How To Debunk These 6 Common Bug Bounty Misconceptions

BY ANNA HAMMOND · APRIL 28, 2021 · LAST UPDATED ON MARCH 6, 2025

The value of bug bounty programs is recognised by well-known companies all over the world. However, there are still a few stubborn myths about the concept that persists. This article lists six of the most common misconceptions we hear when speaking to potential customers about bug bounty programs.

The truth about bug bounty programs

There is only one truth to what a bug bounty program does. In short, a bug bounty program invites ethical hackers to test cybersecurity defences and search for vulnerabilities that could let bad actors penetrate an organisation's system. For every vulnerability discovered, the company that the program belongs to will pay a predefined bounty to the finder.

However, despite them being around for decades, many bug bounty myths linger on. Here are six of the most common ones we come across:

- **Too much risk:** A bug bounty program exposes us to hackers.
- **We're too small:** A program requires a lot of time and a large infrastructure.
- **They're too expensive:** Only large companies can afford the budget.
- **Ethical hackers aren't trustworthy:** They may be tempted into working maliciously.
- **We're not ready:** We're still working on new features and products.
- **We'll never get sign-off:** It's a PR team's worst nightmare to work with hackers and we'll never get our legal department to grant us permission.

Interestingly, some of these misconceptions have some truth to them — but not in the way you might think. Read on to get a better handle on bug bounty programs so that, moving forward, you can confidently separate the truths from the myths.

1. Bug bounty programs encourage hackers to hack you

The verdict: True

Indeed, bug bounty programs expose you to hackers — but not all hackers are malicious. Due to a desire to do good, many hackers choose to extend their descriptive name to 'ethical hacker', 'white-hat hacker' or 'bug bounty hunter.' They'll attempt to hack into your systems with the objective of helping you find exploitable weaknesses.

Yet, even without a bug bounty program, you're already exposed to hackers from both sides of the law. Actively involving ethical hackers will streamline the reporting process and empower your security team to build stronger defences against cybercriminals.

Key takeaway: Ethical hackers work with you, not against you

The sad truth is bad actors won't seek your permission to hack your business. A simple yet proven method to protect against cyber threats is to invite ethical hackers in. Bug bounty programs follow this concept at scale by applying a crowdsourced mentality to security testing.

2. You can't trust ethical hackers either

The verdict: Misconception

Many people associate hackers with criminals, imagining a person who can take out whatever he or she desires through their computing skills. However, in 2021, becoming an ethical hacker is a popular ambition amongst security professionals around the world. Like malicious hackers, they're driven by the goal to break through a target's cybersecurity defences. However, ethical hackers operate within the law and will disclose bugs to the companies they work with.

Despite this, when speaking to businesses who are less experienced with bug bounty programs, there is still a genuine concern that white-hat hackers could be malicious in disguise. It's important to consider what a cybercriminal typically seeks out in a target: an easy win that they can quickly exploit. When you publish a bug bounty program, you're publicly announcing that you take security seriously.

Key takeaway: Ethical hackers operate within the law

At Intigriti, we often refer to ethical hackers as 'security researchers' because we find that this term does more justice to the long hours of research, study and perseverance it takes to find vulnerabilities. The term also helps to avoid any of the negative connotations that are sometimes associated with the term hacker.

3. We don't have the time or the infrastructure

The verdict: Misconception

Most companies would agree that time and resources are precious — no matter their size or level of maturity. Companies find bug bounty platforms to be one of the most reliable and stable ways to set up programs. When you sign up to Intigriti as a client, for example, a customer success manager will help you optimise for success. They'll work with you to define a clear scope for your program and advise on aspects like bounty budget and spend management.

Another benefit to running a program through a platform is that when security researchers take part in a program and find a bug, they submit a report via the platform. This allows the report to go through a process of quality control, known as triage.

The triage team will first check if the report is valid, unique, and in scope and they'll also act as the middleman between companies and security researchers. The added steps ensure your internal team only receives actionable, valid reports so they can stay focused on business-as-usual activities.

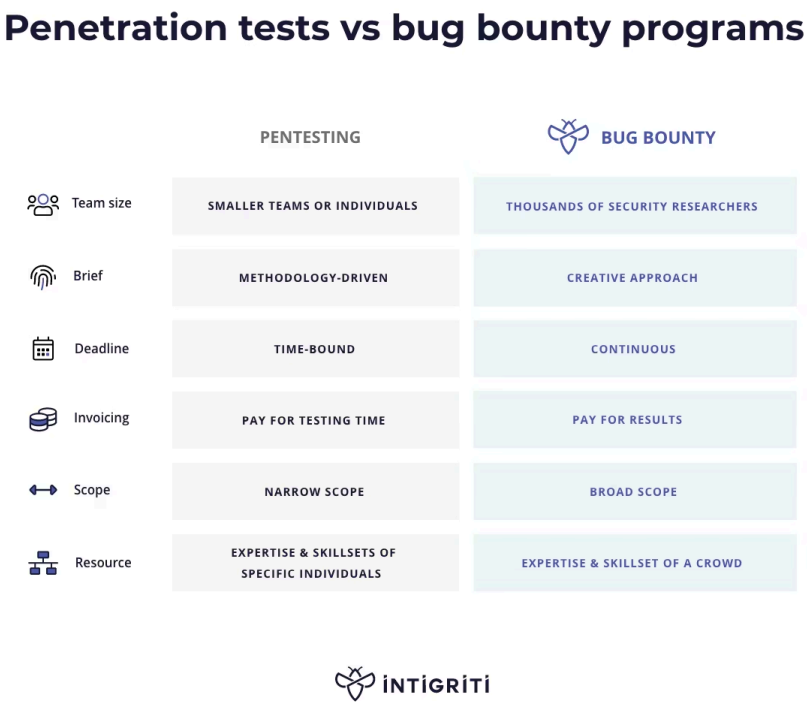
Key takeaway: Bug bounty platforms provide a stable infrastructure for programs

Before launching a bug bounty program, consider first how you'll manage quality control to ensure you only get valuable bug bounty reports. A proven solution to this challenge is to partner with a bug bounty platform. Not only will it help to avoid time-wasting reports, but your internal team will thank you for it too. They'll be able to fix bugs faster while staying focused on their usual work tasks.

4. Only larger businesses can afford a bug bounty program

The verdict: Misconception

It's a common bug bounty misconception that only large companies can afford one. Unlike penetration tests and other alternatives, bug bounty programs operate by a pay-for-results model. This means a company pays a researcher for a previously unknown vulnerability that requires action.



Penetration tests vs bug bounty programs

What you set as a budget for your program is up to you — but the fact that it even exists is going to help your team drive up defences against malicious actors.

When you first launch a bug bounty program on Intigriti's platform, we apply safety limits through a soft launch. This typically involves starting with lower bounty amounts and a restricted number of researchers to ensure the attention you receive from researchers balances out with the budget. When managed poorly, the cost of pay-outs can indeed add up fast. It can also be energy draining for an already busy department to be reviewing and triaging all incoming reports. Using a bug bounty platform, and the service that comes with it is an extremely impactful way to ensure your budget gets maximum leverage.

Key takeaway: Bug bounty platforms work well with small and large budgets

While many companies take reasonably good measures to prevent breaches, hackers never sleep. As the form of threats keeps changing, understanding your vulnerabilities and keeping up to date has never been more vital. Bug bounty platforms offer a realistic and affordable solution to these pain points. Most importantly, investing in testing today will reduce the risk of your business becoming victim to a costly hack later.

5. Bug bounty programs aren't suitable for pre-launch testing

The verdict: Misconception

The whole point of being hacked is that you're never ready for it. If you're nervous about pre-launch testing, it may be worth considering a private program first.

A private bug bounty program enables you to work with a few hand-selected security experts. Plus, you can choose to exclude certain areas from external tests until you're happy that it's fully stable — these details can be included within the scope of your program. You can also direct researchers to look for specific breaches, such as vulnerabilities with potential financial impact.

Key takeaway: Pre-launch testing helps businesses launch more secure products

When doing pre-tests, start small and focused. Once you're comfortable handling more reports, you can open up the scope or consider launching a public bug bounty program.

6. PR and legal departments will never approve a bug bounty program

The verdict: Misconception

"Don't underestimate your legal department," is the advice Intigriti's CEO, Stijn Jans, gives in this case. "Legal departments are facilitators. What corporate lawyers understand better than anyone, is that being hacked is a huge legal risk, and ensuring the right precautions are in place is high on their list of priorities."

As far as PR is concerned, embarking on an ethical hacking program is good for public relations. Why else would Microsoft, Apple and other major brands be delighted to talk about their bug bounty programs? Their stakeholders, be it clients, investors, shareholders, boards, staff and even the general members of the public place great value in the security of their data and their assets.

Key takeaway: Bug bounty programs send a positive message to stakeholders

Far from being a PR or legal problem, bug bounty programs highlight the responsible attitude of a business doing all it can to protect its customers against cyber threats. It sends a message that you take data protection seriously.

Ready to streamline your vulnerability disclosure process? Speak to a member of the Intigriti team today to request a demo.

REQUEST A DEMO