bugcrowd

7 Bug Bounty Myths, BUSTED

Utilizing the power of the crowd through bug bounty programs

An attacker only needs to exploit one security flaw to compromise an entire organization, while the organization must defend against EVERY potential flaw. 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.

MORE COVERAGE

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 diverse crowd of researchers with the determination and skills to find critical vulnerabilities quickly and efficiently. Some researchers have deep expertise in one area, while others have mastery in a few specialized areas. Their creativity contributes to the wide range of vulnerabilities found in a bug bounty program.

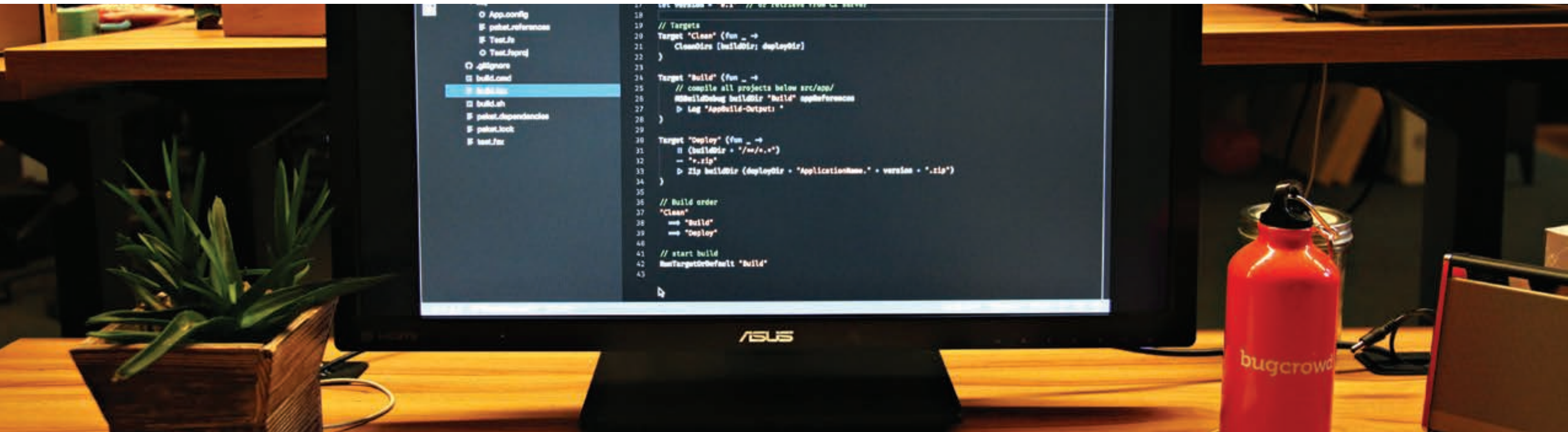
BETTER RESULTS

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

The crowdsourcing model has proven to deliver 7X more critical findings than traditional methods.

BETTER ROI

Bug bounties utilize a pay for results model, ensuring you only pay for valid results, versus paying for time and effort spent like with traditional testing methods.



```
// Targets
Target "Clean" (fun _ ->
    CleanDirs [buildDir; deployDir]
)

Target "Build" (fun _ ->
    // compile all projects below src/app/
    MSBuildDebug buildDir "Build" appReferences
    |> Log "AppBuild-Output: "
)

Target "Deploy" (fun _ ->
    !! (buildDir + "/**/*.*")
    -- "*.zip"
    |> Zip buildDir (deployDir + "ApplicationName." + version + ".zip")
)

// Build order
"Clean"
  ==> "Build"
  ==> "Deploy"

// start build
RunTargetOrDefault "Build"
```

Despite the fact that bug bounty adoption continues on a steady rise and ROI has been clearly demonstrated, perceived misconceptions still remain.

From years of running bug bounty programs for more of the Fortune 500 than any other crowdsourced security platform, we will address seven of the most common myths surrounding the bug bounty model:

1. **ALL BUG BOUNTIES ARE ‘PUBLIC’**
2. **ONLY TECH COMPANIES RUN BUG BOUNTIES**
3. **RUNNING A BOUNTY PROGRAM IS TOO RISKY**
4. **YOU CAN’T TRUST HACKERS**
5. **THEY DON’T YIELD HIGH QUALITY RESULTS**
6. **THEY’RE TOO COSTLY AND HARD TO BUDGET FOR**
7. **BUG BOUNTIES ARE HARD TO RUN AND MANAGE**

MYTH #1:

ALL BUG BOUNTIES ARE ‘PUBLIC’

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

Since their inception, bug bounty programs have offered organizations a radically improved method for vulnerability discovery. By harnessing the power of crowdsourcing, 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 the public, open-to-anyone competitions that were popularized by those tech giants. The biggest change in the bug bounty model has been the addition of private programs.

> “We have products that cover a wide variety of applications that utilize various technologies. Bugcrowd offers the continuous private testing coverage we need at scale.”
>
> **Jon Green, Vice President & Chief Technologist of Security,** aruba

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 competitive environment – in a more controlled and stringent environment. Where public programs are open to all researchers, private programs and limited to vetted and trusted researchers, giving companies the power to control what is tested and how it’s tested. This type of program is a great entry point for anyone looking to start their first bug bounty program or introduce testing on a new asset — it offers significant breadth and depth of coverage without overwhelming your security and development teams.

Which researchers 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, 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 trustworthiness receive invitations to private 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 every size and type.

While bug bounties have been used for more than 20 years, widespread adoption 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.

Our public programs run the gamut, from B2B technology companies such as Barracuda and consumer Internet companies such as Pinterest, to conservative financial bodies like Western Union and automotive manufacturers such as Fiat Chrysler. Private programs also allow more conservative organizations to run bug bounty programs with more control.

By welcoming only the most trusted and vetted researchers to participate in their bug bounty programs, organizations with lower risk tolerance can get buy-in from internal legal and procurement departments. More traditional organizations such as financial services companies or government organizations opt to engage a private crowd to limit exposure to personally identifiable information. Private programs are also useful for testing applications that are not publicly accessible, and for testing hardware.

FCA FIAT CHRYSLER AUTOMOBILES   TESLA   mastercard   credit karma   WESTERN UNION WU

MYTH #3:

RUNNING A BOUNTY PROGRAM IS TOO RISKY

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

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

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. Externally accessible apps are already targets and are almost certainly under attack anyways. Granting permission for security research is a great way to receive more vulnerability findings, giving your organization more knowledge of unknown vulnerabilities, and ultimately reducing risk.

How does Bugcrowd mitigate risks associated with running bug bounties?

Running a bug bounty program with a trusted partner lowers potential risk, as all community members follow a set of rules and guidelines, 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.

What happens if a researcher goes rogue?

Within the bug bounty landscape, public disclosure incidents are extremely rare and we actively work to prevent them.

We closely monitor public researcher communications and activity constantly. Researchers are penalized for not complying with our Standard Disclosure Terms and Researcher Code of Conduct.

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:

YOU CAN'T TRUST HACKERS

False. With the right guidelines and incentives, white hat hackers are the good guys, security researchers that approach breaking into code like an adversary to help organizations.

During the past year alone, we have witnessed a number of devastating cyber attacks. 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.

Bugcrowd security researchers have expertise in many technologies—opening direct access to hard-to-find resources and skill sets. 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.

Who are they?

Bug hunters are young, ambitious, and always looking to expand their knowledge and build on their skill set through the challenge of the hunt. 62% of bug hunters reinvest earnings from bug hunting back into their craft, spending it on security tools and training. Most researchers aren't "full-time" bug hunters—they hold regular 9-5 jobs... though many would like to be.

The bug bounty community is a truly global group of people, coming from all walks of life, with diverse backgrounds, technical skills and expertise. This diversity is what fuels the power of the bug bounty model, connecting a community of skilled, creative individuals with organizations that need their help. 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.

We encourage all of our researchers to go through our I.D. verification process in which we verify identity and geography through a third-party provider. This may be useful for organizations that require identity or geography verification for compliance or legal reasons, or if geography may impact application accessibility. This goes beyond the vetting process of many pentesters, who may only go through an interview, reference calls or criminal background check.

MYTH #5:

BUG BOUNTIES DON’T YIELD HIGH-QUALITY RESULTS

ALL YOUR BUGS ARE BELONG TO US.
MY OTHER COMPUTER IS YOUR COMPUTER

False. Bug bounties help organizations uncover 7X more critical vulnerabilities than traditional security assessment methods.

It’s important to remember that the majority of organizations that 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.

How do bug bounties fit with traditional security assessment methods?

Given the cybersecurity landscape, we’ve always been proponents of a layered approach to security, prioritized based on specific organizational capabilities, needs, sensitivities, and goals. It’s also no secret that, no matter how advanced, automation only goes so far—it can only find what it knows to find. Penetration tests have a place in many security programs also but are limited in perspective and in time and effort. This leaves a gap that requires human creativity to fill, and crowdsourcing that creativity is by far the most effective way to bring it into the mix.

What do bug hunters find?

Of the tens of thousands of valid bugs our researchers find, thousands of high severity bugs, in a wide range of bug types, are found and fixed by our customers. For a detailed view of many of these vulnerabilities, reference our Vulnerability Rating Taxonomy.

> “The effect and the impact of an external person reporting a vulnerability or lots of vulnerabilities is very different to your own internal AppSec team reporting some vulnerabilities. The impact is just different, and everyone around an organization looks at this with a very different set of eyes when these things get reported externally.”
>
> **Daniel Grzelak, Head of Security,** ATLASSIAN

MYTH #6:

THEY'RE TOO COSTLY & HARD TO BUDGET FOR

False. You can control your bug bounty budget, and we help make the best recommendations for your organizations need.

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 talent. Often, attracting the right talent includes offering rewards. Without guidance and proven methodology, offering rewards and managing a budget for a bug bounty program presents several unknowns.

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–a trusted partner 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 things you can do to optimize the success of your program and minimize cost.

Clearly articulate what you want to be tested by defining a clear and thorough scope, focus areas and exclusions.

Decide how you want to run your program–private or public, continuous or time-boxed. You may want to start private to limit your testing pool and eventually grow to a public program. Our On-Demand Program offers organizations a capped-cost project-based option to engage the Crowd.

Determine your incentive program. You may start by offering "kudos only" at first, adding and increasing cash rewards throughout the lifetime of your program. Security maturity and submission priority are the most important variables when determining the appropriate value of a bug.

Bug bounties don't have to be "blank check" affairs — a trusted partner can help you manage your budget from start to finish.

MYTH #7:

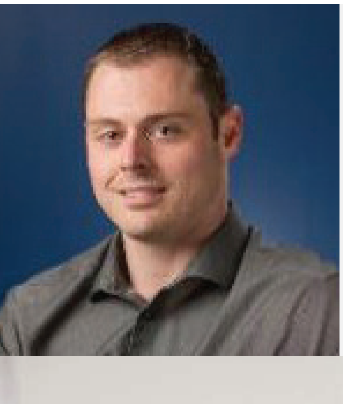
BUG BOUNTIES ARE HARD TO RUN & MANAGE

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

Running a bug bounty program on your own is difficult. Organizations hardly have the time or resources to triage and validate incoming vulnerability findings from outside researchers. We recognized this pain point at the onset and have remained committed to providing our customers with full-scale bug bounty support and services since day one.

How does Bugcrowd support program management?

We provide full-service management, including expert technical review and escalation of valid vulnerability submissions. In addition, our teams provide the facilitation of researcher communications crucial for detailed reports, deeper context, and high engagement.



> “For us, the managed approach reduced our requirement time and effort by at least 80% allowing us to not only focus on what matters the most, implementing the remediations, but also freeing up our security team to focus on other components of our security program.”
>
> **Johnathan Hunt, VP, Information Security,** invision

Researchers put a lot of time and effort into their submissions. For this reason, we feel that every submission deserves full attention and a quick response. That’s why each and every vulnerability submitted through our platform is reviewed by one of our application security engineers.

Our response time is unsurpassed – our average time to first response for all submissions is well under the 24-hour SLA we set for critical vulnerabilities.

Further, our payouts are industry leading with more than 80% of all valid vulnerabilities rewarded within 1 minute of acceptance.

We set the bar high for bug bounty triage and validation providing nearly all signal (94.76% to be exact) for customers across all of our managed programs.

Getting Started
Want to learn more about how your organization can leverage the crowdsourced security model and start discovering and fixing high-value vulnerabilities missed by traditional security testing? Bugcrowd offers a full line of crowdsourced security solutions.
www.bugcrowd.com/get-started