How do I know I’m paying the right amount of bug bounty?

BY ELEANOR BARLOW · SEPTEMBER 29, 2025 · LAST UPDATED ON JANUARY 2, 2026

What you will learn

- **How to set the right bug bounty payouts** by aligning reward amounts with vulnerability severity, risk exposure, and industry benchmarks to attract skilled security researchers.
- **How to optimise bug bounty pricing strategies** using flexible reward ranges and asset-based scoping to balance program costs and researcher engagement.
- **How to maximise ROI from your bug bounty program** by understanding researcher motivation, avoiding under or over paying, and scaling rewards as your security maturity grows.

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?
- What is the pattern that can be expected after going public with a bug bounty program?
- How should I scope third-party assets in my bug bounty program?
- How can I get more bug bounty submissions and higher-severity findings?

Today, we discuss determining if you are paying the right amount of bounty for submissions.

Defining the right amount of bounty reward can be a challenge, especially for companies just getting started with a bug bounty program. Pay too little and you won’t interest researchers. Pay too much and you impact your Return on Security Investment (ROSI).

“Anyone can set up a bug bounty program, but if you aren’t sure what you’re doing, you may pay too much for vulnerabilities. Even worse, set your bounties too low and you may not attract any researchers at all. Our experience as a leading crowdsourced security platform shows us that researchers are highly tuned to payments. It’s important to find the sweet spot to ensure your program remains an attractive proposition.” – Inti De Ceukelaire, Intigriti

Payouts should match vulnerability severity level to engage researchers and build trust and transparency within the community. To do this, there are many elements to consider, including the value of assets, program maturity and budget, researcher effort, report quality, and industry benchmarks.

Industry standards, benchmarking, and calculators

While many in the cybersecurity space are familiar with CVSS (Common Vulnerability Scoring System), an open cybersecurity framework used to calculate the severity of cybersecurity vulnerabilities, there have been multiple versions and adaptations of this framework. The latest version (4.0) is designed to assess the severity of security vulnerabilities across multiple environments and dimensions, including exploitability, impacts, scope, and more, and provide a numerical score (0.0 to 10.0) of said vulnerabilities. Each score corresponds with a severity label (none, low, medium, high, and critical), for which reward payouts are set.

By using CVSS in bug bounty, the evaluation of bug severity is standardised, which means a reduction in bias of payouts, especially when multiple submissions are made. It also means that bounties are aligned with risk, and reasoning is provided as to why a bounty is worth 'x' as opposed to 'y'.

Bug bounty calculators, such as Intigriti's, automate this process and show you how your payouts stack up across severity levels.

Other elements can be used to complement CVSS, such as the Exploit Prediction Scoring System (EPSS), which can be used to predict the probability of vulnerabilities being exploited. This can complement CVSS v4.0 as it identifies theoretical vulnerabilities that are most likely going to be targeted, which means teams can further prioritize their efforts.

Enabling flexible bounties

With this in mind, set minimum and maximum payout to cover severity levels. Why? Because not all assets are equal, bounty tiering systems are needed to ensure that higher payouts are made for business-critical targets. With a minimum and maximum range, researchers are aware of the potential payouts, while you maintain flexibility to reward fairly based on the asset or depth of exploitability.

'A more advanced approach, ranged bounties allow program editors to define a minimum and maximum bounty amount for each severity level. This range enables a more granular reward system. Submissions' severities are mapped to CVSS scores, which in turn determine the possible bounty within the set range. Program members can manually override the severity level if needed, and in cases where no CVSS score is available, the minimum range amount will be used.' – Ranged Bounties

On occasions when a researcher discovers a critical or exceptional vulnerability in complex systems or in a new way, custom bounties can be used to show recognition for great work. This could additionally incentivize other researchers, as it shows that, while a cap is in place, the company is willing to reward innovative research and has the financial capacity to do so.

Read more on how to attract security researchers to your program as you grow here.

Why does financial scope matter to researchers? Does benchmarking higher help?

The majority of researchers are driven by financial gain. While many other factors may motivate a researcher, such as recognition, charity, or simply the thrill of a challenge, financial gain is a top

contender. This means that they value fair and predictable awards, transparency regarding payouts, and recognition of high efforts.

When budgets are tight, it can often be a difficult decision to set higher bounties. But this can significantly pay off in terms of ROSI, as your program attracts more talented researchers. Remember, prevention is always more cost-efficient than treatment in cybersecurity.

'Higher-tier rewards can help incentivize researchers to invest time in these more complex or hardened targets. Many program owners start the newly added scope at Tier 3, 4, or 5, then move it to higher tiers as it matures and the easy-to-find vulnerabilities are addressed.' – Bounty Tiers

Talented researchers are more inclined to prioritize programs that set higher reward structures and compete fairly for their time and skills. Organizations benefit not only from deeper testing but also from more valuable findings and a stronger security posture. Plus, if a researcher knows what to expect from hunting on your platform and can see a quick and fair response to their work, they are more likely to engage with your program and try for more complex bugs well into the future.

To stay competitive in the market, ask your Customer Success Manager (CSM) for industry comparisons to become aware of what the real-time averages are so that your program remains attractive and is effective in the long run.

Adapt as you grow

A successful bounty program systematically rewards both the severity of discovered vulnerabilities and the effort of researchers, ensuring fair and consistent compensation. Benchmark ranges and fine-tune based on impact. And don't be afraid to adjust your program as it evolves. It is best to review the structure every six to twelve months to see if bounties need to be altered.

Explore more on what patterns to expect and actions to take in the first six months of starting a bug bounty program, here.

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.

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com