## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVERVIEW</td>
<td>1</td>
</tr>
<tr>
<td>KEY FINDINGS</td>
<td>2</td>
</tr>
<tr>
<td>THE CROWD “BY THE NUMBERS”</td>
<td>3</td>
</tr>
<tr>
<td>AGE, EDUCATION, PROFESSION</td>
<td>4</td>
</tr>
<tr>
<td>EXPERTISE AND SKILL SETS</td>
<td>5</td>
</tr>
<tr>
<td>GEOGRAPHY</td>
<td>7</td>
</tr>
<tr>
<td>MOTIVATIONS</td>
<td>8</td>
</tr>
<tr>
<td>SECURITY RESEARCHER PROFILES</td>
<td>11</td>
</tr>
<tr>
<td>THE KNOWLEDGE SEEKER</td>
<td>11</td>
</tr>
<tr>
<td>HOBBYISTS</td>
<td>12</td>
</tr>
<tr>
<td>FULL-TIMERS</td>
<td>12</td>
</tr>
<tr>
<td>VIRTUOSOS</td>
<td>13</td>
</tr>
<tr>
<td>PROTECTORS</td>
<td>13</td>
</tr>
<tr>
<td>WHY IT MATTERS</td>
<td>14</td>
</tr>
</tbody>
</table>
OVERVIEW

During the past year alone, we have witnessed a number of devastating cyberattacks from the massive Equifax breach to the seemingly never ending Yahoo! breach. Be it stolen healthcare records, voter files, credit card information, or social security numbers, today nearly every American has been impacted by the loss of personally identifiable information (PII) data. And the threat continues to rise.

Though “black hat hackers” are responsible for each of these attacks, these individuals represent a small segment of a much larger community. White hat hackers, bug hunters, or the like, are the good guys, security researchers that approach breaking into code like an adversary. These allies are fueled by a desire to help combat cyber attacks using their technical skills and expertise, rather than malicious intention. Central to our mission here at Bugcrowd is cultivating this community.

The 65,000+ members that make up our community of bug hunters, or “the Crowd,” is a global group of talented individuals, with diverse backgrounds, technical skills, and expertise. Using data collected from our 2017 survey of the “Crowd,” the 2nd annual Inside the Mind of a Hacker report sheds light on the makeup of the bug hunting community and gain insight and understanding into who they are as well as what motivates them.

Using the data collected, this report will:

• Provide an overview of the Bugcrowd security researcher community, their geographic distribution, skill sets, and growth over time
• Identify 5 distinct bug hunter personas and what they are motivated by
• Explore program variables that help tap into those motivations

“BY ADDING THE POWER OF THE TALENTED RESEARCHER COMMUNITY TO OUR PRODUCT SECURITY PROGRAM, WE’VE LEARNED A LOT ABOUT HOW PEOPLE OUTSIDE THE COMPANY THINK ABOUT OUR PRODUCTS, ADDITIONAL SCENARIOS WHERE PRODUCTS CAN BE AT RISK AND WHAT ELSE WE COULD DO TO PROTECT OUR PRODUCTS. WE’VE USED THIS INFORMATION TO PUT A SHARPER FOCUS ON THE AREAS OF GREATEST RISK, WHICH HAS BEEN INVALUABLE TO US AS WE SCALE.”

— COLEEN COOLIDGE
Sr. Director, Information Security
The Crowd continues to grow. Since last year’s report, the Crowd has grown by 71% to 65,000+ members, represented by more than 100 countries around the world.

**KEY FINDINGS**

Bugcrowd security researchers have expertise in many technologies—providing direct access to hard-to-find resources and skillsets.

- **41%** of bug hunters have been participating in bug bounties for 1-2 years, up from only 20% last year.
- **14%** of respondents said they are not in the security industry at all, holding broader IT positions such as software engineers, developers or system administrators.
- **46%** have 3+ years of professional experience working in the security industry.

**Bug hunters are young, ambitious, and always looking to expand their knowledge and build on their skill set through the challenge of the hunt.**

- **71%** of bug hunters are 18-29 years old, with 82% having completed some form of higher education (i.e., college, university or graduate).

**No. 1**

When asked why they participate in bug hunting, bug hunters ranked “the challenge” as a top source or motivation.

**Top 5**

- top skillsets include web application testing, web API assessment, network pentesting, social engineering, and source code analysis.
- **22%** of respondents said they are not in the security industry at all, holding broader IT positions such as software engineers, developers or system administrators.
- **46%** have 3+ years of professional experience working in the security industry.

**When asked what best describes their profession, 22% of bug hunters responded “Penetration Tester,” 18% responded “Security Consultant,” and 15% responded “Student.”**

**62%** reinvest earnings from bug hunting back into their craft, spending it on security tools and training.

**27%** When asked about their career aspirations, 27% of respondents hope to become a full-time bug hunter.

**14%** have 3+ years of professional experience working in the security industry.
According to our 2017 State of Bug Bounty Report, bug bounty programs have become much more accessible in the past year. No longer limited to large technology companies, the sheer number of programs available to “hack on” have proven an attractive target for everyone from the most experienced security researcher to the student novice.

Over the past year, we have continued to cultivate and invest in our security researcher community, watching it grow into the vibrant, self-educating group of talented and passionate experts that it is today.
AGE, EDUCATION, PROFESSION

71% of bug hunters are between 18-29 years old, up from 60% last year, indicating more hackers are getting an earlier start.

Despite popular belief, most bug hunters are highly educated. 82% of bug hunters have completed some form of higher education, with 16% holding a master’s degree or higher.

22% of bug hunters identify as penetration testers, 18% as security consultants, and 15% as students. 19% consider bug hunting their primary source of income.

18 to 29 71%
19 to 44 20%
> 45 9%

EDUCATION

Completely College 41%
Some Post-Secondary 18%
Completed Graduate 16%
Some Graduate School 6%
Completed High School 9%
Some High School 9%
Completed High School 9%

PROFESSION

Penetration Tester 22%
Security Consultant 18%
Student 15%
Security Engineer 11%
Other 6%
Software Engineer 9%
Bug Hunter 21%
EXPERTISE & SKILL SETS

41% of bug hunters have been participating in bug bounties for 1-2 years, up from just 20% last year. More hackers are seeing the value of getting involved and staying involved.

46% of bug hunters have 3+ years of professional experience working in the security industry.

14% have no experience in the security industry (outside of bug hunting), and instead hold broader IT positions such as software engineers, developers or system administrators.
• When asked which technologies they have the most skill with, 82% of bug hunters rated their web application testing knowledge as intermediate or advanced.

• Nearly 60% felt they have intermediate or advanced knowledge of web API assessment.

• Nearly 41% said they have intermediate or advanced knowledge of Android mobile app assessment.

• 23% said they have intermediate or advanced knowledge of IoT consumer appliance testing, up from 15% last year.

• 53% felt they have intermediate or advanced knowledge of social engineering.
This year the U.S. surpassed India in the number of security researchers. U.S. is 27%, India is 23%, GB is 6%.
MOTIVATIONS

WHY DO YOU PARTICIPATE IN BUG BOUNTIES?

When asked why they participate in bug hunting, bug hunters ranked “the challenge” as a top source or motivation.

36%
indicated that professional development drives their participation in bug bounty programs.

HOW DO YOU SPEND YOUR BUG BOUNTY EARNINGS?

62%
reinvest earnings from bug hunting back into their craft, spending it on security tools and development.
HOW DO YOU CHOOSE A BUG BOUNTY PROGRAM?

- Broad Scope: 45.35%
- High Maximum Reward: 32.85%
- High Minimum Reward: 33.03%
- Challenging Targets: 33.04%
- Unique Application: 28.01%
- High Profile Company: 27.83%
- Good Feedback: 27.88%
- High Potential to Find Bugs: 42.12%
- Untouched Program: 31.98%

“45% of bug hunters gravitate toward bug bounty programs with a broad scope, followed by high potential to find bugs (41%), indicating bug hunters are very results driven.”

—— THIBAULT CANDEBAT
Information Security Manager

OUR PRIVATE BUG BOUNTY PROGRAM ALLOWED US TO TAP INTO THE CREATIVITY AND ABILITIES OF HUNDREDS OF RESEARCHERS TO FIND AND REPORT THE MOST COMPLEX BUGS—THE ONES APPLICATION SCANNERS JUST CAN’T UNCOVER. NOW WE’RE EXPANDING OUR PROGRAM FOR ACCESS TO A BIGGER POOL OF RESEARCHERS TO IMPROVE OUR ABILITY TO FIND AND FIX VULNERABILITIES.

—— THIBAULT CANDEBAT
Information Security Manager

INTERCOM
WHY PROGRAM MANAGEMENT MATTERS

We asked the Bugcrowd researchers who consistently contribute to our security programs, “what keeps them coming back?” They responded,

1) clear and accurate scope
2) response time and clear communications
3) correct bounty amounts

A CLEAR AND ACCURATE SCOPE

Providing clarity about exactly what is and is not in scope creates a better experience for both the bug hunters and customer. Hackers know exactly what to look for, and customers keep focus on the areas that matter most.

How do we do it? Every single Bugcrowd customer goes through a comprehensive onboarding process, forming a close partnership between teams to align on program goals, target areas, and expectations.

RESPONSE TIME AND CLEAR COMMUNICATIONS

After hackers have devoted their time and effort into submitting a vulnerability, the last thing they want is a long delay in response. Providing timely feedback and clear communication speeds up the bounty payout for hackers and shortens the time to remediation for customers. On average, all submissions receive an initial response in 1.2 days.

How do we do it? Bugcrowd’s Researcher Operations and Security Operations teams provide industry-leading support for both hackers and customers. Our in-house teams provide accurate and quick assessments throughout the entire vulnerability submission cycle.

CORRECT BOUNTY REWARDS

Hackers want to know approximately how much a bug is worth before they start investigating it. Reducing variation on payout amounts allows researchers to appropriately allocate their time, and helps customers budget correctly for their programs.

How do we do it? Bugcrowd’s Vulnerability Rating Taxonomy offers a systematized structure for recommended payouts, based on criticality. Every vulnerability submission is automatically tagged with a recommended “priority” and a corresponding payout amount. All payouts are managed through Bugcrowd for easy execution.

“WITH BUGCROWD, ATLASSIAN’S SECURITY TEAM ADDS NEARLY 60,000 EXTERNAL CYBERSECURITY RESEARCHERS. THIS HIGHLY CAPABLE COMMUNITY IS CONSTANTLY TESTING OUR PRODUCTS, USING WELL-DEFINED GUIDELINES AND A SAFE TESTING GROUND TO PERFORM THEIR RESEARCH.

—MATTHEW HART
Security Engineer

ATLASSIAN

bugcrowd
In last year’s Inside the Mind of a Hacker, we found five very distinct groups of security researchers: Knowledge-Seekers, Hobbyists, Full-Timers, Virtuosos and Protectors. This year, we built on those profiles, digging deeper into their motivations.

**SECURITY RESEARCHER PROFILES**

**KNOWLEDGE-SEEKERS**

Knowledge-Seekers are excited about getting more involved with bug hunting. Most of these hunters are new to the bug bounty scene and have been at it for less than two years. 63% reported that they invest earnings from bug hunting back into professional development and security tools.

**MOTIVATORS:** Education, challenge, fun

**AGE:** 69% are 18-29, making them one of the younger bug hunting groups.

**EDUCATION:** Nearly 56% have either a bachelor’s or advanced degree, with 23% of these researchers still identifying as students.

**YEARS OF EXPERIENCE:** This group is largely new to bug bounty hunting, with nearly 84% having less than two years experience and 67% with less than a year.

**CAREER ASPIRATIONS:** They are interested in security: 29% aspire to be penetration testers, and 27% aspire to be full-time bug hunters.

*WHAT EXCITES ME IS THE PROCESS OF LEARNING, NOT THE OUTCOME. I FEEL PARTICIPATING IN EVERY BUG BOUNTY PROGRAM TEACHES ME A SOMETHING NEW AND FUELS MY DESIRE TO KEEP GOING. PLUS, I LOVE THAT MOMENT WHEN I GET AN EMAIL FROM BUGCROWD LETTING ME KNOW A BUG HAS BEEN TRIAGED FEELS VERY REWARDING.*

—MICO
HOBBYISTS

Motivated by expendable income and fun, these bug hunters spend their “free-time” hunting for bugs. This group has the most experience bug hunting, 65% have been participating for more than a year.

MOTIVATORS: Expendable income and fun
AGE: 66% of hobbyists are 18-29, with the next biggest group (23%) 30-44. A whopping 9% are under the age of 18.
EDUCATION: 34% use it for tuition, highlighting the fact that many hobbyists are students. 82% have completed some college, and the majority of that group (79%) have a bachelor’s degree or more.
YEARS OF EXPERIENCE: On average hobbyists have a good amount of experience bug hunting: 65% have been participating for more than a year, with 26% doing it for 3-5 years. This group has a strong background in infosec (70% have been in the security industry for at least a year and 52% for at least 3).
CAREER ASPIRATIONS: And while they are hobbyists, 34% hope to become full time bug hunters in the future. So what’s preventing them from doing so? Possibly income. The average required income to move over to full time bug hunting is $57,796, with 17% requiring $0-$24,999, 22% $25,000-$49,999 and 21% $50,000-$74,999. 29% require more than $100K.

FULL-TIMERS

The Full-Timers use bug bounties as their main source of income, with 43% spending 21+ hours hunting bugs per week. 71% of respondents plan to do even more bug hunting than they currently do in the next 6 months. With the money they make bug hunting, they spend it paying bills and living expenses. Just like most full time jobs.

Not surprisingly, Full-Timers are a highly-skilled and seasoned group with nearly half (47%) having 3+ years professional experience working in the security industry.

MOTIVATORS: Primary source of income, challenge
YEARS IN BUG HUNTING: 72% have been hunting bugs for 1+ years.
TIME SPENT HUNTING: This group participates in bug bounties more than other groups, typically 10 - 30 hours.
BOUNTY SELECTION CRITERIA: Challenging targets and positive feedback from researcher community.

―TODAYISNEW

―SYNTAXERROR

BUG BOUNTIES GIVE ME THE OPPORTUNITY TO WORK WITH SOME GREAT COMPANIES, LEARN ABOUT THEIR BUSINESS MODELS, PRODUCTS AND TECHNOLOGIES. ALONG WITH MAKING THE WEB MORE SECURE, I GET TO LEARN SOMETHING NEW EVERYDAY.

―SYNTAXERROR

TWO YEARS AGO MY DAUGHTER WAS BORN. BEING ABLE TO SPEND MY DAYS WITH HER AND WORK FROM HOME BUG HUNTING WAS A PERFECT MATCH.

―TODAYISNEW
VIRTUOSOS

Virtuosos have worked in the security industry longer than anyone, primarily motivated by the challenge of hunting. 52% of this group chooses which bug bounties they want to participate in based on difficulty. On top of that, they are always trying to better their craft. Nearly 70% of all Virtuosos spend their bug hunting earnings to purchase security tools and professional development. Virtuosos want to be part of the security elite.

**MOTIVATORS:** Challenge, education, skill retention

**AGE:** The vast majority (70%) of Virtuosos are 18-29, with the next biggest group (30-44 years old) dropping down to 23%. Only 1% are above the age of 45-years-old.

**EDUCATION:** Virtuosos are highly-educated. 60% have completed college diploma or received a university degree, and 15% have completed their master’s degree.

**YEARS OF EXPERIENCE:** While this group is new to bug hunting, they are well-versed in the security industry. 55% of Virtuosos have been in the security industry for more than 3 years, 29% have been in security for more than 5 years.

**CAREER ASPIRATIONS:** When asked about their career aspirations, the majority want to be top security engineer at highly esteemed company. They are using bug bounties to perfect their craft and get ahead of their peers.

---

PROTECTORS

Proectors participate in bug bounties to make the internet (and other technologies) safer. This altruistic approach differentiates themselves from others, with many aspiring to be full-time bug hunters and a significant percent of Protectors donating their bounties to charity. They are a young but highly-educated group, who are attracted to bug bounty programs that have a broad scope, challenging targets, and a high potential to find a valid bug.

**MOTIVATORS:** Making the internet safe

**AGE:** 74% are between the ages of 18-29; 19% are between the ages of 30-44.

**EDUCATION:** 66% have started or completed secondary education (College / university)

**YEARS OF EXPERIENCE:** Nearly half (48%) have been in security for 3+ years, with 59% having participated in bug bounties for more than one year.

**CAREER ASPIRATIONS:** 27% aspire to be full-time bug hunters; 57% would need $50K or more to become a full-time bug hunter.

**BOUNTY SELECTION CRITERIA:** Not deterred by programs that have been running for awhile, as long as they have a broad scope, challenging targets, and a high potential to find a valid bug.
WHY IT MATTERS

The power of the crowd lies in its depth and breadth. In the first two weeks of a bug bounty program, the crowd finds an average of 5 critical vulnerabilities—a results-driven model proven to deliver a 7x increase in critical findings over traditional tests.

As the bug bounty ecosystem matures, the goal is to tap into each of the researcher personas, as they each bring his or her own perspective and expertise to the table. That is the true benefit of crowdsourced security testing. However, we know it’s often difficult to gather the right mix of researchers with the right mix of targets to build a truly successful program. That is where our managed services and team of experts come in.

Bugcrowd’s Researcher Operations and Security Operations teams ensure you get the right researchers who understand your technology stack and can quickly identify new attack surfaces for vulnerabilities.

Our Researcher Operations team prides itself on building impactful relationships with high performing bug hunters, through incentive programs, gamification, and constant communication to retain the highest quality researchers, and provides the tools and education needed to enable new bug hunters to get started on our programs. The team handles any incidents and manages direct communication, facilitating healthy relationships.

At the same time, our Security Operations team works one-on-one with customers, determining severity and reproducibility of each bug found by our researcher community. This vetting and triaging process enriches the vulnerability data to ensure submissions are actionable and highlighted depending on the severity of the bug.

“WITH BUGCROWD, WE ARE ABLE TO EXTEND OUR SECURITY TEAM WITH THOUSANDS OF RESEARCHERS WITH SKILLS AND TIME NOT AVAILABLE TO US INTERNALLY. WE GET BETTER RESULTS WITH THE RIGHT, TRUSTED RESEARCHERS FOR OUR PROGRAM.”

—RON WHITE
VP of Engineering

ibotta
A large, growing crowd naturally translates to a bigger pool of talent with varying backgrounds, skill sets, and perspectives. Some researchers have an extensive breadth of skills and expertise, while others have mastery in a few specialized areas. This collective creativity contributes to the wide range of vulnerabilities found in bug bounty programs.

At Bugcrowd, we see it as our responsibility to understand and support our community of researchers, and it is our hope that by connecting this diverse group to a market that desperately needs them we can help grow the community, providing opportunities for security researchers around the globe, while ultimately making the Internet safer.

While we don’t see this as an all-inclusive report, we do believe this a unique look at bug hunters, what motivates them, and the factors in play when they choose bug bounty programs to work on. As the Crowd continues to grow and the security industry continues to evolve and change around us, we expect to see even more diversity and perhaps new personas with new motivation and reasons for bug hunting.

If you’re interested in learning more about our researcher community, check out our “Meet the Crowd” web page.