How to get more valuable bug bounty reports from security researchers

BY INTIGRITI · APRIL 8, 2021 · LAST UPDATED ON MARCH 6, 2025

Bug bounty programs are a great way to test the security of digital assets continuously. However, if most of the reports are low-quality or invalid, the system can quickly become a burden on your team. In this article, we provide tips on how to improve the value of your bug bounty reports.

Before launching a bug bounty program, consider how you'll manage quality control. This will help avoid time-wasting reports and empower your team to focus on fixing bugs faster.

Read on to discover our four actionable tips.

1. Craft a clear and detailed bug bounty policy

The first thing you should do is craft a clear and detailed bug bounty policy. Security researchers often submit informational reports and invalid issues because they don't understand the company's priorities. To ensure that security researchers spend their time on the issues you care about, you need to craft a detailed bounty policy. Critical information that you should include in your bug bounty policy is:

- The assets and domains that you want testing
- The assets and domains that you don't want to be tested
- Issues and vulnerability types that you want to be reported
- Issues that you do not want to be reported and issues that would be classified as informative or invalid
- Rules of participation, such as reporting format and disclosure policy
- And bounty amounts for each bug type.

A good bug bounty policy states prevent researchers from submitting reports that you don't care about due to misunderstanding.

2. Disclose a bug bounty report example

The next step to improving bug bounty reports is to disclose a well-written sample. You can publish excellent reports submitted to your program, along with their bug types, triage timelines, and reward amounts. These disclosure reports can serve as a positive example of what you are looking for so that researchers understand what findings your company values and rewards.

Disclosing a bug bounty report example will also help create an atmosphere of transparency and openness in your bug bounty program. Researchers will be more incentivized to produce new findings if they understand that their results will be valued and rewarded.

You can also disclose poor examples, such as reports that include invalid findings or confusing language. Researchers will be more cautious of submitting these reports once it is demonstrated that they will not result in a reward. Disclosing feedback about bad reports will also help educate the hacker community about your product and business priorities.

3. Maintain long-term researcher relationships

One of the best strategies to maximize the benefits of a bug bounty program is to generate long-term relationships with top-performing researchers. Bug bounty programs will often have a handful of "star researchers" who consistently report highly critical and valuable vulnerabilities.

To maximize the signal-to-noise ratio of your bug bounty program, strive to build and maintain relationships with these expert hackers by showing your appreciation to them. This doesn't have to be through financial incentives—although you should always aim to reward every valid submission fairly and on time. Other ways to show appreciation include being professional in your correspondence, triaging issues quickly, and keeping researchers updated on the progress of the fix. This will build trust and attract top performers to your program.

In addition to cultivating relationships with current superstar hackers, help beginners improve by providing them with feedback about their reports. Researchers tend to submit more valuable reports as they learn about a particular vulnerability and a specific product. Researchers who aren't currently submitting valuable reports can most certainly become superstars in the future. Fostering these relationships often leads to fruitful collaborations down the line.

4. Use a bug bounty platform to manage the triage process

Finally, there will always be invalid reports, informative reports, and duplicates in any bug bounty program—and managing these reports can be time-consuming. To ensure that your developers and security team spend their time on actual vulnerabilities, you can employ a managed bug bounty service.

Managed bug bounty services take out the administrative burdens of running and managing a bug bounty program. Bug bounty platforms automate much of the process, and a team of experts will deal with false-positive reports for you. For example, at Intigriti, a dedicated group of security experts filter the reports submitted to your program and only forward you the ones that matter.

To learn more about how Intigriti can make running a bug bounty program a breeze, schedule a demo with us today.