How to attract security researchers to test on my bug bounty program?

BY ELEANOR BARLOW · SEPTEMBER 3, 2025 · LAST UPDATED ON JANUARY 2, 2026

What you will learn

- **How to attract top security researchers to your bug bounty program** by offering competitive rewards and structuring bounty payouts that align with researcher motivations and industry standards.
- **How to improve program engagement and researcher experience** with clear communication, fast response times, and a strong, comprehensive program brief that reduces ambiguity.
- **How to boost participation through strategic launch incentives and ongoing visibility** using promotions, expanded scope, and external outreach to make your bug bounty stand out.

You asked, and we answered.

At Intigriti, we've been paying close attention to the questions most frequently asked by those with a bug bounty program in place. That's why we've launched this blog series dedicated to answering the most asked questions, diving into hot topics, and sharing practical and expert-backed strategies to help you maximize your bug bounty success.

So far in this series, we have answered the question [**"What is the pattern that can be expected after going public with a bug bounty program?"**]

Today, we look at "How do you attract top security researchers to your program?". Let's explore what draws in the best talent and how you can stand out in the crowd.

What to do once you go live

To attract and retain top talent, there are a multitude of activities that need to take place.

But where do you start?

Below are four proven ways to increase participation in your bug bounty program.

Competitive bounties

First, offering rewards that match the research involved is critical.

In our '[Ethical Hacker Insight Report, 2024]', it became clear that financial motive is the top driver for our hacking community. Over 76% of security researchers hunt for bugs with some financial motive in mind. 33% look for a large or maximum payment.

Simply put, don't underpay for high-severity vulnerabilities. We are not saying to throw all your money at the problem, but if your bounties are below market average, the top researchers will move on.

'If you pay under market value, you will not attract the top hackers' - Bug bounty calculator

Responsive communication

42% of researchers look for a responsive team.

In the hacking community, first impressions count, and speed and clarity matter. The faster you respond to reports, especially valid ones, the more likely researchers are to stay engaged and continue testing.

An Intigriti researcher who goes by the name Kuromatae666, explains how he picks a target for bug bounty hunting:

"When I pick a target, the most important aspect to me is how the company responds – including the time they take to do so. Sometimes, I only report one or two vulnerabilities at first and see how they respond before sending others. To me, first impressions count."- Kuromatae666

Prompt triage and feedback are just as important as monetary reward, as pointed out by top researchers...

"Setting a clear scope, along with offering competitive bounty ranges and efficient average response time, will make the program significantly more attractive." Lyubomir Tsirkov, in Hacker spotlight.

Strong program brief

This may seem obvious, but review your brief and make sure it is clear, comprehensive, and well-structured.

The scope should detail what ethical hackers can or cannot test, and include more systems or assets to test. Clearly define the scope of testing, include up-to-date documentation, known limitations, and provide test credentials where applicable.

Security researchers sometimes submit invalid issues simply because they don't have a clear idea of the company's priorities.

A strong scope not only reduces noise but also attracts quality researchers by helping them understand exactly what systems are in scope and what are not, meaning no time is wasted and no frustration is experienced in trying to understand what is allowed.

'68% of security researchers said they seek out programs that offer a lot of scope. Similarly, 43% said they're most interested in programs with fresh scope, such as recently added elements to the bug bounty program.' - How to get more valuable bug bounty reports from security researchers

Launch incentives

Kick off your program with a bang!

Consider offering time-limited bonuses or gamified contests. Such promotions can generate buzz and give your program early momentum, especially among top-tier researchers seeking fresh opportunities.

While it's a key component, attracting researchers isn't just about money; it's about clear communication, fast engagement, and providing a rewarding experience.

'Make your program stand out compared to the other programs and entice the researchers to get started. This may be through an attractive bounty table, a specific way of communicating, a large scope, information about releases (more chances of success after a recent release), or specific rewards like swag or vouchers.' – Program setup

Your program needs to stand out among hundreds of others. Ensure feature spots are placed, and news is shared externally via social media and newsletters.

Next steps to enhance your bug bounty journey

With a strong foundation and attention to detail, your program can stand out and thrive with Intigriti. We continually engage with our community and promote programs in a multitude of ways, including options to co-market public programs and ensuring the researchers' skills align to each unique program scope.

For more information on any of the points made in this article, contact the team today to discuss further. And keep an eye out for our next blog, where we dissect another popular question posed to our team!

Interested in a particular topic? Send us the questions you would love to get answers to by emailing pr@intigriti.com

AUTHOR

Eleanor Barlow

Eleanor Barlow is a London-based Senior Cyber Security Technical Writer at Intigriti, with 9+ years' experience reporting on and writing for the cyber and tech sector. She specializes in data-driven content on cybersecurity and bug bounty intelligence, helping organizations benefit from the latest trends and insights.