What is a bug bounty program? A guide for businesses

BY ANNA HAMMOND · SEPTEMBER 24, 2024 · LAST UPDATED ON MARCH 25, 2025

Bug bounty programs have proven to be an effective strategy for companies looking to proactively enhance their security posture. As a result, more and more organizations are investing in them, including major global brands such as Coca Cola, Microsoft, Ubisoft, and Nestlé.

In this guide, we'll provide a comprehensive overview of bug bounty programs for businesses. We'll answer key questions such as "What is a bug bounty program?" and "What are bounties?", helping you understand how these initiatives can be a valuable part of your cybersecurity strategy.

What is a bug bounty program?

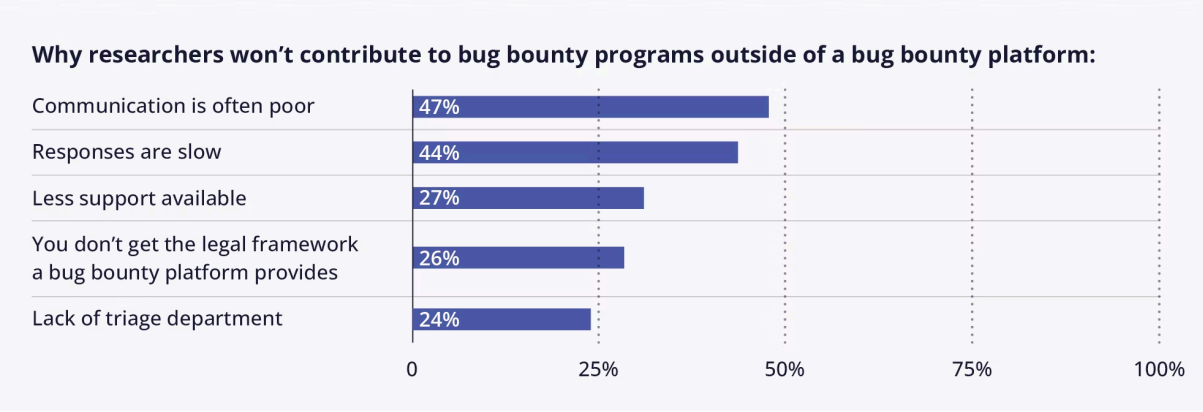
Bug bounty programs reward skilled security researchers (ethical hackers) for identifying and reporting vulnerabilities, tapping into the collective expertise of the global security community. By leveraging these insights, businesses can significantly strengthen their defenses and stay one step ahead of potential breaches.

Bug bounty programs are beneficial because they provide access to a larger pool of talent than would be available internally, and they do so in a cost-effective manner. By crowdsourcing cybersecurity, organizations can identify and fix potential security issues before they can be exploited maliciously, thus maintaining the trust of their users and protecting their own data and systems. This approach not only helps in fortifying security but also promotes a collaborative relationship between companies and the cybersecurity community.

What is a bug bounty platform?

A bug bounty platform is a centralized online hub where businesses can connect with security researchers to identify and report vulnerabilities in their software or systems. These platforms manage the process from submission to resolution, including triage, which involves evaluating and prioritizing reported vulnerabilities based on their severity and potential impact. This streamlined approach helps ensure that security issues are addressed promptly and efficiently.

According to Intigriti's Ethical Hacker Insights Report 2024, 40% of security researchers won't participate in a bug bounty program unless it's hosted on a bug bounty platform.

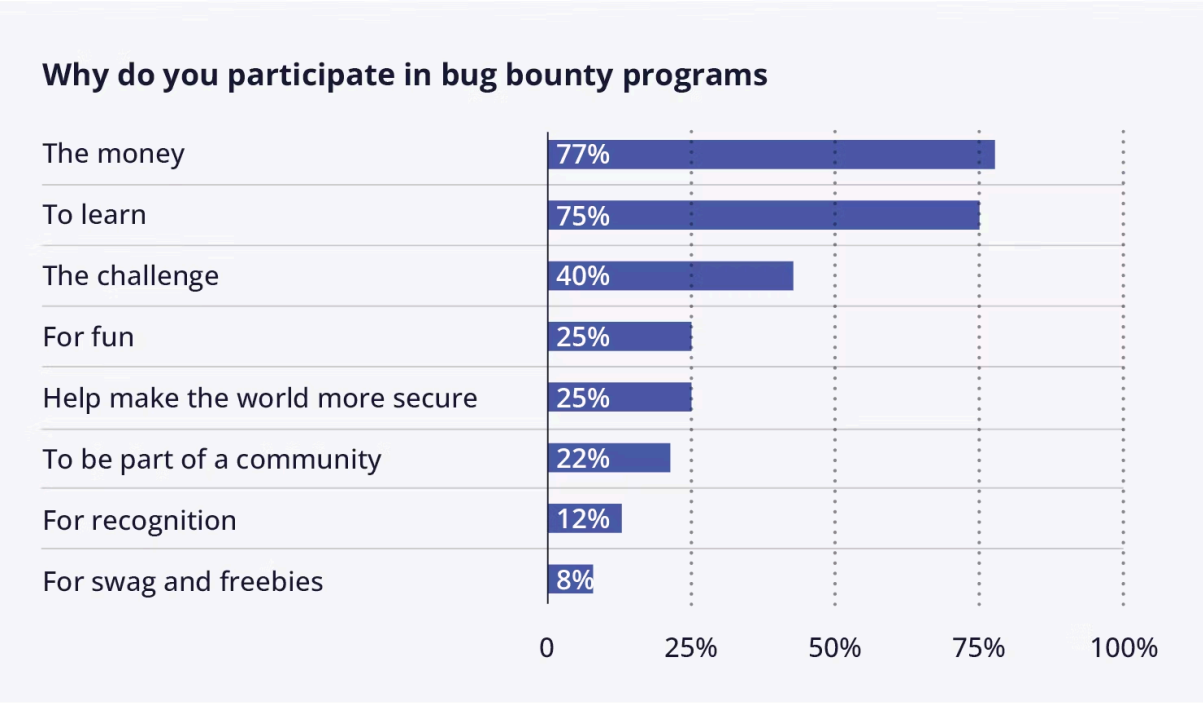


Survey respondents could select more than one answer

The top reasons for avoiding programs outside of bug bounty platforms include inadequate communication (47%) and delayed responses from organizations (44%). Insufficient support (27%), an inadequate legal framework (26%), and a lack of triage (24%) also contribute to their reluctance.

What is a bug bounty?

A bug bounty is the reward offered by companies to individuals who identify and report bugs or vulnerabilities in their software or systems. These rewards, typically monetary, vary in amount based on the severity and complexity of the identified vulnerability. Year after year, Intigriti polls have demonstrated that earning potential is the biggest motivator for ethical hackers to participate in programs.



Survey respondents could select more than one answer

This system not only enhances security but also fosters a collaborative relationship between businesses and the researcher community, promoting continuous improvement in vulnerability discovery. Unlike

pentesters, who are paid for their time regardless of findings, bug bounties incentivize security researchers and ethical hackers to proactively search for and disclose security weaknesses.

How do bug bounty programs work?

Bug bounty programs operate on a simple premise: when a security researcher discovers a flaw in the software, they report it to the organization in a responsible manner, rather than exploiting it or making it public. In return, if the bug is validated by the organization, the reporter receives a bounty.

Here's a typical timeline of a bug bounty program from launch:

Program launch

A company starts by deciding what type of bug bounty program suits their needs. With Intigriti, this looks like:

- **Private:** Only visible to invited security researchers.
- **Application:** Researchers must apply to participate and can only do so once accepted.
- **Registered:** Only registered researchers on the platform can see the full program details and submit reports.
- **Public:** Anyone can see the program but must still register to participate.

The company will then define the scope of their bug bounty program. This includes specifying which of their products or services are eligible for testing, the types of vulnerabilities they are interested in, and the rules for engagement. This information is crucial to ensure that ethical hackers know their boundaries and focus areas.

Vulnerability discovery

Security researchers, also known as ethical hackers, then begin their search for bugs within the defined scope. These individuals use their skills to identify security weaknesses that could potentially be exploited by malicious attackers.

Reporting

Once a vulnerability is discovered, the researcher reports it to the company through a secure channel, like Intigriti's platform. The report includes detailed information about the vulnerability, how it can be exploited, and sometimes suggestions for mitigation. This allows the company to understand and verify the issue.

Verification and validation

After going through the triage process, the company reviews the submission to verify its validity and assess its severity based on the potential impact and exploitability. This step is crucial as it determines whether the bug qualifies for a bounty and how much the bounty will be.

Reward issuance

If the report is accepted, the researcher receives a reward. The bounty amount usually correlates with the severity and complexity of the vulnerability.

Resolution and disclosure

The company works to resolve the issue and may later publicly disclose the vulnerability once it is fixed, often crediting the researcher who discovered it. This not only helps to maintain transparency but also enhances the reputation of the researcher in the cybersecurity community.

Through this process, bug bounties create a win-win situation whereby companies enhance their security, while researchers gain recognition and compensation for their work.

Bug bounty examples

TrueLayer is a particularly noteworthy bug bounty example, and 18 months after launching their program, the open banking payments network published an insightful account of their journey.

Lee Boynton, Senior Cloud Security Engineer at TrueLayer, shared: "In our first year, there was one submission that stands out as a really good find, one that should make not just TrueLayer more secure, but can also help protect other websites."

The issue, identified by a researcher known as @redge4r, highlighted the advantages of incorporating bonuses into a bug bounty program. TrueLayer awarded a bounty for @redge4r's discovery but also added a bonus since the report pertained to a newly launched feature. This marked the first instance they used a bonus to direct attention to a specific area of their services, a strategy that proved to be effective.

In September 2022, TrueLayer was alerted to a Multi-Factor Authentication (MFA) bypass issue in the TrueLayer Console via their bug bounty program. MFA is crucial as it adds an extra layer of security to customer accounts, helping to mitigate the risk of compromised credentials.

The security teams at both Intigriti and TrueLayer triaged the report within one day, despite the involvement of some intricate technical steps. Tools like Burp Suite, which intercept HTTP traffic and allow for detailed inspection of requests, played a crucial role in reproducing the issue. Their investigation revealed that the problem originated from a third-party provider. TrueLayer worked collaboratively with this provider to address the issue, and it has since been resolved.

The result of this bug bounty report strengthened the security for TrueLayer but also for other customers of the third-party provider, creating a safer environment for all involved.

How to build a bug bounty program

A bug bounty program is more than a vulnerability discovery tool; it thoroughly tests an organization's security posture, ensuring it is strong, agile, and effective against emerging cyber threats.

Intigriti has helped launch over 400 programs on its platform for organizations across the globe, helping them to proactively address vulnerabilities before they can be exploited by cybercriminals. To speak to a member of the team about building and launching a successful bug bounty program, get in touch today.

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com