Overview

High-profile breaches continue to be the norm, driving more enterprise organizations to adopt crowdsourced security programs. As a result, the idea of “ethical hacking” has finally begun to resonate with the general public. This rise in popularity has inspired many — from aspiring hackers to seasoned security professionals — to join the hacking community and seek out crowdsourced security testing programs to “hack on”.

The beauty of the crowdsourced security model is that it brings together these hackers from all around the world — with different experiences, perspectives and backgrounds, enabling organizations to leverage this untapped talent — something that would be nearly impossible otherwise. Whitehat hackers range in experience — from students just learning about security to some of the world’s top security talent.

Crowdsourced security programs are great not only for new hackers to get familiar with security testing but also for industry pros to stay up-to-date on their skills or earn cash on the side. If you stick with it, the elite whitehat hackers can make hundreds of thousands of dollars per year bug hunting.

According to a recent report, **71% of cyber criminals say they can breach the perimeter of a target within 10 hours**. We need the whitehat community to combat this threat. By putting the numbers, expertise, motivation and speed of the whitehat hacker community to work in your favor, a crowdsourced security program will give your enterprise the tools and processes to rapidly test your product and discover and fix flaws in record time.

The 2019 Edition of the Inside the Mind of a Hacker Report highlights the makeup of the whitehat hacking community to provide insight and understanding into who they are, what they like to do, their experiences, skillsets, as well as what motivates them. In the 2019 edition, we look at gender inequality, hacking education and the Bugcrowd Elite, MVP and Top 50 – All Time Crowds.

Key Findings

81% of hackers say their experience bug hunting has helped them get a job in cybersecurity.

43% of hackers learned how to hack via online resources and blogs and 41% are self-taught.

A mere 4% of the global hacking community are female; more than 91% are male.

More than 20% of hackers aspire to be top security engineers or CISOs at large tech companies.

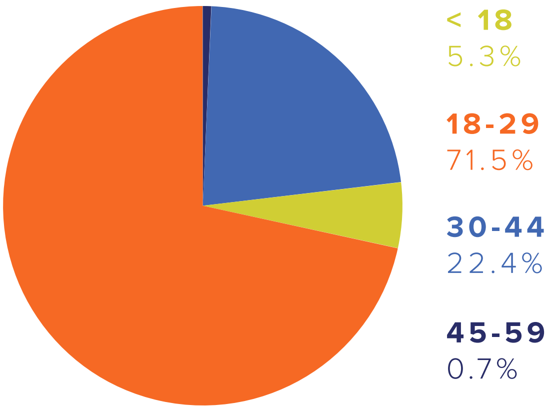
35% of the community say they currently collaborate with other hackers, and 50% expect to collaborate more in the next 12 months.

66% spend up to 10 hours per week bug hunting. That is significant given more than 50% of the hacker community bug hunts on top of a regular 9-5 job.

The average yearly payouts of the top 50 hackers is $145,000 USD with over 600 valid submissions. The average submission payout per vulnerability across the platform is $783 USD.

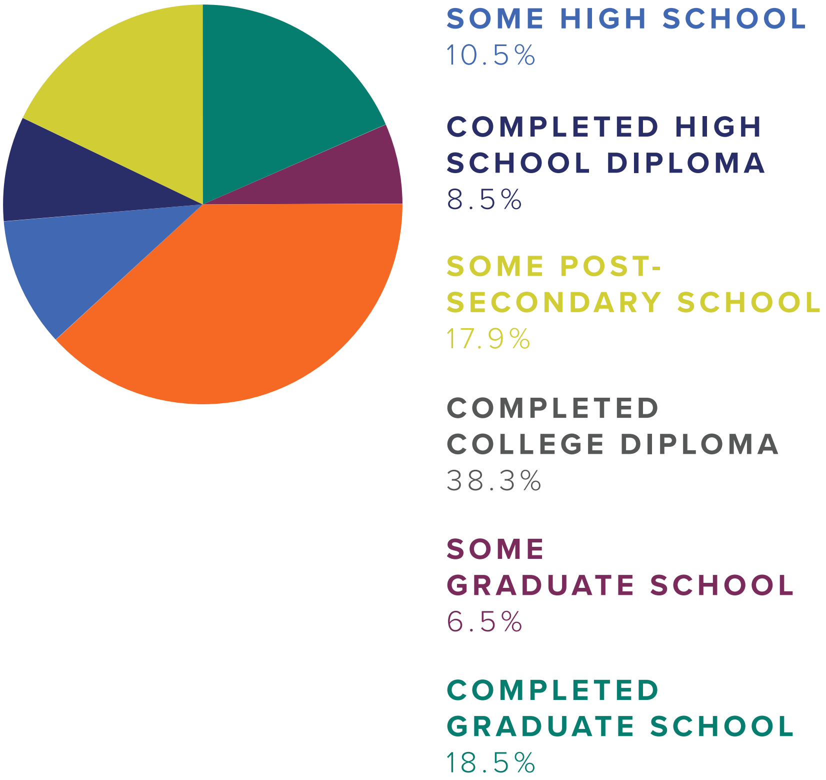
The Crowd by the Numbers

AGE

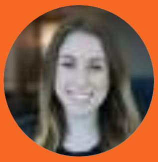


Nearly 72% of the hacker community are ages 18-29. They're young, ambitious and eager to develop their skills.

EDUCATION



More than 80% of hackers have completed some form of higher education, with 18% holding masters degrees. Only 18% have completed some form of high school.



HACKER SPOTLIGHT

Rachel Tobac

How did you get started in info-security?

I got my start in information security on the SECTF (Social Engineering Capture the Flag) stage at DEF CON where I got into a sound proof glass booth in front of 400 people and live hacked a real company over the phone. I was not involved in the info-sec field at all at the time -- my background is in neuroscience, human behavior, and user experience research -- but my husband went to DEF CON and called me the Friday night of the conference and told me I needed to buy a ticket to Vegas that night because he needed me to see the SECTF live hacking phone calls in the morning.

Do you have any female info-sec role models?

I do! I have a long list, some of which are: @kimzetter for her cybersecurity reporting and research, @keirstenbrager for her work and writing on helping women in info-sec get the pay and career they deserve, @tetrakazi for her phishing research, @hydens33k for her physical SE pen testing work, and so many others.

Why do you think there are so few women in info-security?

I believe the imbalance we see starts all the way back in middle school for many. I remember expressing interest in "InfoTech" in 6th grade only to be told "There's really only boys in that class, may I suggest HomeEc?" You've probably also heard the stat from HP that states that men apply for jobs when they have 60% of the qualifications, whereas woman historically apply when they meet 100%. This issue may affect women applying for jobs that they could succeed at within info-sec, as well.

What do you think is needed to change that?

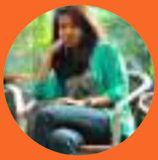
We need more women (and diverse women) in positions of leadership to ensure that we "send the elevator back down" for those who are next to advance within the field. To ensure women don't leave the field and continue to build their technical skills, they also need a strong sense of community, belonging, and support -- which we are working to create within WISP (Women in Security and Privacy, @wisporg). WISP works to step in for women who don't receive that support so that they can attend trainings, workshops, and conferences within the field to advance within their career.

What do you think is the biggest problem in info-sec at the moment?

I personally think that one of the biggest challenges in info-sec is the way we think about our users (the people who use our products). Many people say humans are our weakest link, but I actually see them as our first line of defense. Our people need training and technical controls to ensure they are set up to succeed.

Any advice for women just starting out in info-security?

The biggest piece of advice I have for women starting out is to jump right in and get told "no." Women are statistically less likely to jump in when they feel they don't meet the requirements. Don't self select out. Submit your presentation to the CFP, sign up for the CTF, join the meet up, speak up and raise other women up, make a Twitter if you like chatting with others, write that blog post. Let others tell you "no" rather than self selecting out.



HACKER SPOTLIGHT

Mehidia Afrin Tania

How did you get started in info-security?

For me entering the information security (info-sec) field was bit elusive, with mixed signals and conflicting information about what background or skill I need to start out with. My background was in computer science and engineering but I felt like i was in the middle of the sea no idea which direction I was going! After swimming for a few months in info-sec, I knew I was in the right direction. When I seriously started learning bug bounty at first it was self-taught but after 3 or 4 months, I was lucky enough to find a mentor. He is an active bug bounty hunter who let me in on tips and tricks of the trait; he gave me direction. It's been one and half years, I'm still learning from him and I am very grateful.

Do you have any female info-sec role models?

I can tell you that I am looking for more female info-sec role models because when you have role models or people you aspire to be like, your skill gets so much better! Consciously or subconsciously you want to reach their level of skill which is great for self-improvement. I do want to mention one name. She is **Rachel Tobac**. I follow her on Twitter and she is great!

Why do you think there are so few women in info-security?

The fact that there are so few women in cybersecurity is disappointing and I think there are a couple of different reasons for this. Clearly, women are not a homogeneous group, so the answer varies based on each individual, but I can say some general thoughts based on my own experience. I am from Bangladesh and we still face lots of challenges like we don't have any academic courses for cybersecurity. Because of this, I don't feel that women have a clear concept about this field, and obviously lack mentors, training and workshops.

What do you think is the biggest problem in info-sec at the moment?

It's not just a single problem! But when it comes to the most prevalent causes of breaches it could be users, devices, or access to applications. It could be Crime-as-a-service (CaaS) which will expand available tools and services. The internet of things (IoT), the supply chain will remain the weakest link in risk management.

Any advice for women just starting out in info-security?

Well, be patient, keep consistent and don't give up! Starting something new is always hard but through this journey, you will discover a better version of yourself.

HACKER SPOTLIGHT

Anonymous

How did you get started in info-security?

I was playing CTFs and wargames and such. In my time doing these CTFs, I heard about bug bounties and it sounded interesting—getting paid for what I like to do. I'm a developer by trade, so I basically taught myself how to hack. It helps to know how things work to break them.

Do you have any female info-sec role models?

Well I do appreciate there are some really good women in this field and they are inspiring. But I'm not really the type of person that looks for role models. I find inspiration everywhere, however I'm the type that forges my own path. Mostly focused on making myself successful.

Why do you think there are so few women in info-security?

I do feel like to be successful in this field you have to be quite strong, willing to do things on your own, and be aggressive—those are all male attributes. Women, as social creatures, we need support and community. There is a lack of awareness and support. It sometimes seems to be an old boys club. Some top ranked hackers get treated differently and their words mean a lot to the program owners. They have more influence and its hard to get a word in edgewise.

What do you think is needed to change that?

The more open it gets and the more resources and support are available, the more open women will be about joining info-sec. I think there is a lack of awareness that needs to be overcome.

Any advice for women just starting out in info-security?

Like with anything, just get out there and do it. No one is going to do it for you. You have to do it yourself. Start doing CTF and **wargames** to get your feet wet. They're fun and you meet a lot of cool people along the way. Get involved.

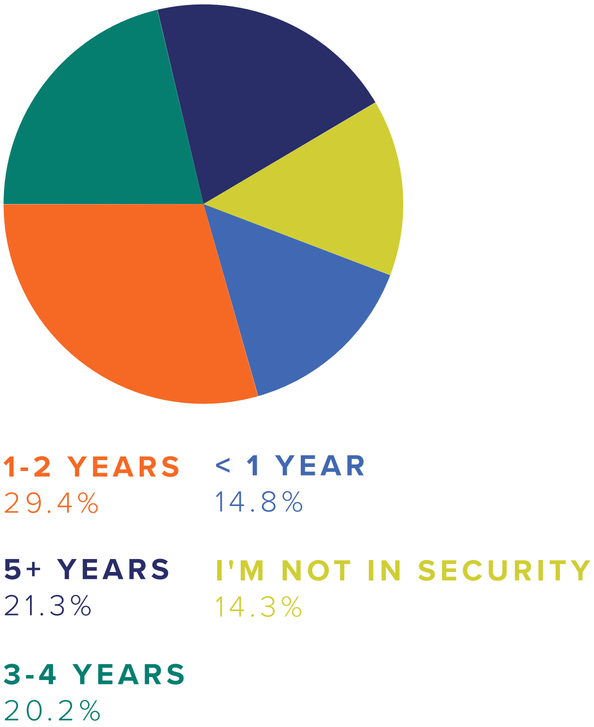
Any advice for bug bounty program owners?

My number one advice for program owners is to take every submission seriously, decrease response time and respect the hacker community. There needs to be a level of respect on both sides. The more professional a program owner is, the more likely I am to continue to participate in a program.

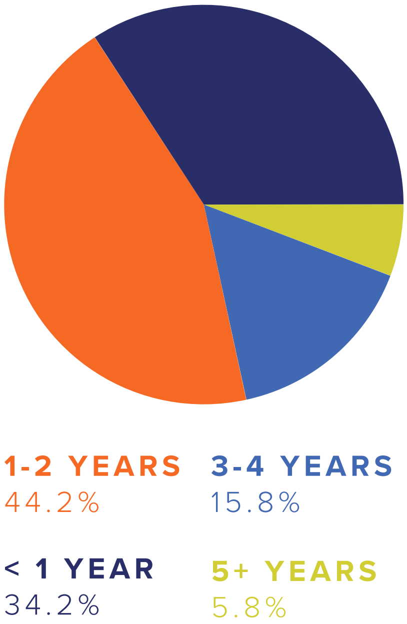
Crowd By the Numbers

In terms of bug hunting, more than 34% of hackers have been participating in crowdsourced security programs for less than a year, 44% for 1-2 years. New researchers have the ability to test on kudos-only programs in their initial stages, so they can gain experience with real websites and increase their ranks in the respective platforms leading to private invites.

SECURITY INDUSTRY EXPERIENCE



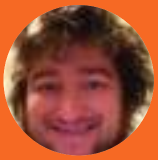
BUG HUNTING EXPERIENCE



HOW DID YOU LEARN HOW TO HACK?

43% of hackers learned how to hack via online resources and blogs and surprising 41% are self-taught.

Nearly 30% of hackers have 1-2 years of professional security experience and 41% of hackers have more than 3 years of experience. 43% of hackers learned how to hack via online resources and blogs and a surprising 41% are self-taught.



HACKER SPOTLIGHT

TodayIsNew

What motivates you to bug hunt?

Support my family.
Learn new skills.
Help secure the internet.

What programs do you tend to focus on?

Those with larger scopes, responsive programs, that like to engage throughout the entire process from submit, to resolution.

What was the most extravagant thing you bought with your earnings?

Bug hunting value lets me stay home with my 2 little girls (3 years and 2 months) and there's nothing more worthwhile then valuable time. Bug bounty earnings opens up that freedom for me. That and a minivan, we got a minivan that plays DVDs which makes life a little easier for the driver ;)

Any advice for bug hunters just starting out?

It's likely going to be challenging. There is a great amount of competition. If you can look where others are not looking you are likely to have more success. If your running the same tools against the same targets your likely to not find bugs, or those you find will be duplicates.

If you can pick some aspect of the online process that is interesting or not as widely used, and dig in deep, understand it more then others, your likely to find something.

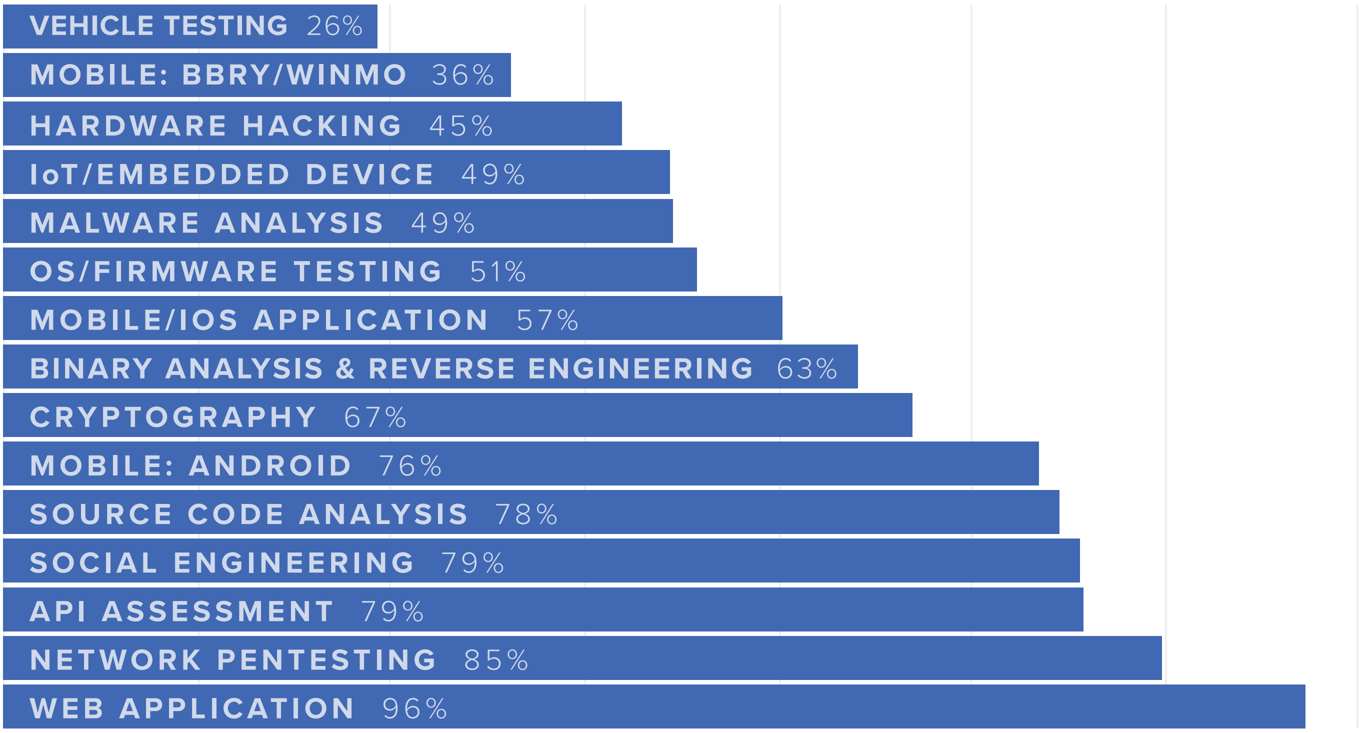
Any advice for program owners?

Patience. I know they must deal with a great number of challenging reports, from a variety of skilled reporters. When I first started it was a rough go, and I can remember a few programs or triggers kind words and direction that encouraged me to keep going.

Try to see the report from the Hackers point of view. They likely have good intentions. We're all in this unique group that gets to explore, and secure what is likely backing the future of our civilization. Often it feels its Hackers vs Programs, or Hackers vs Platforms. I'd like to put us all on the same side, (Hackers and Platforms and Programs) vs (an insecure world).

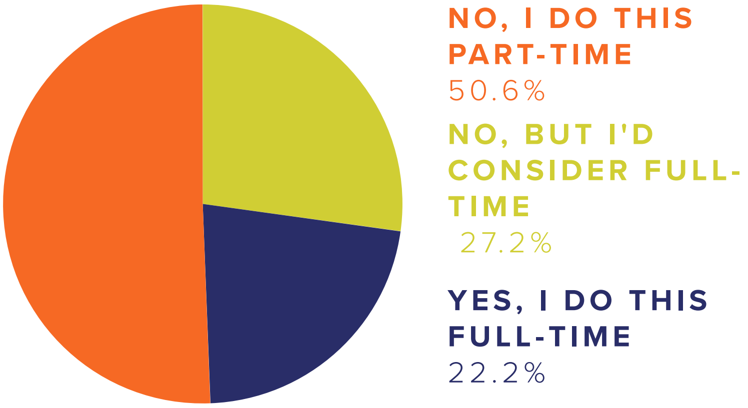
SKILLS & TARGET TYPES

The Crowd's skills continue to grow, across the board, specifically in vehicle and IoT hacking. We have a large and growing number of IoT bug bounty programs and we are seeing increased traction in submitted vulnerabilities.

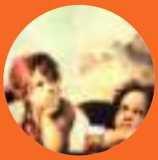


According to the **2018 State of Bug Bounty**, web is still the largest attack surface out there, which speaks to the amount of hackers who are skilled in that category, but others are gaining traction quickly with more user adoption and hacker sophistication. 7% was paid out for hardware (IoT) and 6% was paid out for API's.

FULL-TIME STATUS



More than 22% of hackers consider bug hunting their full-time profession. 77% of bug hunters have a full time profession outside of bug hunting.



HACKER SPOTLIGHT

0ang3el

What motivates you to bug hunt?

For me, bug bounties are an additional source of income. Also learning new things and playing with new technologies are very important to me. I get a rush of adrenaline when I find bugs with high severity and a feeling of deep satisfaction when I'm rewarded for them.

What programs do you tend to focus on?

I appreciate a friendly relationship from the program owner and quick response time. Also, bounty amount per issue or bounty pool is important. I tend to participate in paid programs and avoid kudos only programs. My current skills play important role in program selection. Now I mostly focus on web application programs. I have some experience with mobile and desktop applications. And I'm totally new to IoT, cryptocurrencies, hardware and car hacking.

What has made you so successful?

My pen testing experience and earning OSCP certification helped me a lot to develop a hacker's mindset. I was also a full-time developer in the past, then worked closely with developers in an appsec engineering role. Now I'm a security researcher at software company. This background gave me understanding of the mindset of a developer and helps much in bug hunting.

I read a lot every day and learn via twitter, reddit, slack and telegram bug bounty channels, and recordings of talks from security conferences. From these sources I know about new techniques, tricks and vulnerabilities. I try to understand them, and research how I can apply them during bug hunting.

There are well-known techniques and vulnerabilities used by many bug hunters, like subdomain takeovers, searching secrets on github, searching for files with sensitive information mistakenly exposed on company web servers, image and video processing issues, open redirects and CRLF injections. I tend to find my niche and look for less known things or find new vulnerabilities and techniques by myself. This tactic increases my success and helps to avoid duplicates.

I always try to understand the application that I'm testing as deep as I can. This helps in finding bugs with higher severity and avoid duplicates.

What was the most extravagant thing you bought with your earnings?

A new car. Bounties I earn are enough for life expenses, traveling, and new electronic gadgets.

Any advice for bug hunters just starting out?

Don't lose courage if you struggle at first. Develop positive thinking, learn new things, try harder. Good bugs and bounties surely will come with the time and experience. Don't stop.

Find your unique approach. Read as much as you can, research and apply your knowledge.

Any advice for program owners?

Define clear rules in program brief and SLAs, be clear and responsive to researchers.

Motivations

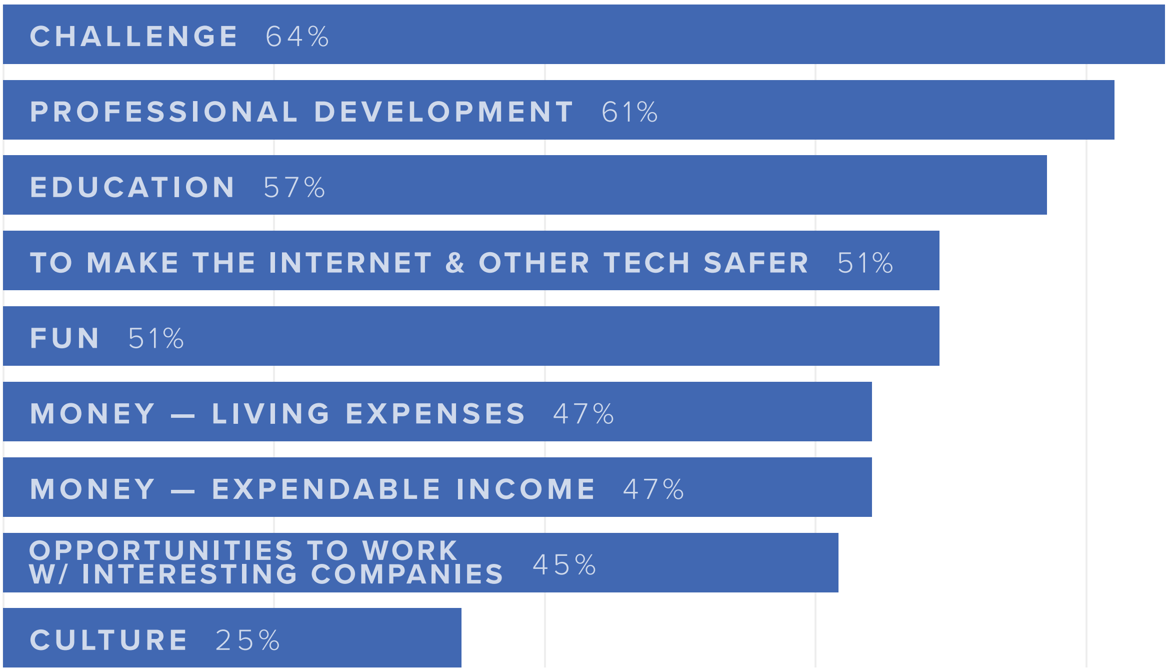
CAREER ASPIRATIONS

Nearly 32% of bug hunters aspire to be full time bug hunters. They prefer to operate autonomously and better their skills through whitehat hacking and exploration. In some cases, bug hunters believe they are making more of an impact than if they were employed in a 9-5 job.

In an interview with **MIT Tech Review**, Bugcrowd ambassador and bug hunter Evan Ricafort stated, “he enjoys the impact his work has.” While he says he’d entertain the right offer for a full-time cybersecurity position, he feels he can make the biggest difference where he is now: fighting vulnerabilities in the background.

A large portion of the hacker community are penetration testers by day, and many others aspire to become pen testers. 15% of hackers aspire to be top security engineers at large tech companies. 6%

WHY DO YOU BUG HUNT?



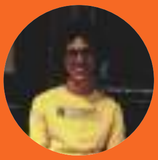
The top 3 reasons for participating in crowdsourced security and whitehat hacking are, respectively:

The Challenge

Professional Development

Education

It's the challenge, perhaps even more than the money, that keeps bringing people back to bug hunting. While most do bug hunting on top of a regular 9-5 job or schooling, bug hunting allows them to chase down bugs without reporting to a boss. They'd rather be on their own. Professional development and education are added benefits of bug hunting. You gain real-world application security experience and learn to think outside of the box.



HACKER SPOTLIGHT

Nijagaw

What motivates you to bug hunt?

The excitement of the hunt. I work as a pen tester and scopes are generally a bit limited. When you are done with the job, you provide a report and that's it. End of the game. With bug bounties the game never ends. I enjoy the hunt.

The challenge. With bug bounties you have plenty of competition and scopes can be massive.

The rewards. Who wouldn't like to make $20K in a single night?

The community. I've met a lot of great like-minded people thanks to the bug bounty community.

The learning process. Bug bounty hunting and pen testing are slightly different. With bug bounties you need to focus on speed to beat the competition, you have to learn new techniques that you wouldn't necessarily use during a pen test. You need to learn how to manage your time as there are too many bounty programs and so little time. Many programs also mean that your possibilities to learn increase.

What programs do you tend to focus on?

I love programs with huge scopes (*.domain.com). I like to go back to them a few weeks/months later and start looking at new subdomains/endpoints.

I like responsive programs. If I see that a program owner is not responsive, I will avoid that program in the future.

I like fair programs where owners are not just trying to get a cheap pen test. If certain rewards are indicated for certain vulnerabilities, program owners should be honest about them.

What has made you so successful?

Working hard and thinking outside the box.

Speed at finding vulnerabilities.

Persistence. You can spend a week or two not finding some cool vulnerabilities. Not giving up is fundamental.

What was the most extravagant thing you bought with your earnings?

An HTC Vive for VR and a car.

Any advice for bug hunters just starting out?

Don't give up. It is difficult at first (the first few months).

Focus on learning not on the money. Money will come only if you learn.

Make your own virtual environment. Install vulnerable software and hack it. There are many ready-made vulnerable machines online.

Learn from your mistakes, learn from others. There are plenty of available resources online.

Ask questions, but Google for an answer first.

Don't waste people's time because you are being lazy.

Work hard.

Be humble, don't be an ass to people.

Respect the rules.

Write a diary of what you have learned day by day. You will see that even if you don't find epic vulnerabilities, you are still learning— lot.

Any advice for program owners?

Be responsive with loyal researchers.

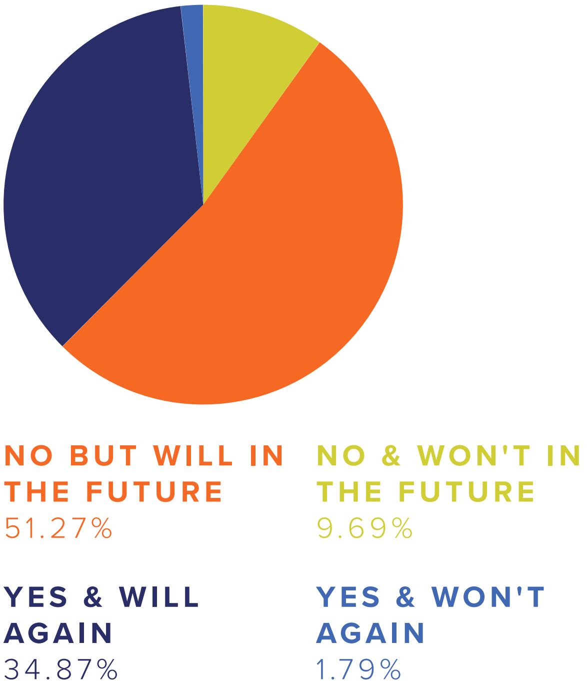
Provide credentials. Sites protected by a login page are not necessarily secure.

Start with a small scope and increase it after a while to include more of your assets. The end goal is to make your assets safe and researchers love new targets.

Evaluate vulnerabilities at their true risk/value, no matter how easy the fix is for you.

The higher the rewards, the more motivating the hunt is.

HAVE YOU PREVIOUSLY COLLABORATED?



Bug Bashes

Bug Bashes are one- or two-day events that bring together security researchers and companies to compete to find priority vulnerabilities, as well as foster positive, real-time engagement that can benefit both parties.

Bug Bashes attract and engage some of the best researchers in the world. Through these hackathon events, companies are able to engage and interact with top security talent, excite them about their bug bounty program, and in return receive high-quality security vulnerabilities.

Internal engineering teams and Bugcrowd security researchers rarely get the opportunity to directly interact, but are vital to each other's success. Bugcrowd Bug Bash events bring these two groups together in one room, creating a environment where engineers can learn how to make their code more secure and researchers get a better understanding of the products they are testing.

> “I would definitely recommend a Bug Bash event for any organization looking to squash a TON of bugs in a short amount of time.” **@cha5m**

> “The Bug Bash gave me a chance to hack with real time access to program engineers, letting me dive deeper into the targets and produce findings that I would never have otherwise discovered.” **@cboan**

The Elite Crowd

The Bugcrowd Elite Crowd is a group identified within Bugcrowd's wider hacker community comprised of the top researchers as measured in two key areas:

Skill

A standard of high-impact submissions, averaging only high and critical submissions across a range of specific attack surface areas.

Trust

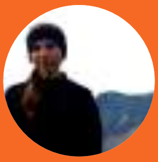
Proven trust through ID verification and success working on private programs for top customers.

Proprietary algorithm for matching researchers to programs, combined with extensive verification checks, this Elite group is the largest crowd of skilled and trusted security researchers in the world.

Anyone can sign up to become a Bugcrowd hacker and participate in public bug bounty programs. As bug hunters submit bugs, climb the ranks within the community, and prove their trustworthiness they may gain access to private bug bounties and Next Gen Pen Test programs. Bugcrowd researchers are vetted and measured in four areas–activity, quality, impact and trust. Only the top performers who have proven their skill and trustworthiness receive invitations to private programs.

What makes someone Elite versus a dedicated hacker isn't that they have different career aspirations or reasons for bug hunting. It's the hours spent and skill specializations and earnings. Relationships are one of the biggest motivations for the Elite Crowd. **Researchers who have a good experience on a program are 10 times more likely to go back to the program.**

More than a quarter of the Elite Crowd spends 6-10 hours per week bug hunting. More than 15% of the Elite Crowd spends 11-20 hours, and nearly 10% spends 21-30 hours per week.



HACKER SPOTLIGHT

Sophia d'Antoine

How did you get started in info-security?

I got started in security doing CTFs. When I was going through schooling, I wasn't really interested in security or computer science. And to be honest, security and exploitation wasn't something offered as a class. But when I found CTFs, I got addicted.

Why do you think there are so few women in info-security?

Info-security is a specialization, and in specialized fields, there are less women in general. And since there are less women, I could see women being intimidated.

What do you think is needed to change that?

I think if we applied more structure and actual educational resources toward info-sec, more women would get involved. Right now, I think that the number of women is growing, but they are less willing to jump right in. Security has gotten much bigger in the last five years. The structure and education really matters. Getting women exposed to and aware of info-sec at younger age will be key.

What do you think is the biggest problem in info-sec at the moment?

The community in info-sec tends to be an echo chamber. That is a direct result of still being small and immature. It's really community-driven. This is either a great opportunity or a big burden. There are superstars in the industry that have the power to influence, and that is not always a good thing.

Any advice for women just starting out in info-security?

Don't rely on other people leading you to do things. If you want answers, go out and find them yourself. Don't be afraid.

Any advice for bug bounty program owners?

Open up your scope.

Be very explicit in what is considered bugs or not.

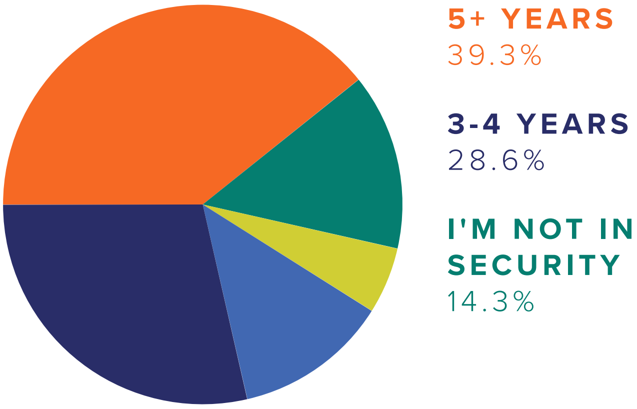
Clarity is king.

MVP

Bugcrowd's MVP program is designed to recognize our exemplary Crowd's consistency, with yearly qualification open to all hackers. MVP is essentially a year long challenge that our researchers engage in to win bonus rewards.

To qualify for MVP status, hackers would have had to maintain a minimum average submission acceptance rate of 80% and an average submission priority between 1.0 and 2.99 on all submissions between July 1, 2017 and June 30, 2018, had a minimum of 10 qualifying (non-duplicate) submissions and no significant enforcement infractions in the prior 6 months of the qualification date.

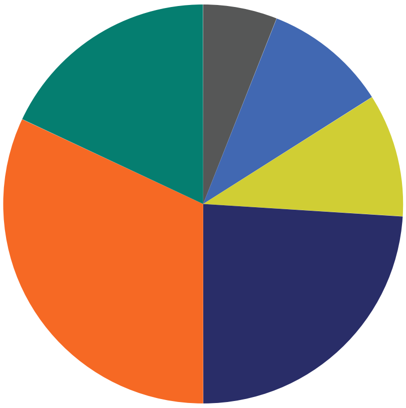
SECURITY INDUSTRY EXPERIENCE



Interestingly, the MVPs have double the security experience than the general Crowd. Nearly 40% of MVPs have more than 5 years of experience.

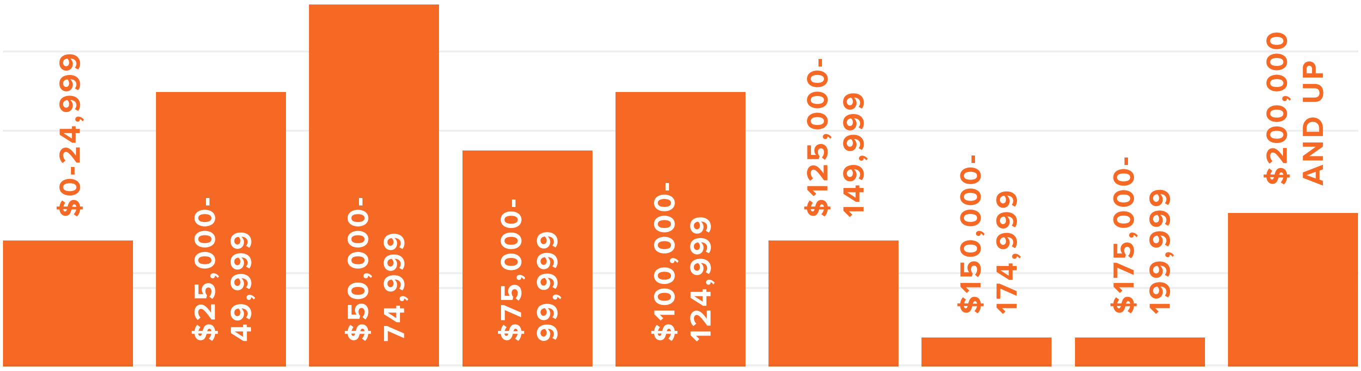
MVPs spend a lot of time bug hunting. 24% of MVPs spend 11-20 hours per week and 26% spend more than 20 hours per week bug hunting. 6% spend more than 40 hours per week.

HOURS SPENT BUG HUNTING PER WEEK



MVPs are going to have higher levels of specialization. They are going to qualify for programs that are more challenging to match. Harder skillsets, higher level of trust. Since they have more security experience under their belt, they are looking for higher price tag in order to consider bug hunting full-time. The majority of MVPs would need to make double ($50-75K) that of the general Crowd to bug hunt full time.

HOW MUCH WOULD YOU NEED TO MAKE TO BUG HUNT FULL-TIME?



HACKER SPOTLIGHT

Phillip Wylie

How long have you been in the industry and how did you get started in security?

I got into security after 6.5 years of working as a sysadmin. I moved into network security in 2004 and then application security in 2005. In 2012 I started my pen testing career and spent my first 5 years in consulting. I got into bug bounties as a way to further improve my hacking skills through some of the unique techniques used by bug bounty hunters.

What advice would you give to someone who is starting out as a beginner?

Learn the underlying technologies of systems, networks, applications and hardware first. Then move on to hacking. It's easier to break it if you know how to build it. If you get command line access to a Linux server and you don't know the operating system you are not going to get very far. A lot of people want to start out hacking, but you are going to have a difficult time if you don't understand the underlying technology.

Tell us about your favorite pen testing tools & why you use them.

Burp Suite, SQLmap, nmap and Nikto. Burp Suite is a have to have tool for web app pen testing and I like using the CO2 plugin which makes working between Burp and SQLmap more seamless. Nmap is a great for discovering open ports and identifying services running on target systems, as well as the NSE scripts that enhance nmap's functionality. Nikto is an often overlooked tool for fingerprinting web servers and frameworks, and vulnerabilities. I've found default creds on systems that Nessus missed.

Do you have a hacking tip for others that you can share?

You need to learn how to manually perform hacking techniques and not be dependent on tools to automate attacks and vulnerability testing. It will help you better understand and use the tools effectively.

How have bug bounties impacted your life?

Bug bounties have impacted my life by teaching me skills that I didn't know of doing traditional pen testing. Bug bounty hunters have some really unique techniques that are helpful in pen tests.

What do you do you like to do in your free time, outside of bug bounties?

I like to spend time with my family and friends in my free time as well as watch movies. Although it is technically work, I teach ethical hacking at a community college. I like to attend security and hacker meetings as well as I run my own meetup called The Pwn School Project. I really enjoy being involved in the security and hacking community.