How can I get more bug bounty submissions and higher-severity findings?

BY ELEANOR BARLOW · SEPTEMBER 22, 2025 · LAST UPDATED ON JANUARY 2, 2026

What you will learn

- **How to increase the quantity and quality of bug bounty submissions** by providing clearer context, business logic, and asset complexity so security researchers uncover more issues.
- **How to prioritize critical systems and design reward structures** (including higher-tier bounties and incentives) that attract researchers and encourage them to find and report high-severity vulnerabilities.
- **How promotions and public visibility can boost engagement** with your bug bounty program and lead to a higher volume of impactful, high-severity findings.

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:

- How to attract security researchers to test on my bug bounty program?
- How should I scope third-party assets in my bug bounty program?
- What is the pattern that can be expected after going public with a bug bounty program?

Today, we discuss the question 'How can I get more submissions, especially regarding higher-severity findings?'

To boost the quantity and quality of submissions, focus on this four-part strategy.

1. Add context and business logic

Researchers are more likely to highlight high-severity findings when they understand how your assets are used in real business scenarios. Provide as much information as possible on how systems are used in your company to provide a clear idea of asset complexity.

'Asset complexity refers to how secure or complex an asset is [...] some assets are hard to hack and require attractive bounties and well-structured programs to keep skilled researchers engaged.' - Security

maturity, complexity, and bug bounty program effectiveness

By providing elements such as user flows and describing business logic, you arm researchers with the knowledge of how best to approach an asset and enhance their ability to dive deep and highlight high-severity bugs or flaws from the start.

The bottom line is that a clear and accessible program is imperative. Intigriti reviews every program, both pre- and post-launch, to get expert opinions from the team and the hacking community.

2. Prioritize impactful assets and clarify bounty structure

It may seem simple, but ensure that your most critical systems, as well as production environments and business-critical apps, are in scope. Researchers analyse assets inside a scope, so ensure that these elements are included to drive high-severity findings.

By assigning higher-tier bounties to your crown jewels, you signal their importance and attract researcher attention.

‘Bounty tiers let you strategically allocate rewards, prioritizing critical assets while maintaining broad coverage in your program.’- Bounty tiers

Make sure your rewards reflect the severity and impact, especially for critical issues. If you assign scoped items to specific tiers, then it is easier to prioritize critical assets with higher tiers, offering, typically, larger rewards.

This transparency helps researchers understand what they can earn and encourages them to focus on high-impact targets.

3. Running promotions and incentivising researchers

Create urgency and excitement by offering time-limited bonuses.

For example, you could offer the first valid critical submission within launch week a bonus. By offering bonuses or elevated tiers for critical and time-sensitive findings, you create a compelling incentive for deeper and faster research.

'Bounty tiers let you strategically allocate rewards, prioritizing critical assets while maintaining broad coverage in your program.'- Bounty tiers

Offering exclusive swag is also another method used to direct focus to areas you want tested, such as newly released features.

4. Move to a public program

Increase your visibility by moving your program to the public. Private programs limit exposure and the potential value, and can make it harder for marketing and sales to reference and celebrate a successful program.

Next steps to enhance your bug bounty journey

For more information on any of the points made in this article, contact the team today.

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'd 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.