Every organization faces the financial, reputational, and regulatory consequences of a cyberattack. As the average cost of a data breach soars to a **record-high** USD 4.24 million in 2021, it has never been more important for organizations to continuously secure the 400 vulnerable applications, networks, and services they have on average.

Yet, most tools and point-in-time assessments are pulling almost all security teams in too many directions with little context. These passive approaches keep companies stuck in reactive cycles and leave them vulnerable to malicious hackers who increasingly understand the far reaches of their organizations' attack surface better than they do.

Challenging these powerful forces is Bugcrowd, the award-winning crowdsourced cybersecurity platform that helps organizations secure their innovation sooner. Security researchers, also known as ethical hackers, are at the heart of the Bugcrowd Platform. They collaborate worldwide to build remarkable, often unacknowledged, careers defending digital assets and business-critical services for the most targeted companies.

Ethical hackers live across six of the world's seven continents and help organizations face unknown, unexamined, and unfixed bugs throughout their infrastructure or software development lifecycle (SDLC). Security researchers help Bugcrowd customers mitigate risk sooner and with less effort than traditional approaches through their diverse skills, from compliance audits to specialized expertise in niche technologies or particular methods.

$4.24M
The avergage cost of a breach in 2021

While stereotypes have long painted every hacker to be a menacing villain, real security researchers on the Bugcrowd Platform are highly-vetted experts with a demonstrable history of relevant professional success.

▶ **But can organizations really trust them? In this report, we dive inside the mind of ethical hackers to find out.**

Lifestyle

Humanizing Hackers

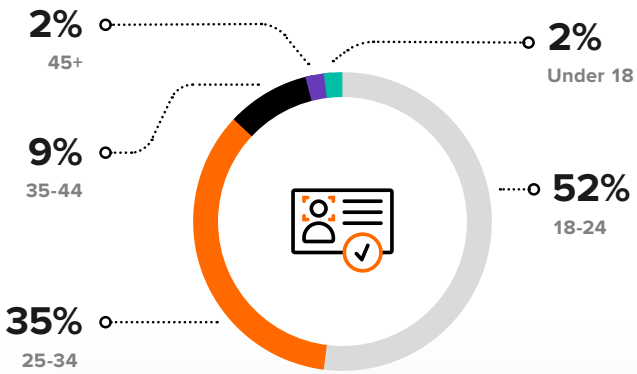
In the four decades since hacking made its first on-screen appearance in *Tron* (1982), Hollywood has relentlessly stereotyped hackers. From their ability to hack anything simply by typing "Override All Security" in *Superman III* (1983) to their representation as battling visualized 3D operating systems in *Avengers: Age of Ultron* (2015), hackers' work is villainized and—all too often—sensationalized by popular culture. Not to mention Matthew Broderick, who breached his school's database in *Ferris Bueller's Day Off* (1986) to change his grades, and a military supercomputer in *WarGames* (1983) that almost launched an unintentional nuclear strike on the former Soviet Union. But while these portrayals have long undermined mainstream perceptions of ethical hackers, today it is more important than ever to recognize these perceptions for what they are: Fiction.

As it turns out, the reality of hacking tells an entirely different story. Spanning 61 countries and more than 19 occupation types across the globe, Bugcrowd security researchers—also known as ethical hackers—make up one of the most diverse and multifaceted industries around the world. These digital natives are not only eclectic in their ethnicities, educations, and occupations; they are also neurodiverse (21%), multigenerational, and worth understanding more fully than ever before.

In this chapter, we will peel back the veil around the *mysterious* hacker and reveal their innermost workings. You will learn about their identities, get to know what makes them tick, and—by the end of this chapter—fundamentally reconceptualize what you think you may know about ethical hackers.

*Hackers are **diverse**, young individuals who come from **all walks of life**.*

AVERAGE AGE OF ETHICAL HACKERS



Ethical hackers are multigenerational and younger than ever. Millennials (born 1981–1996) represent more than a third of all ethical hackers, but 54% now belong to Gen Z (born 1997–2012)—the largest and most ethnically-diverse generation in **history**.

Faced with the worst job market since the Great Depression and disproportionate job loss throughout the pandemic, more skilled Zoomers are turning to the digital economy to kick-start ethical hacking careers. Raised under the ubiquitous influence of the internet and other modern technologies, these ethical hackers are highly engaged, digital natives who recognize their responsibility in shaping a more secure future for everyone.

As well-represented as ethical hackers tend to be in their ages, geographic locations, and educational backgrounds, a stunning 96% are male. The glaring gender gap is not simply an issue to address down the line: It poses a real, immediate threat to the diversity and multiplicity of perspectives that make crowdsourced cybersecurity such a powerful force today.

By incentivizing women or nonbinary individuals with broader scope and more accessible programs, organizations can empower a huge (and necessary) movement toward greater gender representation within the ethical hacking community. Without this continued advocacy, security teams risk spiraling into a homogenous, uninspired culture—not to mention falling short of their social responsibility to promote diversity within the workplace.

We are also proud to call some incredible female security influencers our teammates:

- **InsiderPhD** aka Katie Paxton-Fear
- **Farah_Hawaa** aka Farah Hawa

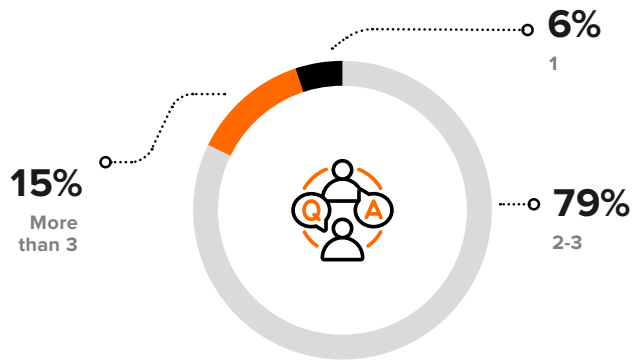
GENDER DIFFERENCES IN ETHICAL HACKERS

96% MALE

3% FEMALE

1% OTHER, NONBINARY, AGENDER, PANGENDER, OR GENDERFLUID

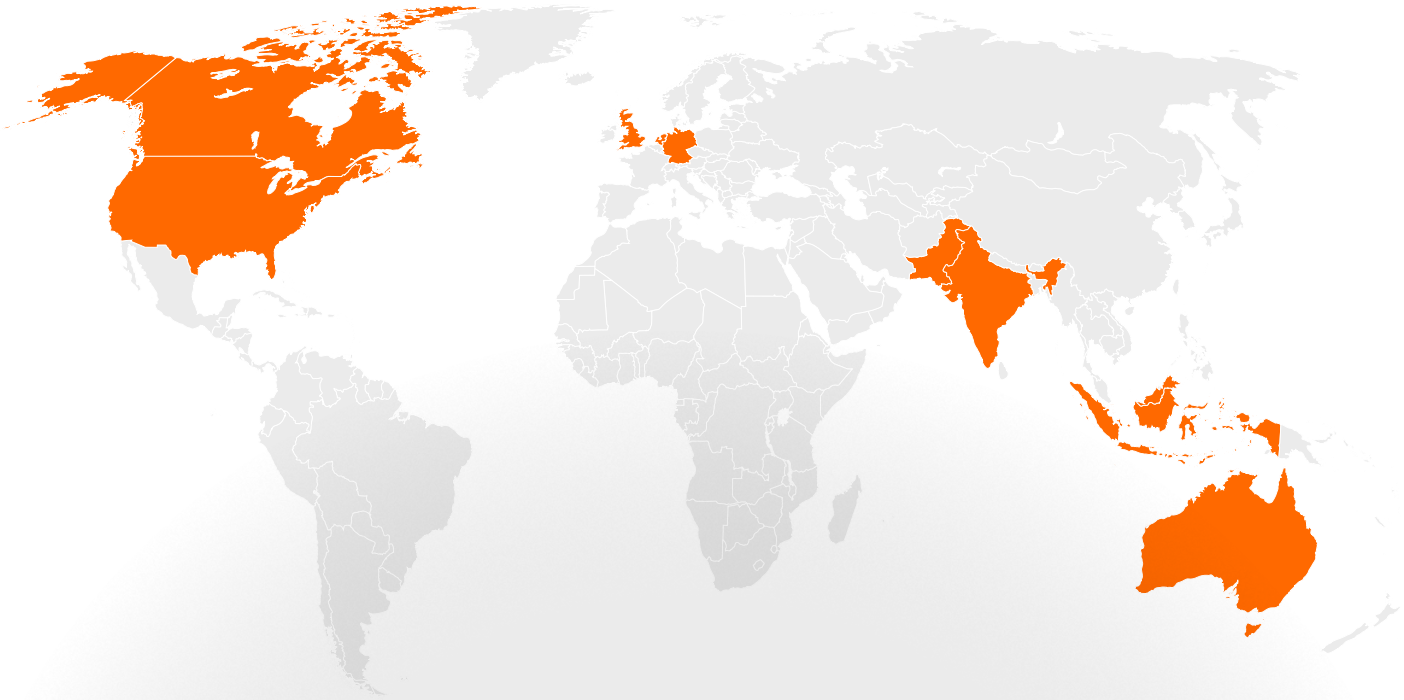
NUMBER OF LANGUAGES SPOKEN BY ETHICAL HACKERS



Language is a vehicle of knowledge, and 94% of ethical hackers are fluent in at least two. The cognitive benefits associated with speaking multiple languages are undeniable. Linguistic diversity enhances creativity and logical flexibility, equipping multilingual hackers to effortlessly switch between competing tasks and recognize changes in their environment.

Remarkably, ethical hackers on the Bugcrowd Platform are more likely to be fluent in three languages rather than just one. Studies also suggest that decisions made in an auxiliary language are more likely to be reason-driven, highlighting the adaptive way ethical hackers may deliberate in a second or third language to minimize their emotional biases.

TOP 10 COUNTRIES WHERE ETHICAL HACKERS LIVE



1. India
2. United States
3. United Kingdom
4. Australia
5. Germany
6. Canada
7. Netherlands
8. Indonesia
9. Pakistan
10. Turkey

*Hackers have **extraordinary** brains and unparalleled expertise in fringe topics.*

NEUROLOGICAL DIFFERENCES AMONG HACKERS

21%
NEURODIVERSITY

Neurodiversity 101

Neurodiversity refers to the infinite range of intellectual, developmental or learning variations in the human brain that can lead to extraordinary differences in areas such as attention, learning, and memory.

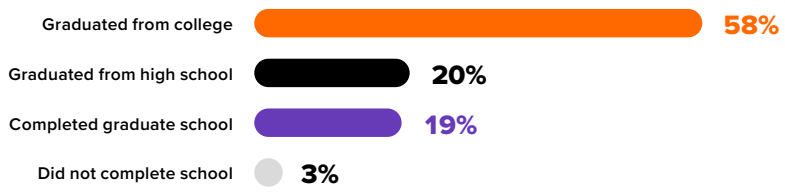
Diversity is routinely described by readily visible features like ethnicity and gender, but there is another set of characteristics that make one in five hackers unique: Neurodiversity. Most people are neurotypical, meaning that their brains behave in ways that society considers *normal*. However, 21% of Bugcrowd security researchers are neurodivergent, meaning that their brains learn and process information differently. This represents an 8% uptick since the last report and suggests that 1 in 5 security researchers perform better when given the opportunity to work remotely.

Science increasingly suggests that neurodiverse attributes were positively selected during evolution for contributing exceptional memory skills, heightened perception, and higher precision for detail. The spectrum of neurodivergence includes, but is not limited to, attention-deficit/hyperactivity disorder (AD/HD), autism spectrum disorder, asperger's syndrome, dyscalculia, dysgraphia, dyslexia, dyspraxia, obsessive-compulsive disorder, sensory processing disorder, synesthesia, and Tourette syndrome.

For example, in hunter-gatherer societies, AD/HD symptoms, such as hyperactivity, distractibility, and impulsivity, were highly adaptive skills because a person's survival hinged on their ability to forage for food, quickly respond to stimuli, and be deft in moving toward or away from potential prey. According to Dr. Devon MacEachron, a psychologist specializing in twice-exceptional and gifted learners, the same individuals now thrive in fast-paced careers—like ethical hacking—where their creativity and out-of-the-box thinking are generously rewarded.

Today, ethical hacking is a profession and subculture that allows the varied cognitive strengths of security researchers to shine without prejudice as to the challenges they might otherwise face. Bugcrowd proudly recognizes individuals of all abilities and will continue to accommodate the tremendous value that neurodiversity contributes to our platform.

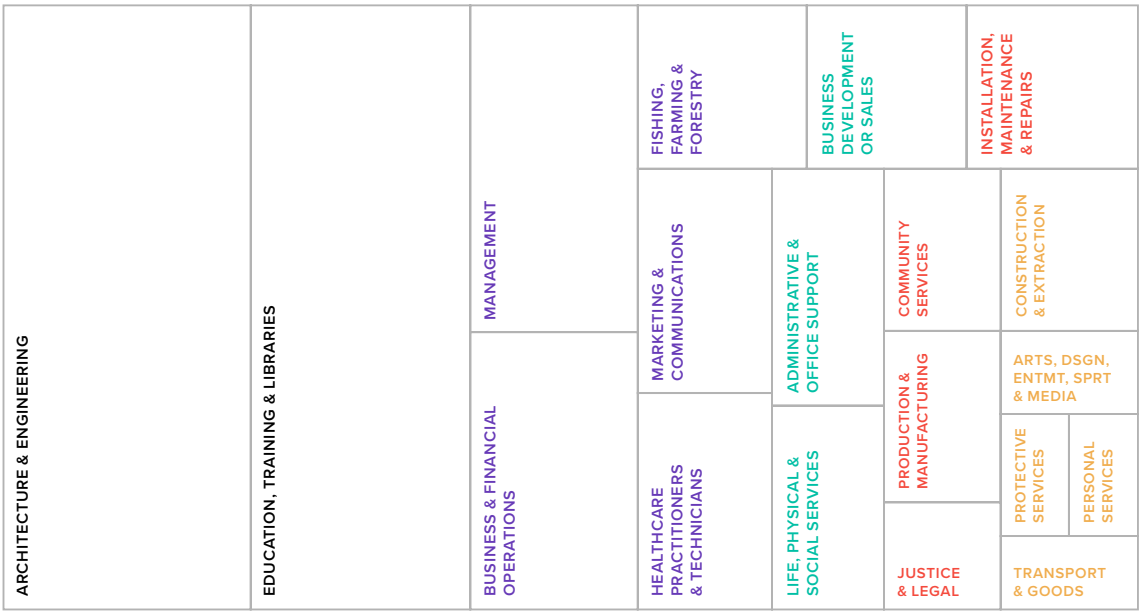
AVERAGE EDUCATION COMPLETED BY ETHICAL HACKERS



Security researchers are not hooded crooks who hack from dusk to dawn in scary, screen-lit basements. In fact, they represent a well-educated subset of the population whose keen resourcefulness, critical thinking skills, and subject matter expertise are in higher demand now than ever before. An impressive 77% of ethical hackers are college graduates, signaling the immense value that they bring to the future of security research and innovation.

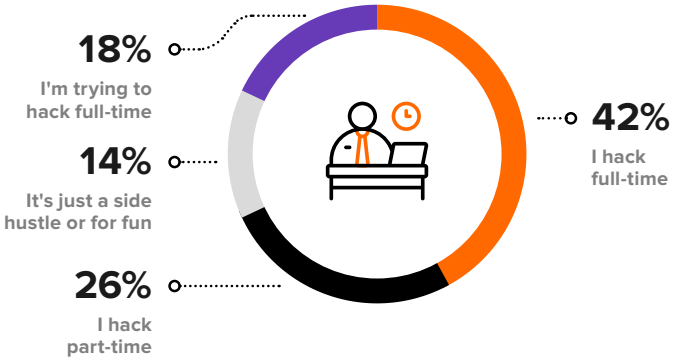
*Hackers have **wide-ranging** professional skills and are going full-time faster than ever.*

OCCUPATIONS HELD BY ETHICAL HACKERS UNRELATED TO SECURITY RESEARCH



Eighty-six percent of ethical hackers report working in IT or cybersecurity. The remaining 14% have jobs in unrelated industries.

EMPLOYMENT STATUS OF ETHICAL HACKERS



Opportunities in security research are expanding at an unprecedented rate. A stunning 42% of ethical hackers who work on the Bugcrowd Platform now report that they do so full-time—a 19% spike in security researchers going full-time over the past year alone. This explosive growth not only indicates the increasing strength of ethical hacking as a career but also underscores how the heightened demand for crowdsourced security continues to fuel the vulnerability economy.

THE ANATOMY OF A HACKER

$27B

of cybercrime prevented by ethical hackers working on the Bugcrowd Platform

21%

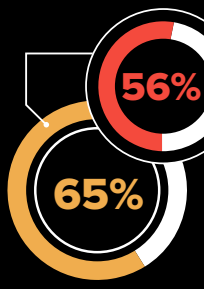
of hackers are neurodivergent and have extraordinary abilities in memory, creativity, or thinking

74%

of hackers agree there have been more vulnerabilities since the start of the COVID-19 pandemic

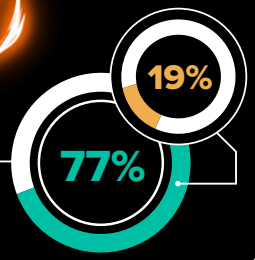
50%

of hackers earn more from Bugcrowd than they expected



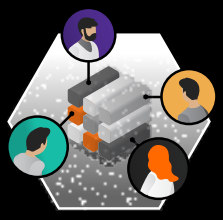
of hackers spend more than 5 hours per week working on the Bugcrowd Platform

of hackers say working on the Bugcrowd Platform helped them get a job in security



of hackers have postgraduate degrees

of hackers are college graduates



86%

of hackers think reporting a critical vulnerability is more important than trying to make money from it

58%

of ethical hackers do not report a vulnerability if the company lacks a clear way to disclose it

91 PERCENT

of ethical hackers agree that point-in-time testing cannot secure companies year-round

bugcrowd

Hacker Spotlight

Meet th3g3nt3lman—an ethical hacker from Jordan with more than a decade of security engineering experience.

th3g3nt3lman

th3g3nt3lman describes himself as a simple person with a passion for cybersecurity, football, world travel, and curating new life experiences. Having a natural curiosity for how things work since childhood, his father encouraged him to pursue future opportunities by studying computer engineering. Eventually, he found his way into a career that blended technology and engineering, and for a decade, he has niched down into ethical hacking.

A systems expert by trade, th3g3nt3lman championed his unique skills working as a penetration tester and auditor before he began consulting for companies on their security programs. However, the road to get there has taken a great deal of perseverance, time, and effort.

"There are always new challenges, new techniques to learn," he says. "The basics of networking and server administration are mandatory, plus basic knowledge of HTML and JavaScript, how web servers work—that's the recipe. If you get that right, the sky's the limit. Plus, there are many **resources out there** to help you start a professional security research career. If you have the passion and learn from your failures, you can succeed in hacking."

When asked which area of security companies should invest in, th3g3nt3lman responds, "People. They are the most important thing to invest in. If you have a well-trained security operations center, well-trained red and blue teams, and a good mentality among employees, you will be better secured than others."

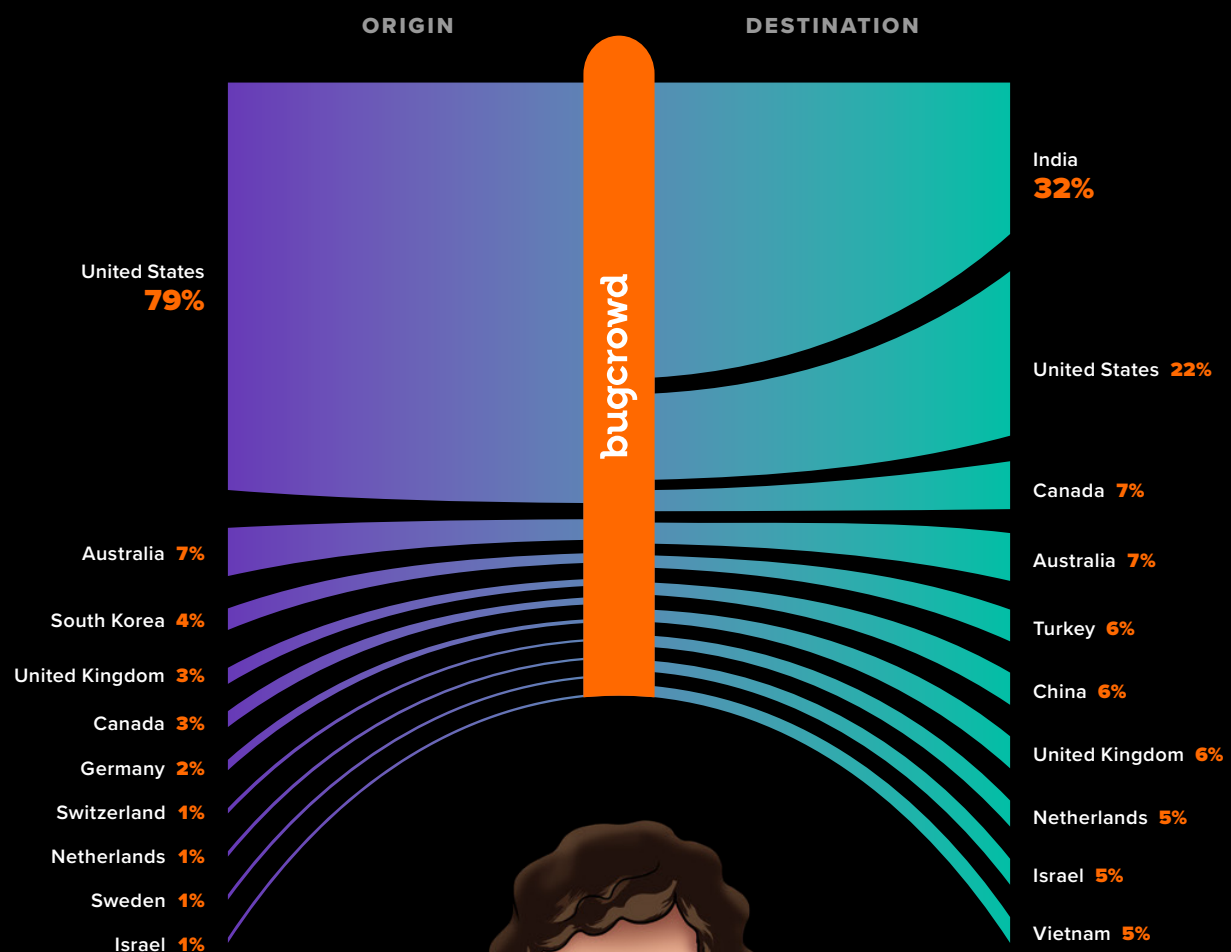
The good news is that companies are investing in people and talent development at an increasing rate. As a result, we understand, more and more every day, how invaluable the human expertise in cybersecurity is.

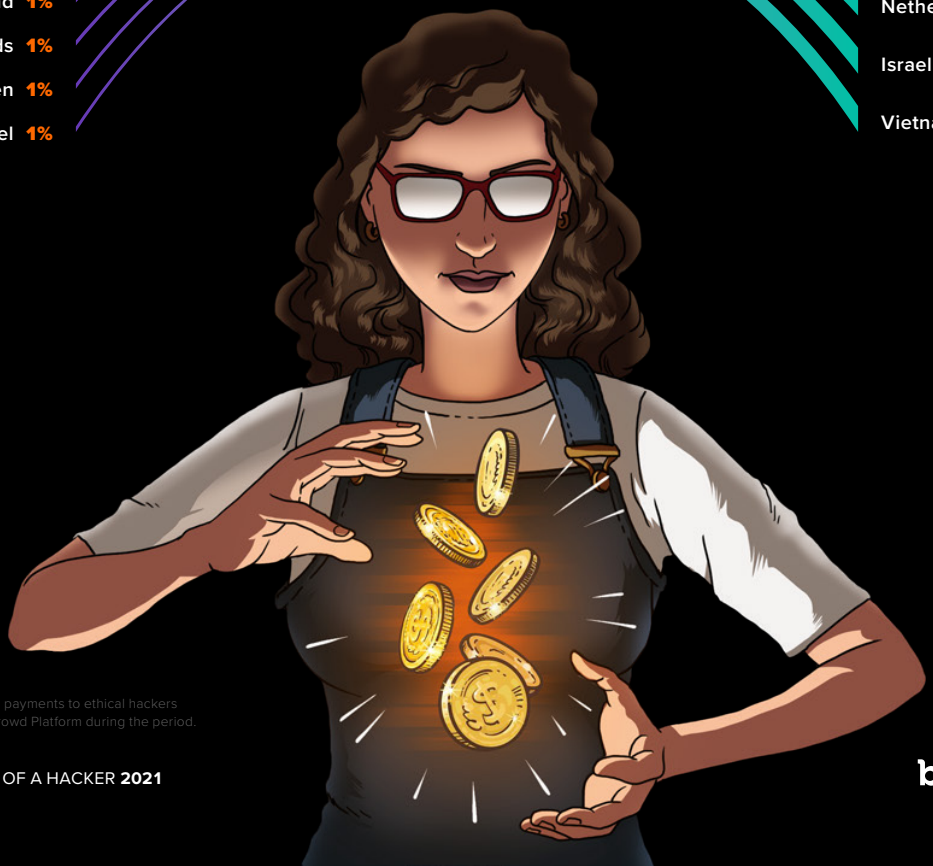
"A single ransomware attack can disable a company in a matter of seconds, turning the entire place into a warzone," says th3g3nt3lman. When the worst happens, a well-prepared incident response executed by knowledgeable and experienced security experts is the only lifeline you have.

The value of security in a growing technological workplace increases the demand for security researchers so that the good guys always outnumber the bad guys. As an ethical hacker, this engineer embraces the idea that he can use his unique skill set to do good in the world.

"The work I do is good for all people—not just for me. It is about making an impact. I like that I'm securing online services used all around the world and helping people to trust their technology without being scared."

GEOGRAPHIC DISTRIBUTION OF CASH FROM HACKING†





†Figure reflects material payments to ethical hackers processed by the Bugcrowd Platform during the period.

bugcrowd

Hacker Spotlight

Meet cinzinga—an ethical hacker from the United States who studied chemical engineering before pivoting into information technology and security research.

cinzinga_

People find their way to ethical hacking in all stages of their lives. Cinzinga, a 24-year-old college student and pop culture buff, got into security research after struggling to find the right academic program for his growing interests and career goals.

"I am quiet at first, but talk to me about hacking, Star Wars, or brewing beer, and you will quickly see my passionate side. A number of years back, I was going through a very uncertain and difficult period in my life. Rather than succumb to indecision and inaction, I decided to focus all my attention on learning cybersecurity as a practical tradecraft."

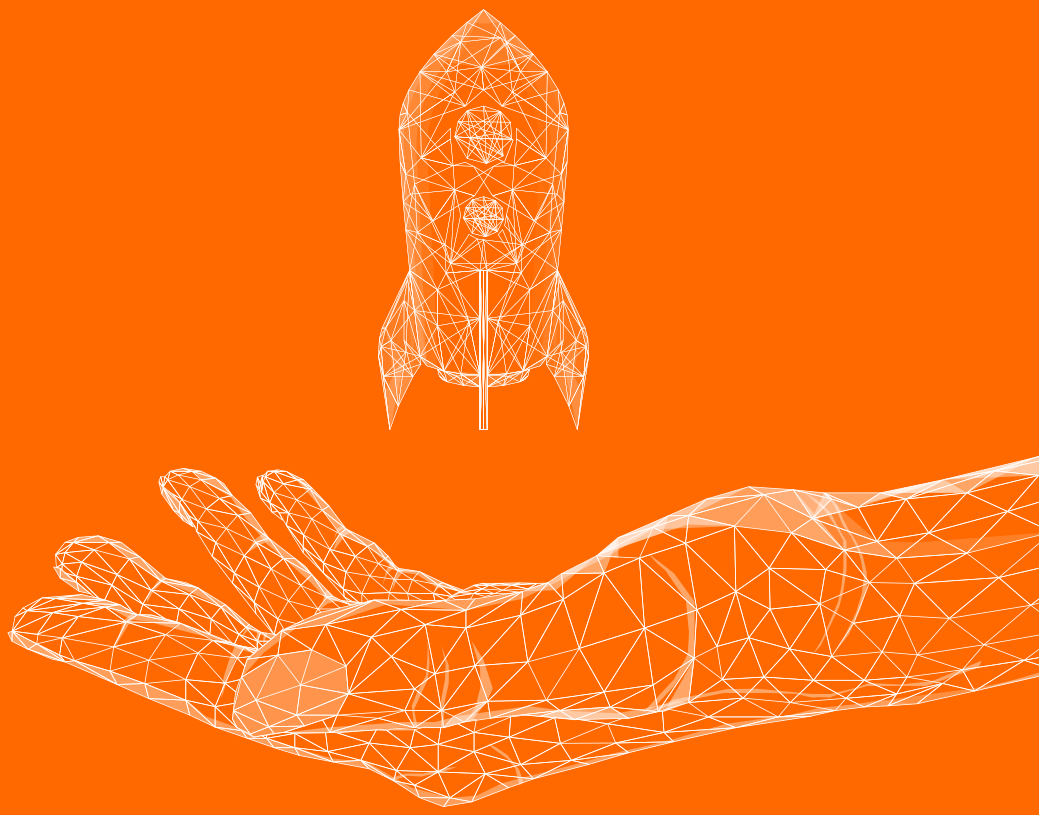
College students face big, life-defining decisions. Instead of allowing the fear of the unknown to hold him back and define his future, he channeled that energy into buckling down and learning the skills that would enable him to become an expert ethical hacker.

"While hacking gets a bad rap, the concept isn't inherently good or bad." Cinzinga explains that it is the intent behind the action that skews one way or the other on the morality scale. For example, malicious hackers are targeting businesses that can afford to pay big bucks when attackers breach their valuable data. But there are also just as many ethical hackers out there who level the playing field by matching their skills for benevolent purposes.

"The ability to learn on your own and do independent research is critical. No one is going to give you the solutions or answers needed to succeed. Success is the result of time and dedication."

The road to becoming a cybersecurity professional does not look the same for everyone. Young people interested in pursuing careers in ethical hacking should embrace the concept of lifelong learning to build agile, adaptable careers that keep pace with constant change.

"As a beginner, I found the Bugcrowd team to be incredibly supportive. They helped me understand why some of my earlier submissions were low-impact, and how I could improve in the future. I found this personalized feedback to be unparalleled among all the other platforms, and it truly helped me in the early days of my cybersecurity journey."



Expertise

Elevating Entrepreneurship

When it comes to pop culture, hackers often appear in spectacular montages (set to a sudden swell of frenetic music) racing to hit "Enter" before a bomb detonates—or some equally unrealistic event occurs. Real everyday successes, however, do not always involve Benedict Cumberbatch as Alan Turing cracking Germany's Enigma code in a climactic finale to win World War II (*The Imitation Game*, 2014). But what exactly, then, does success look like in the world of ethical hacking?

That is the question—one of many related questions, in fact—that we asked Bugcrowd security researchers, and the results are stunning. Seventy-nine percent of ethical hackers, for instance, are self-taught: Driven by a passion for their work (and doing it well), they acquire the skills they need on their own terms, and often on their own time. In the past year alone, 80% of hackers also found a vulnerability that they had never encountered before, suggesting the rate at which the threat landscape continues to shift second by second, day by day.

And that is not all. In this chapter, you will dive deep into the world of ethical hacking as both a practice and lifestyle, catching a rare close-up view of what security researchers really look like in action. What surprising things will you discover about this unique group's entrepreneurial minds?

You are about to find out.

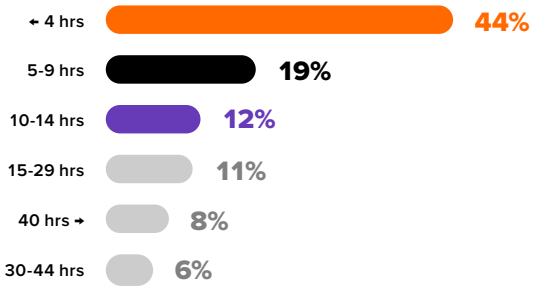
*Hackers are **fiercely loyal** and play a critical role in securing consumers' everyday lives.*

75% of security researchers dedicate up to 14 hours of their week to hacking on the Bugcrowd Platform.

While some reported working hours similar to most corporate professionals (14%), historical submission data indicates that security researchers still work fewer hours while earning an income similar to their salaried peers.

Unlike typical corporate jobs, ethical hacking offers people more flexibility so they can focus on the parts of security research they enjoy most.

HOURS DEVOTED TO HACKING PER WEEK ON BUGCROWD



WHERE HACKERS CHOOSE TO SPEND THEIR TIME

Ethical hackers are independent, free agents. While some work across multiple platforms, 45% choose to spend most of their time hacking on Bugcrowd. This finding underscores the loyalty of the global security research community, who value the care and respect with which their work is treated in programs on the Bugcrowd Platform.

INDUSTRIES THAT HACKERS WORKED WITH ON THE BUGCROWD PLATFORM IN THE PAST 12 MONTHS

CONSUMPTION-DRIVEN

- Consumer Services
- Corporate Services
- Consumer Products
- Food & Beverage
- Automotive
- Real Estate
- Media
- Retail

COMMUNITY-DRIVEN

- Civic & Non-Profit Groups
- Energy & Environmental
- Hospitals & Healthcare
- Telecommunications
- Schools & Education
- Sports & Recreation
- Transportation
- Government

ENGINEERING-DRIVEN

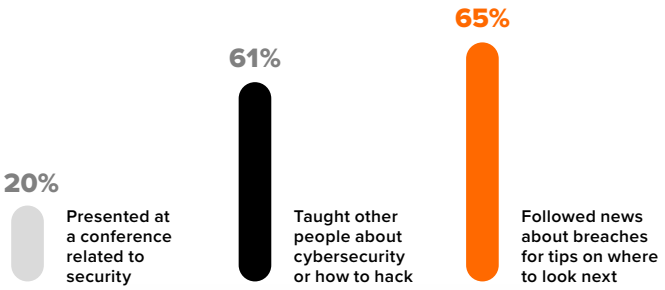
- Pharmaceuticals & Biotech
- Industrial Manufacturing
- Construction & Building
- Aerospace & Defense
- Computer Hardware
- Computer Software
- Electronics
- Chemicals

FINANCE-DRIVEN

- Holding Companies
- Financial Services
- Insurance
- Banks

Words like *cybersecurity* and *hacking* sound futuristic to some, but they extend well beyond the immediate realm of technology, computers, and the internet. Today, ethical hackers solve problems across every single step of the global supply chain, from construction and consumer services to retail and real estate. In fact, security research plays a prominent—and often unnoticed—part in our everyday lives: While the risk of being breached remains real, most consumers have already benefited greatly from the work of an ethical hacker without knowing it.

WHAT ETHICAL HACKERS WERE UP TO IN THE LAST 12 MONTHS



Ethical hackers keep up with the latest vulnerabilities and take self-improvement seriously. Over the last 12 months, 65% followed cybersecurity news closely and 61% taught others about hacking or security.

Driven by a shared desire to understand and grow, ethical hackers are democratizing their unique perspectives to push the boundaries of what is possible.

75%
of hackers think most companies' attack surfaces are getting harder to compromise.

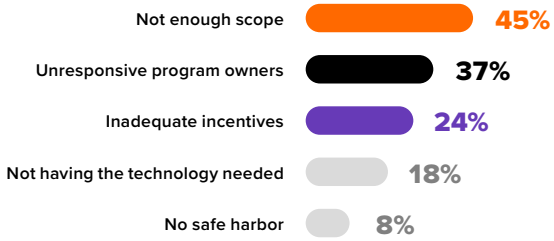
87%
of hackers think companies increasingly view them in a favorable light.

77%
of hackers think it is becoming more difficult to find critical vulnerabilities in assets.

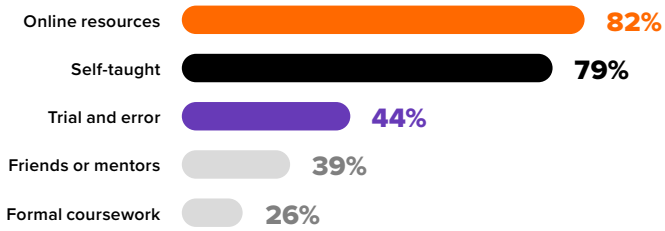
Forty-five percent of hackers report lack of scope as the main roadblock to success when working with organizations. While every company's risk appetite is different, programs with a narrow scope typically stop security researchers from identifying more impactful vulnerabilities. Entrusting ethical hackers with greater latitude allows them to do their work more effectively—and empowers companies to quickly reduce risk through more rigorous, holistic testing.

More than a third of security researchers also called out unresponsive program owners as the second biggest threat to their success. When ethical hackers are given the resources, respect, and responsiveness needed to succeed, organizations attract better talent and derive a greater return on their crowdsourced security investment.

COMMON BARRIERS TO HACKER SUCCESS



HOW ETHICAL HACKERS LEARN SKILLS



Remarkably, 79% of ethical hackers taught themselves how to hack using online resources.

Twenty-six percent of security researchers also report having completed professional or academic coursework related to cybersecurity and hacking.

bugcrowd

80%

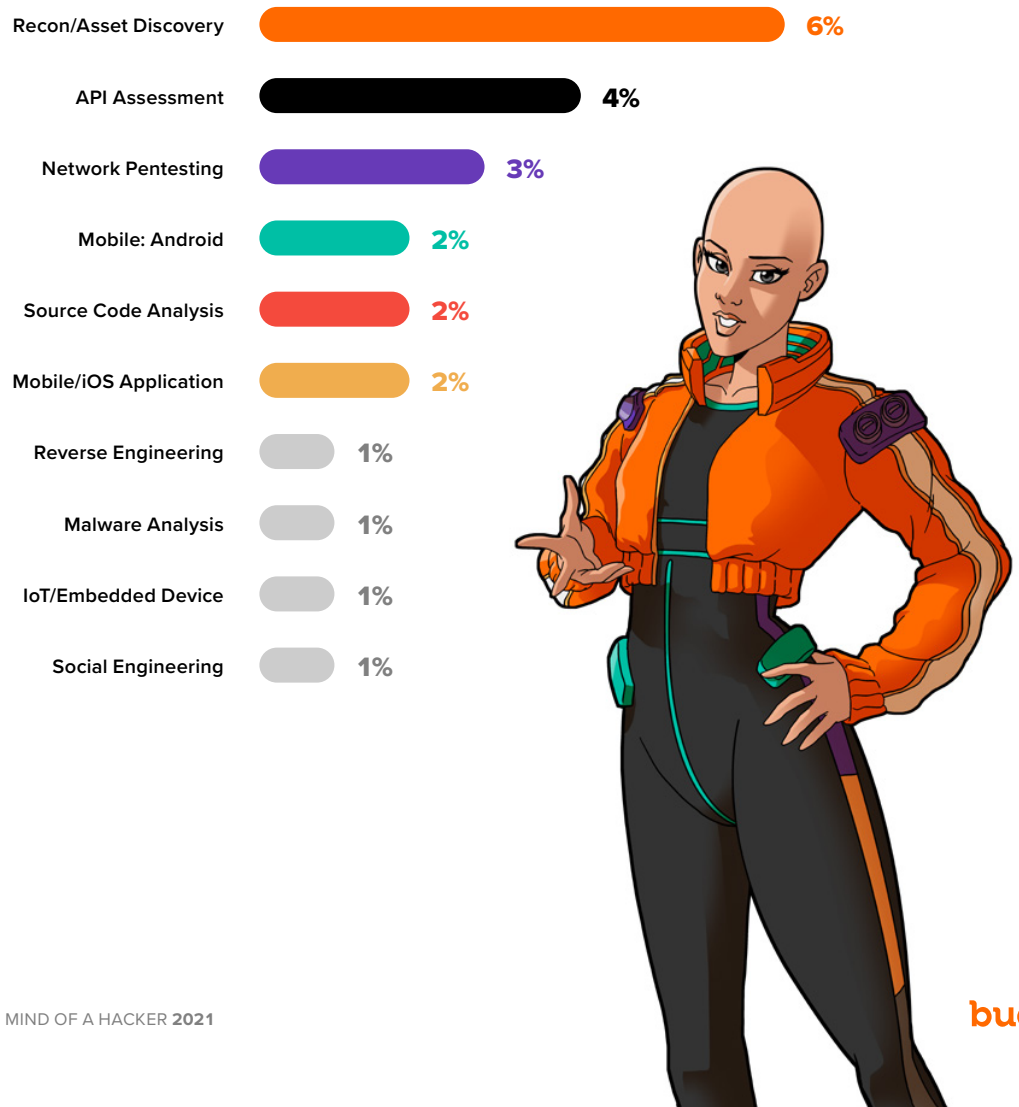
hackers found a vulnerability they had not encountered before in the past year.

New vulnerabilities emerge every day, but their exponential increase over the past year alone is alarming. By working with ethical hackers, organizations can level the playing field and proactively reduce their risk.

ETHICAL HACKERS' FAVORITE SECURITY SKILLS

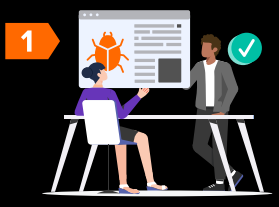
While 76% of ethical hackers prefer working on web applications, this list reveals some of the more specialized areas of their expertise and interests—from assessing APIs to analyzing source code. By dynamically matching the right trusted security researchers to companies' needs and environment, the Bugcrowd Platform paves the way for more diverse, innovative ways to think about cybersecurity and risk reduction.

Web Application Testing **70%**



bugcrowd

LIFECYCLE OF A HACKER SUBMISSION

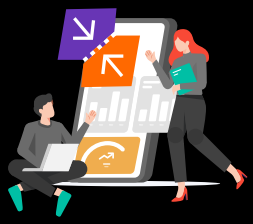


1 Review submission and confirm the alleged vulnerability is within scope

2 Determine if the vulnerability can be exploited and evidence findings

3 Assess the severity and impact of the vulnerability according to the Vulnerability Rating Taxonomy

4 Identify and document any further GDPR risks surrounding the submission



5 De-duplicate submissions so that vulnerabilities are only reported once

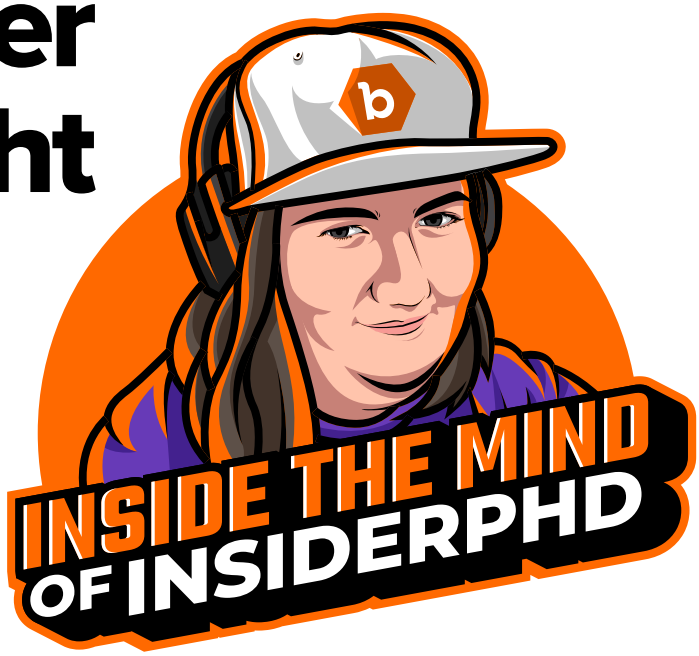
6 Approve all written reports and findings before sending to the customer

7 Redirect out-of-scope submissions based on the program or engagement

8 Provide the customer with a comprehensive checklist of all actions taken

9 Manage ongoing communication between the customer and security researchers

Hacker Spotlight



Meet InsiderPhD—an ethical hacker from the United Kingdom who enjoys hunting bugs, lecturing on cybersecurity, and creating educational content.

InsiderPhD

According to InsiderPhD (Katie Paxton-Fear), the critical skills every hacker needs include communication, attention to detail, and curiosity. While anyone can pick up a book, watch a video, or learn the technical skills to do a job, it is much more challenging to develop the *soft skills* every security researcher needs.

"Most people can think of ten uses for a paperclip, but people who are really good at what's called lateral thinking, don't just stop at thinking of a paperclip as a small, metal thing. They think, what if the paperclip was huge? What if the paperclip was made of glass? What if the paperclip was on your computer as an animated character telling you how to solve problems? We want people to be able to think outside the box, and that is the real value that things like crowdsourced security offers—a bunch of people that think in very different ways all hacking on one piece of software, because you'll get so many answers to a question like, 'How many uses can you think of for a paperclip?'"

As a hacker and educator with a background in academia, Katie recognizes that everyone's path to a career in technology looks different. Formal education programs can be helpful for some people, but they are certainly not a requirement to enter the field. Creativity and diversity, however, are both essential.

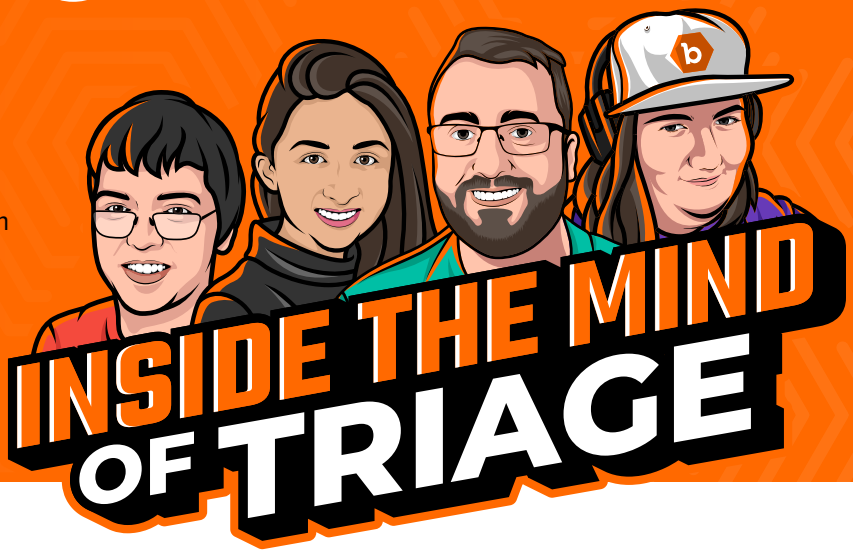
"I feel we need to move away from diversity as a box-ticking exercise and recognize that diversity is just good. It is morally good to say, 'We have a diverse range of people here.' It is also good from an organizational standpoint because when you have a diverse group hacking your stuff, they are all going to find different bugs, they are all going to come up with different ways of working, and that is going to be a net gain to any organization to be able to say, we didn't just have one type of person hacking us. We had so many types of people, which means we found so many types of bugs."

As a female, neurodivergent hacker, Katie is an advocate for social justice and a living example of the reasons to celebrate and embrace diversity in this growing industry.

"I speak all about autism because it's what I have, so therefore I know a lot more about it. But someone who is autistic can have hyper-focus moments where they are so invested in something, it is all they can focus on. They can focus for hours on one thing. And that is a real advantage because if you have somebody like that looking at your website, you have got the most dedicated security tester, right? You have got somebody that will go above and beyond because it is something they really enjoy."

Decoding Triage

Bridging the gap between hackers and organizations, we spoke to a handful of experts from our triage team about life on the front line of security and what sets Bugcrowd apart.



"I'm always really impressed with how creative hackers are."

Dr. Katie Paxton-Fear (**InsiderPhD**) is a lecturer, YouTuber, and one of four expert members of the Bugcrowd triage team who have converged to share their perspective on triaging. She is joined by Michael Skelton (**codingo_**), James McLean (**vortexau**), and Farah Hawa (**Farah_Hawaa**), a small portion of the global team that is responsible for triaging hundreds of reports daily.

"I feel so energized seeing an awesome report, and I'm blown away thinking 'Wow, I would have never thought to do it like that.' As a hacker myself it's a fantastic opportunity to see how other people think about and solve problems," says Katie.

The triage role is demanding, complex, and one that requires a diverse set of soft skills like communication, problem-solving, and a deep understanding of cybersecurity. It is no wonder that most of the Bugcrowd triage team are hackers themselves.

Michael Skelton went from being a Top 50 security researcher on the platform to leading the international triage team at Bugcrowd.

"The Bugcrowd triage team is responsible for the validation, enhancement, and verification of findings from researchers," says Michael. "This includes, but isn't limited to, validating findings, confirming if they are an existing duplicate or not, and supporting the customer through understanding and remediating the findings. Where expectation gaps exist between customers and researchers, the Bugcrowd triage team supports conversations and mutual understanding to ensure all parties are able to reach an equitable outcome."

The largest of its kind, Bugcrowd's in-house triage team are experts who have been hand-picked for their exceptional knowledge, skills, and experience in delivering world class security research.

"Our triage team is truly global, with representation across APAC (Asia-Pacific), US and Europe, making up a diverse and incredibly skilled application security engineer (ASE) team," says James. "The best bit about working with security researchers is seeing the positive influence that ethical hacking has on their economic prosperity— from college students being able to cover their tuition fees, to first-generation digital natives changing the course of their lives with little more than a computer, the internet and some creative ideas."

As well as helping both researchers and customers through verifying, prioritizing and enhancing the Crowd's findings, the triage team supports each other through the demanding and detail-driven workload they face each day.

"Triaging is the kind of job that is very autonomous in nature," Farah says. "Most days we work in our own little bubbles, but what I love about the Bugcrowd triage team is that when things get tough, we all come together as a team to churn and pull through it. Despite the differences in our time zones and cultures, we never hold back from helping each other and working as a team when the situation asks for it."

The strong sense of community and dedication to excellence are what really shine through about the Bugcrowd triage team.

"My favorite part about triaging is when I witness researchers growing on the platform," says Farah. "Quite often, we see researchers submitting informative or non-qualifying submissions when they start hunting, and as they progress we start seeing some valid submissions from them, and then a P2, and even a P1! It is good to know that I work for a platform that helps facilitate the Crowd's growth, and witnessing that growth up close is a great feeling."

Hacker Spotlight

Meet bsysop—an ethical hacker from Brazil with a knack for planning and executing *crazy* ideas that have the potential to influence our everyday reality.

bsysop

Ethical hackers are varied individuals who come from all walks of life. In one corner of the world is bsysop, 34, who describes himself as an imaginative, proactive security researcher who loves helping other people.

"When I was a teenager, I was always impressed by my older cousin who hacked and built things. In my mind, he was performing real-life magic. I actually got my first tip from him: 'You want to hack, kid? First learn TCP/IP.'"

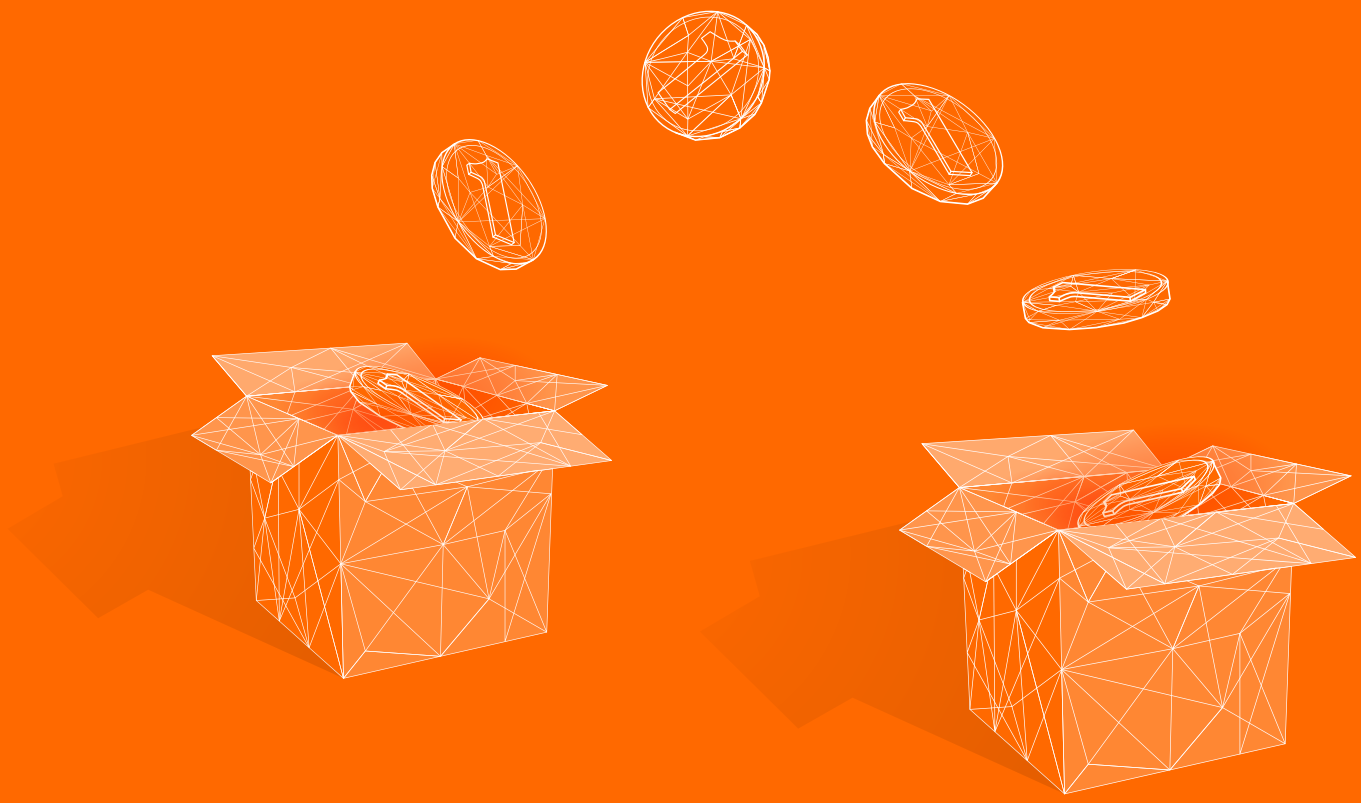
Reminiscing on his first encounter with the internet, bsysop recalls, "I had a Pentium II 550 mhz, a noisy 56kbps modem, and a dream. It was weird, but mIRC and Netscape opened a door for me that is impossible to close now." It takes intense curiosity and an insatiable appetite to build a successful career as an ethical hacker, and bsysop has both.

That said, security researchers must walk a tightrope to avoid landing on the wrong side of a lawsuit. "Even with non-intrusive vulnerabilities, nobody wants to be prosecuted because they're trying to help some company," bsysop says as he speaks about the delicate balance that ethical hackers often face. Having chosen not to disclose vulnerabilities in the past, he notes that most companies lack a clear channel to accept external feedback about their security. Fortunately, Bugcrowd Vulnerability Disclosure Programs (VDP) provide a fully managed framework to securely accept, triage, and rapidly remediate vulnerabilities submitted by anyone.

When asked what security tip he would offer the world, bsysop says, "I recommend everyone use password managers to set strong and unique passwords for everything they use. Humans are the weakest link in security, and in the event that an attacker is able to get your credentials, you want to limit their potential access to as few things as possible."

For bsysop, delving into the world of security research has enabled him to turn his passion into a lucrative career.

"I feel we can change many lives with technology. When we teach one person to use a computer both for the greater good and their work, we can change the life of a whole family and probably the future of a generation. To me, hacking is like a penthouse with many doors and windows, each a potential security gap."



Motivations

Illuminating Incentives

Whether it is an elaborate scheme to steal money from the U.S. mint in *Coin Heist* (2017) or creating a security system breach in *Ocean's 11* (2001), hacking in popular culture is often associated with greed, wealth, or financial gain. When it comes to ethical hacking, though, you might be surprised to learn that money is not the only motivator around town.

As a matter of fact, most ethical hackers on the Bugcrowd Platform are intrinsically motivated: More than half self-report using their skills to cultivate personal development, challenge themselves, and seek excitement from their work—a far cry from the selfish, harrowing hacking heists of Hollywood lore.

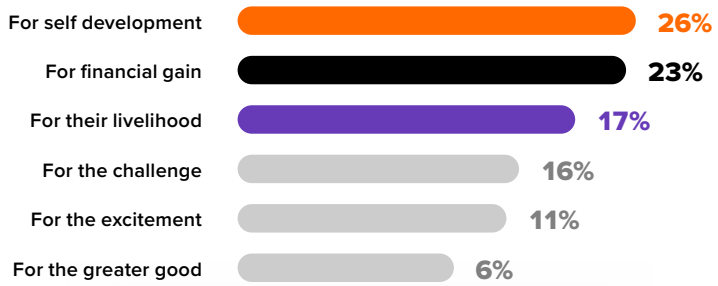
In this chapter, we'll walk you through exactly what goes on in the mind of the ethical hacker, from their perceptions of their impact on the cybersecurity community to their reasons for choosing to work on a particular security program. (**Pro tip: 72% decide to take on a new project because they enjoy collaborating with responsive teams.**) By better understanding why ethical hackers love their work—and why they love working with Bugcrowd, specifically—you will emerge from this chapter better equipped to cultivate great future partnerships with our ethical hackers.

*Hackers are strategic and care more about **personal development** than money.*

While money matters for some, the majority (55%) of security researchers describe ethical hacking as intrinsically motivated work.

They do it to cultivate personal development, challenge themselves, seek excitement, and give back to the community.

WHY THEY HACK



TOP MOTIVATIONS AMONG ETHICAL HACKERS

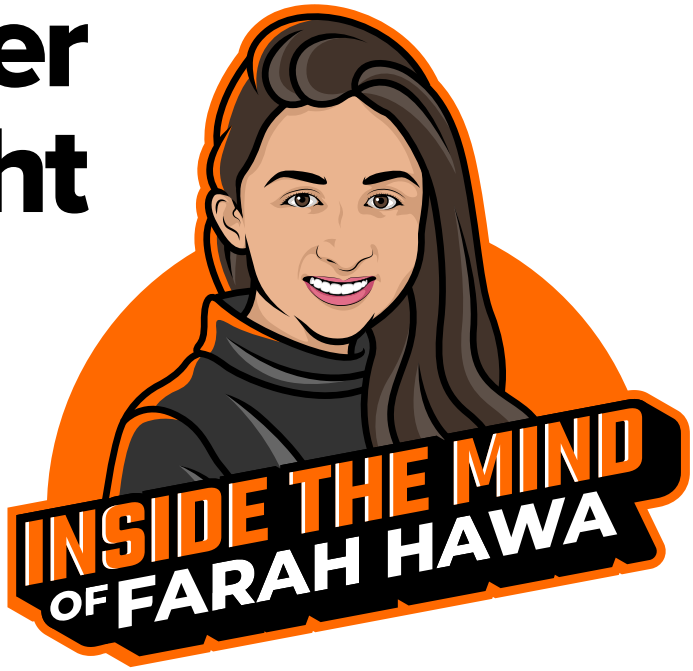
1. To reduce risk of breach and reputation damage for companies
2. To connect with more lucrative programs and engagements
3. To improve the ROI and performance of security in companies
4. To improve processes between security and engineering teams
5. To help companies accelerate their time to market securely
6. To fulfill *super secret* motivations they do not wish to jinx

WHAT MAKES A PROGRAM OR ENGAGEMENT ATTRACTIVE TO ETHICAL HACKERS

There is a common misconception that security researchers are drawn to programs that pay the most; however, our findings suggest that ethical hackers take a much more holistic approach when assessing their professional opportunities.

For most, choosing their next program boils down to a few key ingredients—and not all of them are related to money. An overwhelming 72% report "working with a responsive team" as their top reason for deciding to join a new program, while 54% consider "abundance of scope" as a high priority.

Hacker Spotlight



Meet Farah Hawa—an ethical hacker from India who believes that anyone can follow in her footsteps and enjoy learning the technical side of security research.

Farah_Hawaa

Farah Hawa is a familiar name, not just as a team member and security researcher at Bugcrowd, but as a growing content creator in the hacking community. Farah has a growing **YouTube channel** that is great for beginners and those looking to upskill at any stage in their career.

Farah brings a unique point of view to ethical hacking. Despite not coming from a technical educational background, she had the grit and desire to make it professionally as an ethical hacker, and her perseverance has paid off in a big way. She divides her time between creating bite-sized infotainment videos to help new hackers learn the trade, working for Bugcrowd, and chasing bounties to keep her hacking skills sharp.

"I have niched my channel down in a way that my videos only focus on breaking down complex technical vulnerabilities into more digestible bits. I think my audience definitely appreciates that in my content because I try to explain everything in the simplest way possible and—believe it or not—this is a pain point for a huge chunk of the infosec community, especially beginners."

Farah believes anyone can follow in her footsteps by taking the time to learn the technical side of security research, regardless of their background. A wealth of labs, blogs, and books cover the knowledge and skills that every hacker needs to know.

"I would recommend beginners start hunting on smaller programs because they have less competition and will be more likely to learn, grow their skills, and also build their motivation."

In her experience, it only takes one success to get hooked on hacking. And nobody understands the complexity of learning the trade like Farah. She started as an outsider, facing a steep learning curve to understand the concepts she needed to master.

Farah talked with us about the importance of embracing diversity in hacking. "We need as many different points of view as we can gather. As we diversify our niche across different cultures and backgrounds, welcoming those who have had experiences different from our own, we become stronger."

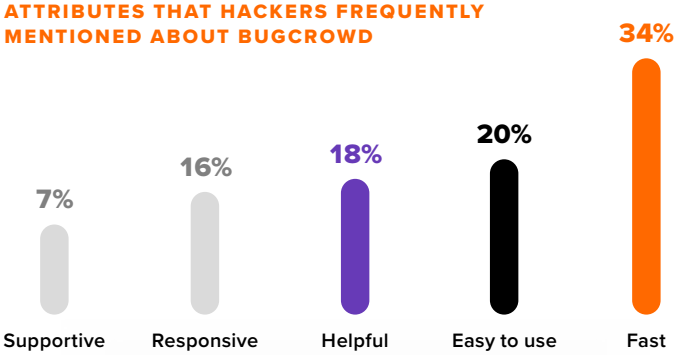
Indeed, strong and diverse teams taking a holistic approach to security is how the growing community can build more robust lines of defense in the face of a changing technology landscape. There is no argument that innovation will only continue to motivate nefarious hackers, which means that security researchers must continually welcome novice ethical hackers with open arms.

Farah has seen a lot of success with her YouTube channel and the various other educational projects she has collaborated on. She takes an authentic approach to help aspiring hackers tackle complex topics.

"I try to explain everything in the simplest way possible." Her refreshing communication style adds value that is hard to find among the sea of technobabble traditionally heard in IT and cybersecurity.

*Hackers are **discerning** and choose where they hack carefully.*

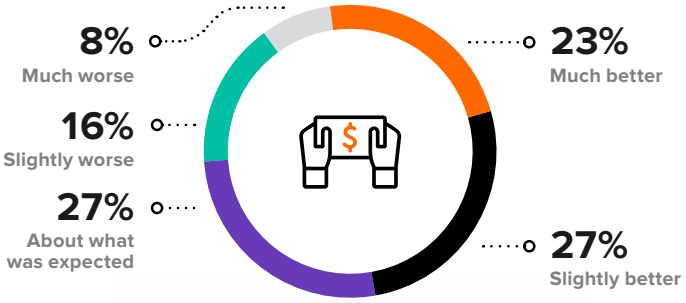
ATTRIBUTES THAT HACKERS FREQUENTLY MENTIONED ABOUT BUGCROWD



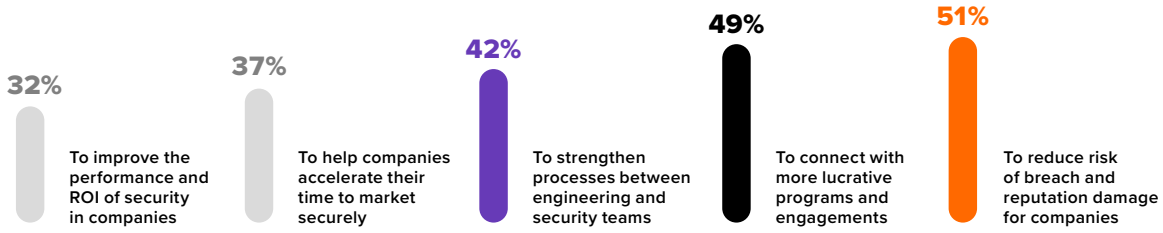
When asked what makes Bugcrowd unique, ethical hackers' responses were staggeringly positive: Over a third of security researchers referred to our triage team and platform as "fast," while others described Bugcrowd as "helpful" (18%) and "responsive" (16%).

The grass always looks greener on the other side, particularly in emerging industries and jobs. So, what do ethical hackers really think about what they earn? As it turns out, the majority have a positive opinion of the income they derive from security research, with half reporting that their current hacking income slightly or greatly exceeds their initial expectations. This positive trend highlights global organizations' increasing adoption of—and investment in—ethical hacking.

PERCEPTIONS OF EARNINGS FROM ETHICAL HACKING

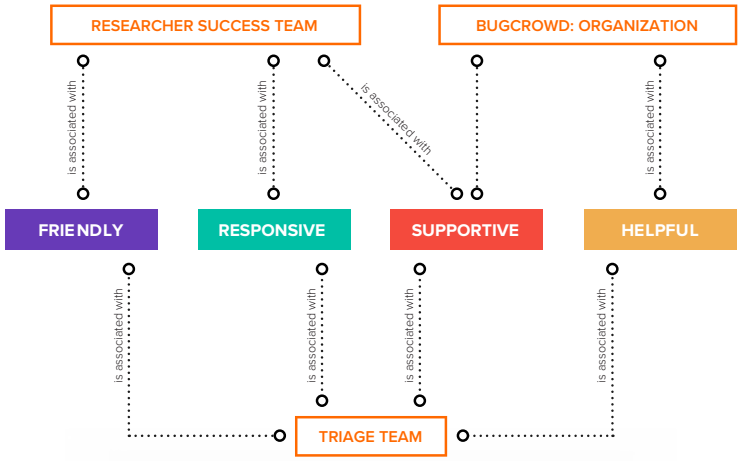


WHY ETHICAL HACKERS CHOOSE TO WORK ON THE BUGCROWD PLATFORM



Bugcrowd security researchers represent a well-educated subset of the population whose keen resourcefulness, critical thinking skills, and subject matter expertise are in higher demand now than ever before. An impressive 77% of ethical hackers are college graduates, signaling the immense value that they bring to the future of security research and innovation.

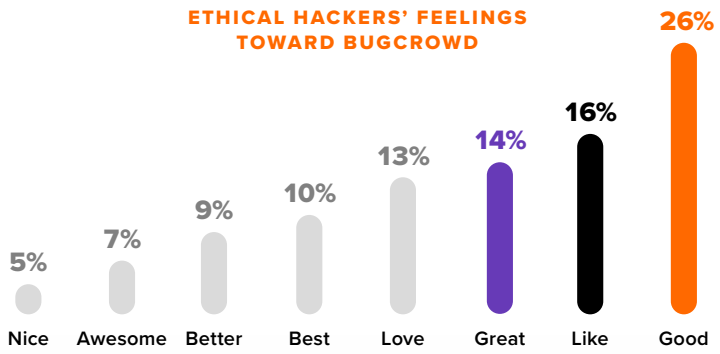
ATTRIBUTES THAT ETHICAL HACKERS FREQUENTLY LINKED BETWEEN TEAMS AT BUGCROWD



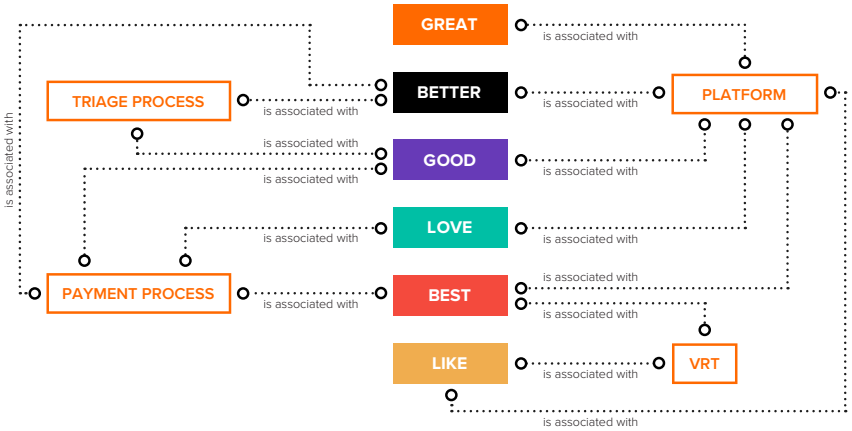
Bugcrowd is not just a platform; it is also an established community driven by distinct team members who help ethical hackers achieve their goals. Security researchers described these interactions with overwhelming positivity, making clear connections between Bugcrowd teams and core traits such as being *supportive* and *friendly*.

Do ethical hackers feel an emotional connection to the people, platform, processes, and technologies that make up Bugcrowd? We are positive they do—and the hackers are pretty positive about it, too. The majority reported feeling emotionally connected to the organization (using words such as *like* and *nice*), with nearly half indicating a particularly deep attachment (through strongly positive words such as *awesome, best, great,* and *love*).

ETHICAL HACKERS' FEELINGS TOWARD BUGCROWD



ATTRIBUTES THAT ETHICAL HACKERS LINKED BETWEEN PROCESSES AND TECHNOLOGY AT BUGCROWD



When it comes to championing collaboration and efficiency at Bugcrowd, processes like triage, payment, and severity rating are key. Ethical hackers working on the platform associate all three processes with a combination of highly positive attributes (*better, best, great*), indicating that they remain loyal to Bugcrowd because of the best-in-class service it provides.

Get to Know Growth

Meet Santerra and Bee—our community leaders who champion the experience that ethical hackers have when engaging with Bugcrowd and working on the platform.

Bugcrowd does not take the loyalty of the Crowd for granted. Instead, we are continuously investing in the growth, experience, and talent development of the security researchers who choose to work on our platform. As part of this mission, our hard-working Growth team crafts purposeful, educational, and inspiring content to engage the Crowd, building loyalty by providing continued professional development.

"Our goal is to provide the existing and new Crowd with the best experience out there," says Bee, the Growth team's researcher experience manager. "We want to ensure they have access to the resources, tools, and opportunities needed to be successful."

The Growth team is passionate about curating cutting-edge content that is both interesting and engaging for hackers. Researcher marketing coordinator Santerra believes that researcher advocacy is an important part of the Bugcrowd ecosystem that leads hackers to find success on the platform. She views engagement as a two-way street, listening to the needs of researchers and addressing their pain points through targeted content that helps the Crowd get the most out of Bugcrowd.

"I try to help the researchers by designing resources with them fully in mind," says Santerra.

"It would be natural to think that members of the Crowd are all in aggressive competition with each other, but what I see is a community that celebrates each other's victories, offers support, and at the end of the day, are a bunch of friends with a common goal."

ETHICAL HACKERS' HOTTEST TAKES

65%

OF RESEARCHERS WORKING ON THE BUGCROWD PLATFORM SAY THAT ETHICAL HACKING HELPED THEM GET A CYBERSECURITY JOB

In a recession of skills, cybersecurity has become a high-interest debt that is becoming impossible for organizations to pay down. Bugcrowd bridges the gap between security testing that must be done, and the shortage of human expertise needed to do it, by connecting today's organizations with the cybersecurity talent of tomorrow. As a result, 65% of security researchers report securing further professional employment thanks to the skills and experience they acquired while hacking on the Bugcrowd Platform.

58%

OF ETHICAL HACKERS HAVE NOT DISCLOSED A VULNERABILITY BECAUSE THE COMPANY LACKED A CLEAR PATHWAY FOR THEM TO REPORT IT

The threat of retaliation remains a real barrier to ethical hackers reporting bugs, as does the inability to report a vulnerability securely without further compromising the company or its data. Bugcrowd VDP overcomes this challenge by providing organizations with a secure, monitored channel that anyone can use to report potential risks, backed by our crowdsourcing-powered SaaS platform for multiple security solutions.

86%

OF HACKERS THINK REPORTING A CRITICAL VULNERABILITY IS MORE IMPORTANT THAN TRYING TO MAKE MONEY FROM IT

When it comes to conducting security research responsibly, ethical hackers understand the importance of doing their work for the right reasons. They do not hack just to make a pretty penny; instead, they uphold trust and prioritize reporting risks that may compromise the integrity of an organization's security, reputation, or customers.

96%

OF ETHICAL HACKERS BELIEVE THEY HELP COMPANIES FILL THEIR CYBERSECURITY SKILLS GAP

Finding a room full of security engineers is easy, but assembling a team of experts who specialize in testing a particular technology can be tricky. That is where crowdsourcing kicks in: Drawing from a global pool of security researchers increases the likelihood that an organization will find the expertise it needs—when it needs it—to reduce risk as effectively as possible.

74%

OF HACKERS AGREE THERE HAVE BEEN MORE VULNERABILITIES SINCE THE START OF THE PANDEMIC

Speed has long been the enemy of security, so it is no surprise that the pandemic spawned a panoply of never-before-seen vulnerabilities almost overnight. While companies continue to struggle with the transition, shifting economic incentives have prompted a wave of attacks across global supply chains and healthcare systems.

71%

OF HACKERS SAY THEY EARN MORE NOW THAT MOST COMPANIES WORK REMOTELY

In today's remote work landscape, ethical hacking has taken center stage—and not just due to the increasing number of vulnerabilities worldwide. Organizations now see the value in proactively engaging ethical hackers, who can help companies innovate more securely and with less risk.

Hacker Spotlight

Meet Ankit Singh—an ethical hacker from India who considers security research an art form and wants to positively redefine the term *hacking*.

AnkitCuriosity

Associations have long skewed negatively towards hackers. Ankit Singh, 27, says these perceptions are outdated and explains that the growing interest in hacking does not exclusively appeal to opportunistic people with questionable ethics. Many hackers—like him—consider it a professional art form, using their creativity to help companies find and fix vulnerabilities in their systems.

"Hacking isn't always a discrete subject. It is about the way you deliver your creativity and exploration to break into something based upon your understanding of how the given technology is built or developed. Your understanding of technology is the 'subject' and the additional creativity you employ is 'ethical hacking.'"

Ankit recalls a time before he knew the Bugcrowd Platform existed, finding it much harder to work as an independent security researcher and communicate vulnerabilities to companies.

"I remember in my early days of ethical hacking when I wasn't aware of Bugcrowd, I had found some bugs in a few organizations' production websites. I tried really hard to find their contact information and even called them about the issue—but they just hung up the phone before I could even explain. Maybe they didn't care, or maybe they had no idea what I was talking about."

Ankit says he got started in ethical hacking by reviewing publicly disclosed bugs. Studying the reports carefully, he learned approaches to implementing real-world attacks and taught himself how to expose vulnerabilities with practical tactics like reverse engineering.

"Organizations that lack a clear cybersecurity strategy and plan are a big problem. It is scary to see there are still companies living in a myth that no-one is going to breach their application or server. And so, they do not bother until a breach actually takes place. Traditional pentesting does not guarantee your security is foolproof. I have been on both sides of the profession, as a full-time penetration tester and now a full-time ethical hacker. And I'm absolutely aware that traditional pentests are not capable enough to cover up all of your bugs."

During our interview, Ankit spoke passionately about what advice he would give to aspiring ethical hackers. "If someone told me about platforms like Bugcrowd—and ethical hacking education opportunities—earlier, it would have changed everything." Anyone interested in pursuing a career in security research should take advantage of the vast **resources available** to learn outside of the confines of traditional college education.

"I am helping to change the world's perception of hackers," Ankit says. "I want people to look at security research as a creative art form, rather than merely a subject or skill."

Conclusion

Underestimating Utility

Last year we predicted that by 2025, the Bugcrowd Platform would prevent more than $55.5 billion in cybersecurity losses for organizations worldwide. It has been just one year since we made that statement, and we are happy to report that—with the help of the global security research community—we have already prevented over $27 billion of cybercrime since the last edition was published. Needless to say, far surpassing our original estimate is a not-too-distant reality, and we want to make sure you are part of the story when the time comes.

Inside the Mind of a Hacker 2021 offers new insight into the world of ethical hackers who are at the heart of the Bugcrowd Platform: Their eclectic identities, their kindred entrepreneurial spirit, and their shared and distinct motivations alike. Opening a door to unique perspectives on hacking, this report highlights the most critical cybersecurity issues of our time, how Bugcrowd security researchers are producing best-in-class results, and why organizations can trust ethical hackers to secure their future with confidence.

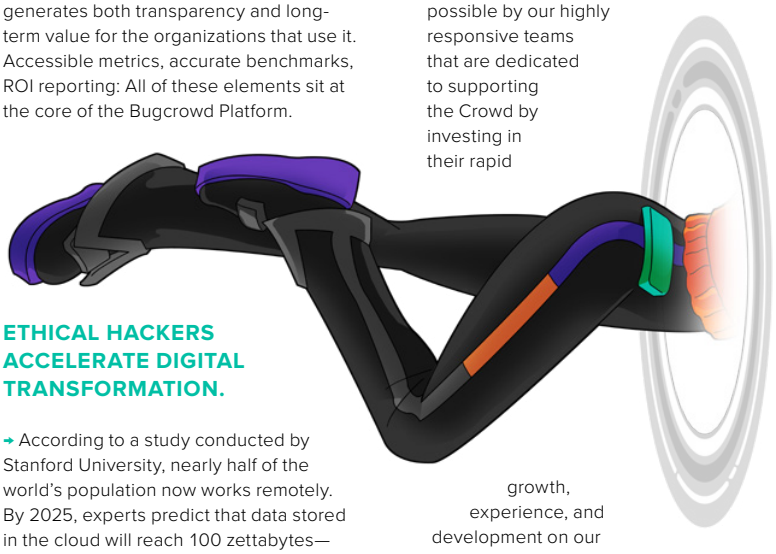
TAKEAWAYS

ETHICAL HACKERS REDUCE RISK.

- Risk reduction drives everything ethical hackers do: They empower organizations to conduct on demand security testing, meet compliance needs, and remediate vulnerabilities at various stages of the SDLC or in critical infrastructure.
- Backed by a crowdsourcing-powered SaaS platform for multiple security solutions, Bugcrowd provides an unparalleled signal-to-noise ratio with actionable remediation advice every step of the way.
- And because our **CrowdMatch™** technology dynamically matches organizations with the ethical hackers best suited to meet their needs, the Bugcrowd Platform has risk reduction down to a science.

ETHICAL HACKERS OFFER THE GREATEST SECURITY ROI.

- Around the world, cybersecurity leaders and CISOs are being asked the same questions: How great is the return on investment for a new security program? Does this security undertaking improve the organization's security posture, really—and if so, by how much?
- With cybercrime accounting for over $1 trillion in global losses (or more than one percent of the global GDP) as of 2021, organizations must now find more cost-efficient ways than ever to run security programs that can also save themselves from astronomical losses through breaches or cyberattacks.
- The Bugcrowd Platform is designed to promote this investment equilibrium. Through its clear reporting on program spending and performance, the platform generates both transparency and long-term value for the organizations that use it. Accessible metrics, accurate benchmarks, ROI reporting: All of these elements sit at the core of the Bugcrowd Platform.



ETHICAL HACKERS ACCELERATE DIGITAL TRANSFORMATION.

- According to a study conducted by Stanford University, nearly half of the world's population now works remotely. By 2025, experts predict that data stored in the cloud will reach 100 zettabytes—constituting 50% of the world's total data, up from 25% in 2015. Digital change is happening every day, and it is happening fast.
- With that change comes a critical need for acceleration and mobilization. The Bugcrowd Platform provides clear reporting that even non-security professionals can understand, empowering entire organizations to leverage insights from ethical hackers and their security programs. Because speed is the enemy of cybersecurity, we ensure that every program or engagement can be launched in record time.
- And all of this is made possible by our highly responsive teams that are dedicated to supporting the Crowd by investing in their rapid growth, experience, and development on our platform. By empowering a global network of unparalleled ethical hackers to remain agile and autonomous, we have created a passionate, knowledgeable community that is flourishing even as the security landscape continues to shift unpredictably.

About Bugcrowd

The world's first crowdsourced cybersecurity platform for multiple solutions, Bugcrowd generates better results, reduces risk, and empowers organizations to release secure products to market faster.

See Everything

Understand the far reaches of your attack surface better than your attackers do.

Find More

Rely on a global network of trusted researchers to find issues in near real-time that scanners and other approaches miss.

Fix Faster

Remediate early across your SDLC through pre-built integrations with JIRA, GitHub and ServiceNow.

Verify & Prioritize

Always know which bugs to fix first, informed with contextual insight, and managed by our in-house triage team.

sales@bugcrowd.com

press@bugcrowd.com

(888) 361 9734

Glossary

- ***Application Security Engineer (ASE):*** Responsible for ensuring the secure function of software application programs
- ***Asset:*** Any data, device, or environmental component that supports information-related activities. Assets generally include hardware, software, and confidential information.
- ***Attack Surface:*** The sum of the different points in a software environment where an unauthorized user can enter or extract data. Minimizing the attack surface is a basic security measure.
- ***Attacker:*** An individual or group who performs malicious activities to destroy, expose, alter, disable, steal, or gain unauthorized access to or make unauthorized use of an asset.
- ***Auditor:*** Someone who looks at the safety and effectiveness of computer systems and their security components.
- ***Bad Actor:*** Also called a malicious actor or threat actor, an entity that is partially or wholly responsible for an incident that impacts or has the potential to impact an organization's security.
- ***Black Hat:*** Bad actors that operate alone or in groups and may be sponsored by nation-states or organized crime rings who break into otherwise secure networks and assets with the primary purpose of stealing, destroying, or modifying data, extorting or stealing funds, or making the networks and information systems unusable.
- ***Blue Team:*** A group of individuals who analyze information systems to ensure security, identify flaws, verify the effectiveness of security measures, and ensure all security measures continue to be effective after implementation.
- ***Bounty:*** Monetary rewards offered in exchange for a vulnerability finding/discovery/report.
- ***Bounty Hunter:*** Highly skilled hackers who receive recognition and compensation in exchange for reporting bugs, especially those pertaining to security exploits and vulnerabilities.
- ***Breach:*** A cyberattack in which sensitive, confidential, or otherwise protected data has been accessed or disclosed in an unauthorized manner.
- ***Bug:*** A software defect that can be exploited to gain unauthorized access or privileges on a computer system.
- ***Bug Bounty:*** Bug bounty programs allow independent security researchers to report bugs to an organization and receive rewards or compensation.
- ***Chief Information Security Officer (CISO):*** The senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure assets and technologies are adequately protected.
- ***Coordinated Disclosure:*** Managed by the Bugcrowd Platform, coordinated disclosure enables program owners and researchers to agree upon a date and scope of the information they will reveal, before publicly disclosing a vulnerability or exploit.
- ***Credentials:*** The verification of identity or tools for authentication. These may be part of a certificate or other authentication process that helps confirm a user's identity in relation to a network address or system ID.
- ***Crowdsourced Security:*** An organized security approach wherein ethical hackers are incentivized to search for and report vulnerabilities in the assets of a given organization. The power of crowdsourced security is derived from the proportion of active testers per asset/ecosystem versus more traditional testing methods.
- ***Customer:*** Organizations that leverage the Bugcrowd Platform or its associated services.
- ***Cybersecurity and Infrastructure Security Agency (CISA):*** A standalone United States federal agency that operates under the Department of Homeland Security's oversight. Its activities are a continuation of the National Protection and Programs Directorate.
- ***Digital Transformation:*** The process of fundamentally changing an organization with technology and culture to improve/replace what existed before.
- ***Disclosure:*** The practice of reporting security flaws in computer software or hardware.
- ***Engagement:*** Refers to professional services or specialized testing for customers on the Bugcrowd Platform.
- ***Ethical Hacker:*** A person who hacks into a computer network in order to test/evaluate its security, rather than acting maliciously.
- ***Ethical Hacking:*** An authorized attempt to gain unauthorized access to a computer system, application, or data.
- ***General Data Protection Regulation (GDPR):*** A legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU). Since the Regulation applies regardless of where websites are based, it must be heeded by all sites that attract European visitors, even if they do not specifically market goods or services to EU residents.
- ***Hacker:*** Someone who uses technical knowledge to achieve a goal or overcome an obstacle within a computer system by non-standard means.
- ***Hypertext Markup Language (HTML):*** The standard markup language for documents designed to be displayed in a web browser.
- ***Internet of Things (IoT):*** Any device (often called a smart or connected device) that connects to and exchanges information over the internet.
- ***Incident Response:*** A term used to describe the process by which an organization handles a data breach or cyberattack, including the way the organization attempts to manage the consequences of the incident so that damage, recovery time, and costs are limited and collateral damage, such as brand reputation, is kept to a minimum.
- ***JavaScript:*** A scripting or programming language that allows you to implement complex features on web pages.

- ***Malicious Hacker:*** Someone who is actively working to disable security systems with the intent of either taking down a system or stealing information.
- ***mIRC:*** mIRC is an Internet Relay Chat client for Windows, created in 1995. It is a fully functional chat utility, and its integrated scripting language makes it extensible and versatile.
- ***Netscape:*** Netscape Navigator was the flagship product of Netscape Communications Corp. and the dominant web browser in the 1990s, but by around 2003, its use had almost disappeared.
- ***Neurodiversity:*** Variation in the human brain regarding sociability, learning, attention, mood, and other mental functions.
- ***Payout:*** The money paid to a researcher once their vulnerability submission has been validated.
- ***P1:*** Critical: Vulnerabilities that cause a privilege escalation from unprivileged to admin or allow for remote code execution, financial theft, etc.
- ***P2:*** High: Vulnerabilities that affect the security of the software and impact the processes it supports.
- ***Password Manager:*** A software application designed to store and manage online credentials, usually stored in an encrypted database and locked behind a master password.
- ***Penetration Tester / Pentester:*** Someone who professionally attacks computer systems in order to find security weaknesses that can then be fixed.
- ***Penetration Testing / Pentesting:*** A simulated cyberattack done by authorized hackers that tests and evaluates the security vulnerabilities of the target organization's computer systems, networks, and application infrastructure.
- ***Platform / SaaS Platform:*** Bugcrowd is an all-in-one SaaS platform that combines actionable, contextual intelligence with the skill and experience of the world's most elite hackers to help leading organizations solve security challenges, protect customers, and make the digitally connected world a safer place.
- ***Point-in-Time Assessment:*** A point-in-time review of a company's technology, people, and processes to identify problems. Such assessments can find vulnerabilities at a single moment, but fail to monitor activity between assessments.
- ***Program:*** A program—which can be public or private—permits independent researchers to discover and report security issues that affect the confidentiality, integrity, or availability of customer or company information and rewards them for being the first to discover a bug.
- ***Program Brief:*** A single page, researcher-facing document that contains all relevant information regarding a bounty program (what is in/out of scope, rewards, how submissions will be rated, instructions for accessing or testing the application, etc.). This is drafted with the Bugcrowd team after the initial kickoff call.
- ***Ransomware:*** A type of malware designed to extort money from its victims, who are blocked or prevented from accessing data on their systems.
- ***Red Team:*** A group that plays the role of an enemy or competitor and provides security feedback from that perspective. Red teams are used in many fields, especially in cybersecurity, airport security, the military, and intelligence agencies.
- ***Scanners:*** A vulnerability scanner is a computer program designed to assess computers, networks, or applications for known weaknesses.
- ***Scope:*** Outlines the rules of engagement for a bounty program. This includes a clearly defined testing parameter to inform researchers what they can and cannot test, as well as the payout range for accepted vulnerabilities.
- ***Security Landscape:*** The entirety of potential and identified cyber risk affecting a particular sector, group of users, time period, etc.
- ***Security Operations Center:*** A centralized unit that deals with security issues on an organizational and technical level, comprising three building blocks: people, processes, and technology.
- ***Security Research:*** The study of technology, algorithms, and systems that protect the security and integrity of computer systems, the information they store, and the people who use them.
- ***Security Researcher:*** Refers to the diverse group of skilled participants that hunt for vulnerabilities using the Bugcrowd Platform. These trusted experts are sometimes referred to as white hats or ethical hackers.
- ***Software Development Lifecycle (SDLC):*** A structured process that enables the production of high-quality, low-cost software in the shortest possible time.
- ***Submission:*** The report a researcher submits to Bugcrowd describing the vulnerability or bug they found.
- ***Target:*** A web or mobile application, hardware, or API that the Crowd tests for vulnerabilities.
- ***Transmission Control Protocol and Internet Protocol (TCP/IP):*** The set of communications protocols used in the internet and similar computer networks.
- ***The Crowd:*** The global community of white hat hackers on the Bugcrowd Platform who compete to find vulnerabilities in bug bounty programs.
- ***Triage:*** The process of validating a vulnerability submission from raw submission to a valid, easily digestible report.
- ***Valid:*** The state of a vulnerability that has been tested and confirmed as real.
- ***Vulnerability Rating Taxonomy (VRT):*** The official standard used by Bugcrowd for assessing, prioritizing, and benchmarking the severity of security vulnerabilities.
- ***Vulnerability:*** A security flaw or weakness found in software or in an operating system that can lead to security concerns.
- ***Vulnerability Disclosure Program (VDP):*** Clear guidelines for researchers to submit security vulnerabilities to organizations while also helping organizations mitigate risk by supporting and enabling the disclosure and remediation of vulnerabilities before they are exploited. VDPs usually contain a program scope, safe harbor clause, and method of remediation.
- ***White Hat Hacker:*** A computer security expert who uses penetration testing skills to help secure an organization's networks and information system assets. A white hat hacker is also known as an ethical hacker. White hat hackers work with information technology and network operations teams to fix vulnerabilities before black hat hackers discover them. White hat hackers operate with the permission of the organization and within the set boundaries.
- ***YouTuber:*** A person who uploads, produces, or appears in videos on the video-sharing website YouTube.

INSIDE THE MIND OF A HACKER

2021

bugcrowd