Preventing the growing costs of repeat and duplicate bug bounty submissions

BY ELEANOR BARLOW · JULY 10, 2025 · LAST UPDATED ON JANUARY 2, 2026

What you will learn

- **How to understand and distinguish duplicate vs. repeat bug bounty submissions**, so you can reduce redundant reports and better manage your program's workflow.
- **How repeat and duplicate submissions impact your bug bounty costs and security ROI**, and why addressing recurring vulnerabilities matters for budget efficiency.
- **How to implement effective practices,** like retesting and clear communication, to minimize duplicate submissions and improve researcher engagement and program quality.

What are duplicate submissions?

Within the bug bounty industry, duplicate submissions refer to when two or more researchers report the same issue or vulnerability.

When a researcher, who works with a bug bounty platform, identifies a vulnerability, they submit a report to the platform, such as Intigriti, where it is reviewed. If the issue has already been reported, then it is marked as a duplicate.

Observing duplicates also shows where researchers are finding the same bug, which can indicate that the discoverability of a bug is higher and, therefore, could be a key indicator to add more priority to address the observed issue.

Sometimes, a duplicate can be marked as an 'accepted duplicate' to acknowledge that, while someone else reported the vulnerability first, the bug is valid and contributes to identifying a real vulnerability in the system, program, or environment.

> **"In general, submissions can be marked as duplicates if they have the same underlying root cause in the code. When in doubt, ask yourself whether the fix for the first report would have fixed the other report as well. If two fixes have to be applied, for example, on two different endpoints, the submission would not be considered duplicate as one fix would not prevent the second vulnerability from being found."**
>
> **Inti De Ceukelaire, Chief Hacker Officer, Intigriti**

Read 'Duplicate, related, or known vulnerability reports' for more research tips on identifying duplicates.

What’s the difference between a duplicate and a repeat submission?

As explored, a duplicate submission is when a hacker reports a vulnerability, but it's already been found, and is still being fixed, or is going through the process of being remedied. These are marked as Dupes and aren't rewarded.

On the other hand, a repeat submission is when a hacker has submitted a request. This submission has been fixed, but another submission is made for the same vulnerability. This signifies that the vulnerability was not fixed, or that it was broken again.

Here are two examples of repeat submissions:

1. The IT security team has informed the development team to fix the reported vulnerability. The workflow ticket is closed. But it turns out the deployment hasn't fixed the issue. A little while later, a hacker exploits the vulnerability again.

2. The deployment fixes the reported issue, but another release further down the line opens the risk again. This is observed particularly in larger organizations that have many releases a week. Here, it can be harder to ensure that the same vulnerabilities occur again, let alone track when they happen.

What is the financial impact of duplicate submissions?

A significant cost to organizations is potential payouts for multiple accepted repeats and duplicates. If multiple researchers all submit the same issue within the same timeframe, it can lead to multiple payouts for the same, single vulnerability, which can lead to frustration.

> **“Our recent analysis found that an average of 3% of a program's reported vulnerabilities had been previously addressed but have since resurfaced. This is costing companies and leaving the risk open to malicious hacks. We've been working with our researcher community and customers to increase retesting adoption so that our customers can have more trust in the security coverage and that vulnerabilities do not recur.”**
>
> **Greg Jenkins, Head of Product, Intigrit**

Implications of duplicate submissions for researchers

Not only do duplications cause frustration to businesses, but researchers can equally be discouraged when a submission is marked as a duplicate without explanation.

> **“Marking submissions as duplicates without the proper explanation or reasoning behind it may cause researchers to move on to another program. Being fair and communicating openly with the researchers will have a positive impact on your program in the long run.”**
>
> **Inti De Ceukelaire, Chief Hacking Officer, Intigriti**

How does the Intigriti platform reduce duplicate submissions and improve Return on Security Investment (ROSI)?

Using their latest Dedupe AI model, Intigriti analysed the number of submission dupes of reports that had been closed and presumably fixed. The idea was to see how many submissions were closed but have either not been fixed, or the vulnerability had reoccurred.

This opens the potential for retesting.

A submission retest refers to the process of evaluating a previously reported vulnerability to determine if it has been successfully mitigated and/or resolved. Retesting is not unique to Intigriti, but the team has done some analysis that shows, on average, 3% of submissions (and in some instances 8%) are on vulnerabilities that have reappeared, which can get expensive.

Retest doesn't provide a guarantee, but it helps ensure you've got a security process where vulnerabilities aren't recurring. Because, after all, it's really hard to continually monitor all the releases being done across a company.

> **"Vulnerabilities will recur, due to the pressures on companies to develop and innovate at pace and stay competitive. Retesting enables great bounty efficiency by reducing the cost of recurring vulnerabilities, provides the initial hacker additional low-effort rewards for retesting, and ensures ongoing assurance on vulnerabilities."**
>
> **Greg Jenkins, Head of Product, Intigriti**

Retesting is conducted completely at the researcher's discretion, and usually, a small bonus is provided for validating a fix once it is highlighted. Currently, almost 95% of all retest requests have been completed.

Next steps for enhanced bug bounty programs

With advancements in AI technology, bug bounty programs will be able to flag vulnerabilities that reappear and prompt customers to switch on recurring retesting while they investigate.

> **"The best resource on your program is to have a good set of loyal researchers who come back time and time again and discover new, more complex issues."**
>
> **Inti De Ceukelaire, Chief Hacker Officer, Intigriti**

If you're deploying a fix but don't have the capacity, expertise, or tools to retest it, Intigriti can help. Request a retest from the researcher, who will check if the vulnerability is still reproducible and resolved. Read more about this here.

For any bug bounty questions, contact Intigriti to speak with a member of the team.

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.