7 BUG BOUNTY MYTHS, BUSTED

bugcrowd

Utilizing the power of the crowd through bug bounty programs

Attackers only need to exploit one security flaw to compromise an organization, while organizations must be able to defend against all potential flaws. Security teams are resource constrained; hackers aren't.

Bug bounties harness the power of a crowd to augment your team's resources, finding more critical security vulnerabilities missed by traditional security assessment methods.

Why is the bug bounty model so powerful?

More Eyes

Bug bounties multiply the potential manpower of traditional security assessment methods exponentially, increasing the odds of finding more valid vulnerabilities at any given time.

Having such a large testing pool gets you as close to 24/7 human testing coverage as you can get.

Collective Creativity

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. Their creativity contributes to the wide range of vulnerabilities found in bug bounty programs.

Better Results

Scanners are extremely limited -they are only able to detect what they have been programmed to recognize. Penetration testers are extremely limited by the knowledge of the few engaged testers and their specific skills.

By nature, crowdsourcing doesn't have those same limitations. More eyes + collective creativity = better results.

Better ROI

Bug bounties utilize a pay for results model, ensuring that only valid results are paid rather than effort.

With traditional testing methods, companies typically pay for the effort required to test their applications, regardless of what results are found.

Busting 7 common bug bounty myths

The bug bounty model, although incredibly powerful, is still continuing to gain traction and overcome misconceptions.

In this guide we will address seven of the most common myths we've heard surrounding the bug bounty model.

1. All bug bounty programs are 'public'
2. Only tech companies run bug bounties
3. Running a bounty program is too risky
4. Bug bounties don't attract talented testers
5. They don't yield high-value results
6. They're too costly and hard to budget for
7. Bounty programs are too hard to manage

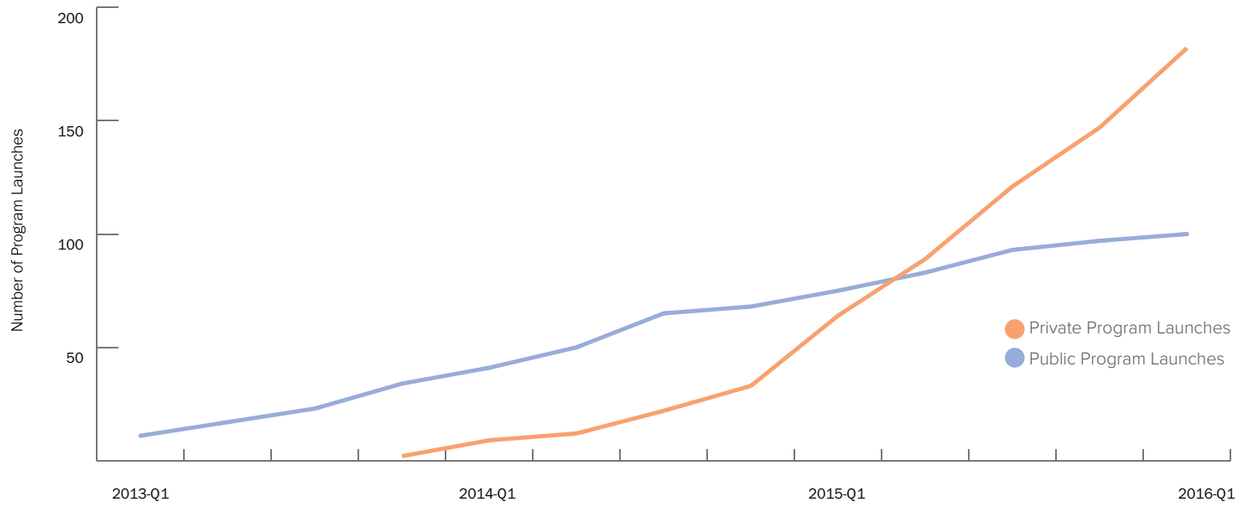
Myth #1: All bug bounty programs are ‘public’

False. Today, the majority of bug bounty programs are invite-only programs.

Since 1995, bug bounty programs have offered organizations a radically improved method for vulnerability discovery. Organizations such as Google, Facebook, Microsoft and others revolutionized application security by launching public bug bounty programs. Bug bounties have come a long way from these initial public, open-to-anyone contests that were popularized by those tech giants. The biggest change in the bug bounty model has been the addition of private programs.

PRIVATE PROGRAM LAUNCHES EXCEEDED PUBLIC LAUNCHES IN EARLY 2015. TODAY, NEARLY 2 OUT OF 3 BUG BOUNTIES WE LAUNCH ARE PRIVATE.

LEARN MORE IN OUR 2016 STATE OF BUG BOUNTY REPORT.



Why are private programs valuable?

Private programs offer organizations the opportunity to utilize the power of the crowd–volume of testers, diversity of skill and perspective and a competitive environment–for more focused testing.

While public programs are open to all researchers, private programs are limited to **vetted and trusted researchers**, giving organizations the power to better control the scope of what is tested, as well as how it’s tested.

Who can participate in private programs?

Bugcrowd has a large, skilled crowd of global security researchers coming from all walks of life, and varying degrees of experience in security research and bug hunting. Anyone can sign up to become a Bugcrowd researcher to participate in public bug bounty programs. As bug hunters submit bugs to public programs, climb the ranks within the community, and prove their trustworthiness, they may gain access to private 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.

Learn more about the different uses for private and public programs.

Myth #2: Only tech companies run bug bounties

False. The bug bounty model has evolved to be effective and flexible for organizations of virtually any size or type.

While they have been used for over 20 years, widespread adoption of the bug bounty model by enterprise organizations has just begun to take off within the last few. Private and public bug bounty programs provide an opportunity to level the cybersecurity playing field—by arming complex organizations with the strength and expertise to combat constant external threats. Companies of all sizes, and from all industries can now realize this advantage.

Our public programs run the gamut from B2B technology companies such as Barracuda and consumer Internet companies such as Pinterest to companies in more conservative industries such as Western Union in financial services and automotive manufacturers such as Fiat Chrysler Automobiles.

Why are private programs spearheading this diversification?

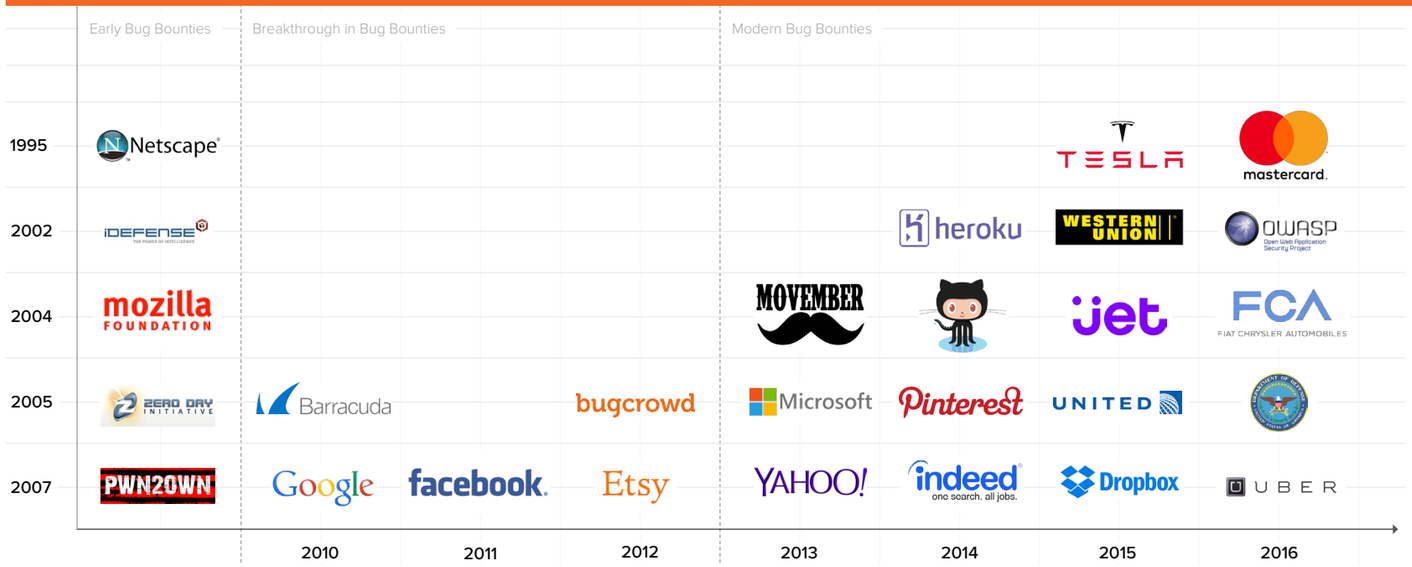
Beyond just public programs, private programs have been instrumental in the broader adoption of the bug bounty model. They have allowed a wider range of organizations to utilize the bug bounty model for various reasons:

- Ability to invite only the most trusted and vetted researchers, including ID or background checked researchers when necessary
- Focus testing more narrowly based on specific skill sets
- Organizations with lower risk tolerance may utilize a private crowd to get buy-in from internal legal and procurement departments more easily
- Limit exposure to personally identifiable information
- Test applications that are not publicly accessible

Learn more about the different uses for private and public programs.

TODAY OVER 25% OF BOUNTY PROGRAMS ARE LAUNCHED BY MORE TRADITIONAL VERTICALS SUCH AS FINANCIAL SERVICES.

READ MORE ABOUT THE HISTORY AND EVOLUTION OF BUG BOUNTIES.



Myth #3: Running a bounty program is too risky

False. With a trusted partner, running a bug bounty program is no more risky than other, traditional security assessment methods.

Although the bug bounty model is **gaining steady traction**, many organizations are still concerned about 'putting a target on their back.' Simply put, these perceived risks are tied to the volume of external testers and the level of control that can be retained.

"YOU CAN VERY WELL QUANTIFY AND CONTROL FOR THE RISKS AND REWARDS OF USING THE CROWD, SUCH THAT IN THE END, THE LEGAL EXPOSURE THAT AN ORGANIZATION HAS FROM USING THE CROWD IS BASICALLY THE SAME AS IT WOULD HAVE FROM ANY OTHER MEANS OF PEN TESTING THAT YOU MIGHT TRADITIONALLY BUY FROM A PEN TESTING PROVIDER."

JAMES DENARO, FOUNDER OF CIPHERLAW

PUBLIC DISCLOSURE INCIDENTS OCCUR LESS THAN .0005% OUT OF ALL SUBMISSIONS

Your organization should operate on the simple premise that **the risk of being vulnerable greatly outweighs the risks associated with running a bug bounty program**. Granting permission for security research is a great way to receive more vulnerability findings, giving your organization more knowledge and control, and ultimately reducing risk.

How does Bugcrowd mitigate the risks associated with running a bug bounty program?

Running a bug bounty program with a trusted partner lowers potential risk, as all community members follow a set of rules, outlining acceptable and unacceptable behavior. However, if the idea of opening up testing to the community-at-large is too much for your organization right now, you can run a private program with a select group of vetted researchers. The bug bounty model has adapted to meet the needs of companies with a wide range of risk tolerance. **Read more about bug bounty adoption in our State of Bug Bounty Report**.

FAQ: What happens if a researcher goes rogue?

In reality, incidents of public disclosure are **extremely rare**, and we actively work to prevent them.

We closely monitor public researcher communications and activity, and researchers are penalized for not complying with **Bugcrowd's Standard Disclosure Terms** which outlines acceptable and unacceptable behavior. In the event of a public disclosure incident–although rare and usually unintended–our team reaches out to the crowd member to ask them to remove the public information and notify them of the consequences of unauthorized disclosure. We reserve the right to issue a warning and/or removal of access to elements of the Bugcrowd platform on a temporary or permanent basis depending on the severity of the violation.

Organizations also have the option to run private programs to utilize strictly **vetted and trusted researchers**.

Myth #4: Bug bounties don’t attract talented testers

False: Many of our bug hunters are the most talented security researchers in the world, and many are full-time security professionals.

Although in public bug bounty programs there is no way to verify the combined talent or skill being utilized at any given time, the bug bounty model leverages volume to increase the quantity of skilled people being applied, and based on experience the volume of high-value results radically improves as a result. For our customers who require a more refined crowd with specific skill-sets, we run private programs with a skills-vetted and trusted crowd.

Who are they?

Our Leaderboard displays many of the world’s top researchers–individuals that most organizations would be hard pressed to hire. There is more to the community, however than those top ten. Our recent report, Inside the Mind of a Hacker, explores the community, including their geography, age, profession, experience and more:

- Many work full time in security, commonly as a penetration tester (17%), or a security engineer (15%). While most respondents are employed outside of bug hunting or identify as students, **15% of respondents identified as full-time bug hunters** and we see this number growing. See the full breakdown in the report.
- Bug bounty hunters are no strangers to the classroom–those with a college degree made up the largest group of participants (37%), followed by those with graduate degrees (21%). **84% had attended college for some period of time.**

What are they motivated by?

As this market grows and evolves from the small group of hackers it once was, it is becoming more nuanced, and the motivations of bug hunters vary widely.

Get the report, Inside the Mind of a Hacker, to learn more about their motivations.

“WE DECIDED TO RUN A BUG BOUNTY PROGRAM TO GET ACCESS TO A WIDE VARIETY OF SECURITY TESTERS. HIRING SECURITY RESEARCHERS IS VERY DIFFICULT IN TODAY’S MARKET… WE HAVE PRODUCTS THAT COVER A WIDE VARIETY OF APPLICATIONS, USING A WIDE VARIETY OF TECHNOLOGIES, SO WE NEED SECURITY TESTING THAT CAN COVER ALL THOSE AREAS.”

JON GREEN, SR. DIRECTOR OF SECURITY ARCHITECTURE, ARUBA

aruba

WANT TO LEARN MORE ABOUT BUGCROWD SOLUTIONS? VISIT BUGCROWD.COM/SOLUTIONS.

Myth #5: They don’t yield high-value results

False. Bug bounties help organizations uncover high-quality vulnerabilities missed by traditional security assessment methods.

It’s important to remember that the majority of organizations that we’ve helped run bug bounties have already had robust security testing programs in place, including automation and penetration testing, but we still find solid results, and usually within the first 24 hours.

“WE THINK OF THE BUG BOUNTY PROGRAM AS ‘PART OF THIS COMPLETE BREAKFAST.’ YOU HAVE ALL THESE INTERNAL ACTIVITIES, AND THE BUGCROWD PROGRAM FOR US... IS A NICE SUPPLEMENT TO THOSE THINGS, IT CATCHES BUGS THAT OUR INTERNAL TESTING DIDN’T CATCH. IT ALSO GIVES US INFORMATION IN WHAT IT DOESN’T REPORT.”

JIM HEBERT, SR. SECURITY ENGINEER, FITBIT

fitbit

ON AVERAGE, A P1 VULNERABILITY, THE MOST SEVERE BUG, IS SUBMITTED EVERY 27 HOURS.

LEARN MORE ABOUT VULNERABILITY PRIORITY IN OUR VRT

How do bug bounties fit with traditional security assessment methods?

Since day one, we have been proponents of a layered approach to security, and for many organizations, running a variety of vulnerability scanners and penetration tests are a general security best practice. It’s also no secret that, no matter how advanced, automation only goes so far–it finds only what it knows. Penetration tests have a place in many security programs but are limited in perspective and in time and effort.

Bug bounties should be part of any mature security program, filling the gap left by scanners, and exponentially improving the potential results found by consultants.

Learn more about the Bug Bounty Lifecycle.

What do they find?

Of the 75,000+ bugs our researchers have found, thousands of high severity bugs, in a wide range of bug types, have been found and fixed by our customers. Bug bounty programs often find bugs listed on OWASP’s Top Ten, as well as less frequently seen vulnerabilities. For a detailed view of many of these vulnerabilities, reference our Vulnerability Rating Taxonomy.

In the past several months the average priority across all vulnerabilities has increased as more complex targets are tested, the community of bug hunters learn and improve, and more talent is attracted to the Bugcrowd community.

Read the State of Bug Bounty Report to see the breakdown of vulnerabilities by criticality and type.

Myth #6: They're too costly and hard to budget for

False. You can control your bug bounty budget, and we help make the best suggestion for your organization.

While the bug bounty market continues to evolve, the key to success remains the same; to run a successful bounty program you must attract the right researchers. Often, attracting the right talent includes offering rewards. Without guidance, offering rewards and managing a budget for a bug bounty program presents organizations with a set of unknowns–a legitimate concern that can be easily mitigated with the support of a trusted partner.

Bugs start in development, and yes, finding a bug in the wild is more expensive to fix than it is in development. There is no such thing as 100% secure code–vulnerabilities will always get past vulnerability scanners, your team, and yes, your penetration test firm of choice. Bug bounties catch those bugs, but they don't have to be "blank check" affairs–we can help you manage your budget from start to finish.

How can I manage the costs throughout the lifecycle of my program?

There are many knobs and levers you can tweak to optimize the success of your program and minimize unknown variables such as cost.

1. Articulate what you do and don't want to be tested by defining a clear scope, focus areas and exclusions. Learn more about the Anatomy of a Bounty Brief.
2. Decide how you want to run your program–private or public. You may want to start private to limit your testing pool. Our On-Demand Program offers organizations a capped-cost project-based option to engage the crowd.
3. Determine your incentive program. You may start by offering Kudos only at first, adding and increasing cash rewards throughout the lifetime of your program.

How do you determine the reward range for bounty payouts?

Security maturity and submission priority are the most important variables when determining the appropriate value of a bug and give enough information to decide on a baseline reward range.

Learn more about What's A Bug Worth.

"EFFICIENCY AND EFFECTIVENESS OF THE CROWD IS REALLY WHY WE BRING THEM ON... BECAUSE WE HAVE THE CROWD INVOLVED IN THE VULNERABILITY MANAGEMENT PROGRAM, IT'S HELPED IN EXPANDING OF OUR TEAM FOR A FRACTION OF THE COST. NOW MY INTERNAL RESOURCES ARE BETTER UTILIZED."

DAVID BAKER, CSO, OKTA

okta

WE'LL WORK WITH YOU ONE-ON-ONE TO DETERMINE WHICH BOUNTY SOLUTION BEST FITS YOUR NEEDS.

LEARN MORE ABOUT OUR BUG BOUNTY SOLUTIONS.

Myth #7: Bounty programs are too hard to manage

False. With a trusted partner, bug bounty programs are easy, efficient and effective. You receive ready-to-fix, high value bugs.

We have run successful bug bounty programs for hundreds of organizations with the help of our all-in-one vulnerability disclosure platform, Crowdcontrol. We also have the world's most experienced team of application security experts and vulnerability disclosure space leaders to help make each program successful based on your needs.

What is Crowdcontrol?

Crowdcontrol connects your security team with Bugcrowd's diverse and skilled crowd of trusted hackers. From start to finish, our platform makes running a bug bounty program efficient and valuable.

- Set up and customize your bounty program, private or public, ongoing or time-boxed
- Connect and communicate with researchers participating in your program
- Crowdcontrol monitors activity, analyzing and categorizing submissions as they come in
- Reward researchers quickly and seamlessly for submitting valid bugs to your program
- Integrate with your development tools to ensure bugs get fixed promptly
- See program data and trends through easy to understand reporting dashboards

Program support and more

In addition to a powerful platform, you also gain access our unrivaled team of experts to ensure that your goals are identified and met, and your program is successful.

We will make sure you're prepared when your program goes live–setting a clear and thoughtful scope, making budgetting and reward recommendations based on your company's capabilities, and aligning expectations. During the life of your program, you'll only receive actionable insights–our application security team give triaged submissions a detailed review and your dedicated account manager works with your team continuously.

Learn more about Crowdcontrol supports our bug bounty solutions.

GETTING STARTED

Want to learn more about how your organization can leverage the bug bounty model to start discovering and fixing high-value vulnerabilities missed by traditional security testing? Bugcrowd offers a full line of bug bounty solutions and hackers on-demand.

Visit bugcrowd.com/introduction to learn more.

The pioneer and innovator in crowdsourced security testing for the enterprise, Bugcrowd harnesses the power of tens of thousands security researchers to surface critical software vulnerabilities and level the playing field in cybersecurity. Bugcrowd also provides a range of responsible disclosure and managed service options that allow companies to commission a customized security testing program that fits their specific requirements. Bugcrowd's proprietary vulnerability disclosure platform is deployed by Drupal, Pinterest, Western Union and many others. Based in San Francisco, Bugcrowd is backed by Blackbird Ventures, Costanoa Venture Capital, Industry Ventures, Paladin Capital Group, Rally Ventures and Salesforce Ventures. Bugcrowd is a trademark of Bugcrowd, Inc.