How should I scope third-party assets in my bug bounty program?

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

What you will learn

- **How to responsibly identify and categorize third-party assets** so you understand which external services can and should be included in your bug bounty scope.
- **How to set clear scope policies with permissions and exclusions** that protect your organization and researchers from legal and operational risks when testing third-party components.
- **How to maintain and adjust third-party asset scope over time** using best practices such as quarterly reviews, explicit authorisations, and impact-based severity evaluation.

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 frequently 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 'What is the pattern that can be expected after going public with a bug bounty program?' and 'How to attract security researchers to test on my bug bounty program?'

In today's blog, we take a look at how to responsibly scope third-party assets in your bug bounty program.

First, check what constitutes a third-party asset

Third-party assets refer to any software, systems, or services that are not fully owned or operated by your company. They can include SaaS tools, CDN services, hosted subdomains, and code libraries and integrations.

Not only can they be legally sensitive but, from an operational standpoint, increasingly complex. Testing assets you don't control, including many third-party services, can lead to legal complications for both your organization and the researchers involved.

'Active testing on unauthorized testing scope exposes the tester to legal risks.'– Intigriti Triage Standards

Even if assets are branded or hosted under your domain, it does not necessarily mean they are yours to assess.

> **“Consider if you actually WANT to put third-party elements within scope. On the one hand, you are not responsible nor able to fix bugs in their systems. So aside from viewing the reports and gaining visibility into potential vulnerabilities, there is not much you can do with these reports apart from encourage the vendor to fix them themselves. On the other hand, knowledge is power, and if you are aware of a bug that might pose a risk, you can make the vendor aware. They may act on it, they may not, but you can also then put in place additional steps to your own security, to safeguard against potential vulnerabilities you are seeing within the supply chain.**
>
> **Of course, the above goes for vulnerabilities in the third-party software; security risks can also arise from misconfigurations in this software. In cases where you administer this third-party software and are responsible for any misconfigurations, having hackers look at these assets is, of course, extremely valuable, because these misconfigurations are something you can resolve without having to rely on the vendor to make changes. ”**
>
> **Lennaert Oudshoorn, Head of Triage, Intigriti**

What to include and exclude in your scope

If, after analysing the pros and cons, you decide you want to allow testing of a third-party asset, you must get written authorization from the third-party, and you must verify if the vendor has a public BB or VDP of its own.

Vendor awareness, transparency, and collaboration are key.

'Vulnerabilities in on-premises third-party plugins, libraries, dependencies or software will always be forwarded to program owners. Bounty eligibility will depend on vendor awareness.' – Intigriti Triage Standards

In your program policy, create a clear section to specify what assets **are in** and **out of scope**, and include third-party assets that you have permission to test, as well as any owned subdomains that point towards external services.

- Do not include any third-party platforms unless you have explicit authorization to scope.
- Do not scope tools that fall under another company's bug bounty program.

For researchers, vulnerabilities that are found in elements or functions that are listed as out of scope are not considered for assessment or reward.

In addition, vulnerabilities found in third-party components will be assessed based on their impact on the overall system.

‘The severity will consider whether the third-party component is critical to the system and if the vulnerability could be exploited in a meaningful way. If a vulnerability is found by a researcher in a third-party component, the finder should always inform the owner or vendor of the vulnerable component prior to reporting it to their users.’

Vulnerabilities found in third-party cloud-hosted solutions, including SaaS or PaaS, should be reported to the party responsible for implementing the fix, and will be treated as out of scope unless the third-party is explicitly mentioned in the scope.

Read more on Intigriti Triage Standards here.

Summary of best practices to implement

1. Always gain permission from the vendor before including any third-party assets.
2. Define an in-scope and an out-of-scope policy that is clear to all.
3. Use labels to clearly define asset limitations.
4. Review third-party usage quarterly and adjust your scope to reflect any changes.

Next steps to enhance your bug bounty journey

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.