



How to appeal a bug bounty submission

BY AYOUB · JULY 30, 2026

 **Want to read the latest version? Visit the link below:**

<https://www.intigriti.com/researchers/blog/hacking-tools/how-to-appeal-a-bug-bounty-submission>

Bug bounty is a collaborative process that involves multiple parties, including the security researcher, triage team, and the affected organization managing the bug bounty program. While the vast majority of submissions are handled correctly, there are exceptional instances in which reports are mishandled, closed incorrectly, downgraded in severity, or left unresolved for extended periods. When this happens, knowing how to respond professionally and effectively can make the difference between receiving the appropriate attention to your case and having your appeal go unresolved.

In this article, we cover the most common scenarios where bug bounty reports are incorrectly handled and walk you through how to appeal these decisions through the proper channels. We also highlight common mistakes researchers make during this process, such as unauthorized public disclosures, and explain why these often do more harm than good.

Let's dive in!

Intigriti is researcher-centric!

The researcher community is at the core of everything we do, and your efforts are always acknowledged and valued. If something goes wrong with the handling of your report, and you're in the right, we'll stand behind you to ensure a fair resolution. That's exactly why we have an appeal process in place.

Why a mediation process?

A mediation, or an appeal process, is a structured way for security researchers to dispute how their submission was handled when they believe a mistake was made. Whether your report was incorrectly closed, downgraded in severity, or left unresolved for an extended period, the mediation process exists to ensure that every submission receives a fair and accurate assessment.

This process can be useful in several scenarios, such as when the triage team closes your report due to insufficient context, when the respective company handling the bug bounty program incorrectly handles your submission, when the severity of your finding is lowered without clear justification, or when your report remains pending without resolution or payment for an extended period of time.

Having a formal mediation process in place is essential to maintaining a standard policy between all parties involved. It ensures that researchers are always treated fairly, that valid security findings are never overlooked, and that companies receive the security value they initially signed up for.

The importance of an appeal or mediation process

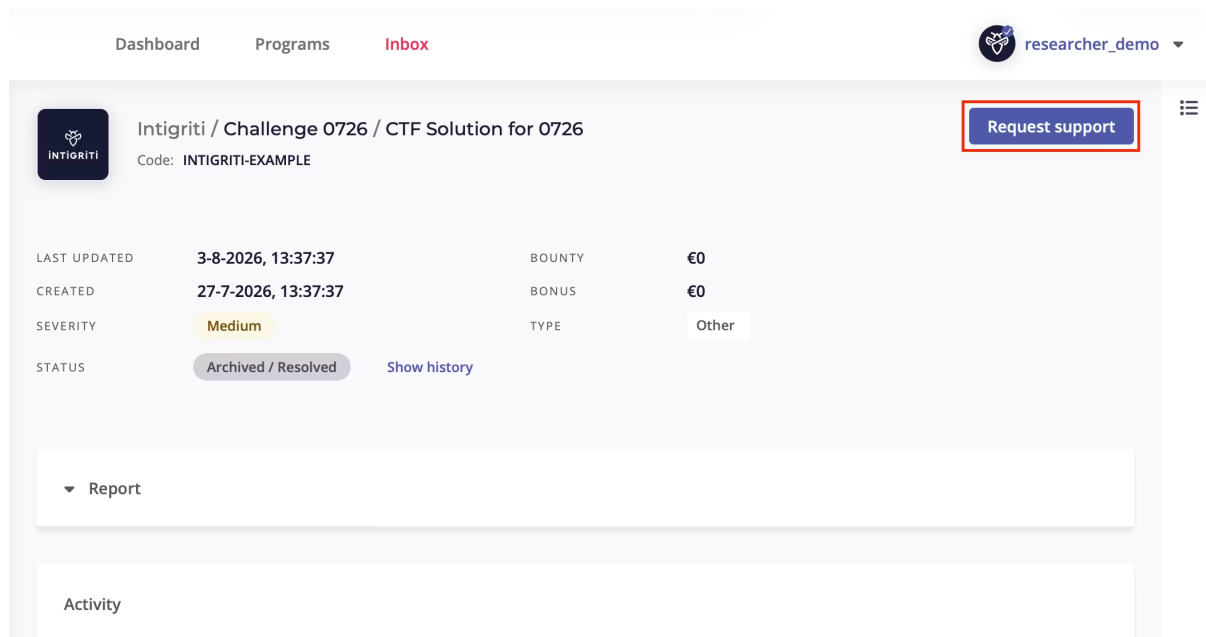
Without a formal mediation or an appeal process, valid security findings could go unrecognized, ultimately impacting both the researcher's efforts and the organization's security posture. Our appeal process is designed to avoid both of these negative outcomes.

How and when to appeal

Requesting mediation on Intigriti is straightforward. Under each submission, you'll find a Request support button that lets you contact our support team directly. Using this button also ensures we can look into your report immediately and gather the necessary context.

Aside from the Request Support option, you may also leave a comment on your report by tagging a member of the triage team for less urgent cases, or if you require more feedback on how or why your submission was handled.

Once your request is submitted, an Intigriti team member will acknowledge it and open a formal mediation case on your behalf, usually within two working days.



The screenshot shows the Intigriti dashboard interface. At the top, there are navigation tabs: 'Dashboard', 'Programs', and 'Inbox' (which is highlighted in red). On the right, there is a user profile icon and the name 'researcher_demo'. Below the navigation bar, the main content area displays details for a challenge submission. The title is 'Intigriti / Challenge 0726 / CTF Solution for 0726' with a code 'INTIGRITI-EXAMPLE'. A blue button labeled 'Request support' is highlighted with a red rectangle. Below this, there is a table of submission details: 'LAST UPDATED' (3-8-2026, 13:37:37), 'CREATED' (27-7-2026, 13:37:37), 'SEVERITY' (Medium), 'STATUS' (Archived / Resolved), 'BOUNTY' (€0), 'BONUS' (€0), and 'TYPE' (Other). A 'Show history' link is also present. Below the table, there is a 'Report' section and an 'Activity' section.

The 'Request support' button allows you to contact our support team directly

From there, a mediator outside of the triage team (to avoid conflict of interest) will investigate your case. Depending on your current situation, we always have a pathway to a fair resolution. Let's cover the most common ones.

Don't wait it out!

Please note that Intigriti is unable to provide mediation for reports that have been closed for over three (3) months. Ensure you initiate a mediation within the respective timeframe.

Learn more about our [mediation process](#).

Common mediation cases

Below, we've listed the most common issues that security researchers face and open a mediation case for. Let's go through them extensively.

1. Your report was incorrectly triaged

In exceptional cases, reports may be triaged incorrectly. This can happen for several reasons, such as insufficient context in the submission, which makes it difficult for the triager to fully assess the finding,

missing or invalid proofs of concept, speculative attack scenarios that don't clearly demonstrate a realistic security risk, or feedback requests that were not followed up on in time.

If you believe your report was incorrectly triaged, we recommend first reading the triager's or program member's feedback. Afterward, we advise you to review the program's out-of-scope list once more, as well as your own submission, to confirm that it includes sufficient context, a valid proof of concept, and clear reproduction steps. If, after reviewing both, you're still confident that your finding is valid, start by adding a comment under your report and tagging the triager who handled your submission. Further action from you at this stage will usually not be required, as our triagers actively monitor report comments and will revisit your case accordingly.

Alternatively, you can use the [Request Support](#) button to contact our support team. In your request, we recommend you include a clear explanation of why you believe the report was handled incorrectly. Throughout this process, always remain professional in your communication, as our triage and support teams are humans too. Additionally, avoid resorting to actions like disclosing full or partial report contents through external channels such as social media. Unauthorized disclosures not only violate Intigriti's [Community Code of Conduct](#), but may also result in sanctions, including a complete ban from the program.

2. Your report has an incorrect severity assigned

In some cases, you may disagree with the severity assigned to your submission as it may not accurately reflect the impact of your finding. This can occur when the report doesn't clearly articulate the full impact, when details around attack requirements are missing, or when the proof of concept doesn't demonstrate the maximum exploitable impact. Most programs follow either CVSS v3.1 or v4.0 in combination with [Intigriti's Triage Standards](#), while others further expand this by defining fixed severity ranges for certain vulnerability types within their program guidelines.

If you believe the severity was incorrectly assessed, start by reviewing the program's severity guidelines and our [Triage Standards](#). The fastest way to resolution is to leave a comment under your report referencing the specific CVSS metrics you believe were incorrectly evaluated, and always provide additional proven evidence that better demonstrates the full impact. Additionally, you can use the [Request Support](#) button to initiate the mediation process. Again, it is important to avoid disclosing the contents of reports on external social media for reasons outlined in our [Community Code of Conduct](#).

3. Your report has been pending for an extended period

Remediating a security vulnerability isn't always a straightforward process. Bugs that appear simple on the surface can take considerably longer to resolve than expected, as companies need to investigate the root cause, develop a fix, and validate it, all without disrupting existing functionality. Programs also have to prioritize reports based on severity, meaning lower-severity findings may spend more time in a pending state than critical ones.

That said, you're not expected to wait indefinitely. As implied in our [Community Code of Conduct](#), report submitters may request a status update every thirty (30) days, even if no additional information can be shared yet. We do ask that you refrain from requesting additional updates before this period, as doing so can inadvertently cause further delays rather than speed up the process.

If your report has been sitting with no movement beyond what you'd reasonably expect, start by adding a comment to your submission to request a status update. If that doesn't move things forward, use the [Request Support](#) button to escalate your case and include a brief timeline of any communication that has already taken place. Additionally, it is important to avoid disclosing the contents of your report on external channels such as social media while your case is under review, as this violates the [Community Code of Conduct](#).

4. Your payout has not been processed

Unlike the other cases covered in this article, delayed payouts are generally not part of a formal mediation process. In most cases, the issue can be traced back to incorrect or incomplete payout settings in your profile. Before reaching out, we recommend double-checking that your payment details are correctly configured. If everything looks good on your end and your payout is still showing an 'Error' state, don't hesitate to contact our support team directly, and we'll help get it sorted.

What to avoid during a mediation process

While the mediation process exists to ensure a fair outcome for everyone involved, how you navigate yourself throughout it matters equally. Here are the most common mistakes researchers make during a mediation, and why you should avoid them.

1. Avoid disclosing report contents via external platforms

Maintaining confidentiality throughout the mediation process is a sign of professionalism, and we take it seriously at Intigriti. Sharing full or partial report contents on social media or any other external channel while your case is under review is a violation of our [Community Code of Conduct](#). It can actively work against you rather than help your case. If you're unsatisfied with how your report has been handled, we encourage you to trust the process and work through the proper channels.

2. Avoid repeatedly requesting updates

We understand that waiting on a report can be frustrating, especially when you're confident in your findings. However, sending repeated follow-ups before the minimum reasonable timeframe has passed doesn't speed up the process, it can actually slow things down for everyone involved. As covered earlier, you're welcome to request a status update every thirty (30) days, and our triage and support teams will always get back to you within a reasonable time. Trusting that timeline goes a long way in keeping the process smooth for both sides.

3. Avoid requesting a mediation before reviewing your submission

Before escalating, start by carefully reading the triager's or program's feedback on your report, the closure reason in particular can tell you a lot. In many cases, what appears to be an incorrect triage decision can actually be traced back to missing or unclear information in the original report. With that feedback in mind, take a step back and review your own submission with fresh eyes, checking whether it includes sufficient context, a valid proof of concept, and clear reproduction steps. Taking this extra step before opening a mediation request not only saves time, but also strengthens your position if escalation is genuinely warranted.

4. Avoiding escalation outside of Intigriti

Before submitting a formal mediation request, always try to resolve the issue by placing a comment under your report and tagging the triager who handled your submission. In many cases, a direct conversation is all it takes to clear up a misunderstanding. If that doesn't lead to a resolution, the Request Support button is the right next step.

Raising your concerns on third-party platforms or community forums before exhausting the proper channels is not the right approach and is unlikely to lead to a better outcome. All mediation processes must be initiated through Intigriti's platform, where we can properly investigate your case and work towards a fair resolution.

Conclusion

Navigating a dispute over a bug bounty submission can be frustrating, but having a clear, structured process in place makes all the difference. In this article, we've covered the most common scenarios where reports are mishandled, how to appeal them through the proper channels, and what to avoid during the process to ensure the best possible outcome for your case.

So, you've just learned something new about escalating your bug bounty submissions... Right now, it's time to put your skills to the test! You can start by practicing on vulnerable labs and CTFs or... browse through our [70+ public bug bounty programs on Intigriti](#), and who knows, maybe earn a bounty on your next submission!



AUTHOR

Ayoub

Senior security content developer

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com