# Uphold celebrates four years with Intigriti

BY INTIGRITI · OCTOBER 21, 2024 · LAST UPDATED ON MARCH 6, 2025

Intigriti is thrilled to announce that Uphold, the leading multi-asset digital money platform, is celebrating four years of its bug bounty program with Intigriti. To mark this milestone, Intigriti sat down with Pedro Queirós, Uphold's VP of Cyber Security, to discuss the impact the bug bounty program has had on the organization's cybersecurity and resilience. Pedro also shares insights into the strategies that have led to long-term engagement with the researcher community and how the program is set to evolve over time.

## Intigriti: Welcome, Pedro! Tell us about Uphold. How did it start as a company and what is its current mission?

**Pedro:** Thanks for having me! Uphold is a multi-asset digital money platform founded in 2013 with the vision of creating a more accessible and equitable financial system. We started as a company committed to democratizing access to financial services by allowing users to easily buy, hold, convert, and transact across a range of assets—including cryptocurrencies, fiat currencies, and precious metals—all in one place. Our current mission is to empower people worldwide by providing a transparent, affordable, and user-friendly platform that breaks down the barriers to financial inclusion.

## Why did Uphold decide to start a bug bounty program?

Recognizing the paramount importance of security in the digital finance space, we initiated our bug bounty program to proactively identify and address potential vulnerabilities in our platform. While penetration tests are valuable, they are often static and limited to a specific point in time. With new threats and vulnerabilities emerging daily, it is crucial to engage a broad community of ethical hackers and researchers dedicated to continuously identifying potential risks within our ecosystem.

By collaborating with the global community of security researchers, we aimed to leverage their expertise to strengthen our platform's security posture. This initiative reflects our commitment to safeguarding our users' assets and maintaining their trust.

## What key changes or improvements have you made to the program over the past four years based on researcher feedback?

Over the past four years, we've continually refined our bug bounty program in response to invaluable feedback from the researcher community. Key improvements include expanding the scope of the program to cover new features and services, increasing reward tiers to better recognize significant findings, and streamlining our submission and response processes for faster resolution.

## What are some of the most impactful vulnerabilities that have been discovered through the program, and how have they influenced your security posture?

Through the program, researchers have uncovered some vulnerabilities related to misconfigurations in cloud and SaaS partners, security headers, API integrations, and data handling processes. These discoveries have been instrumental in allowing us to promptly address weaknesses before they can be exploited. As a result, we've implemented additional security checks, enhanced our software development processes, and improved our overall security infrastructure. These actions have elevated our ability to protect user data and assets.

## How has the scope of your bug bounty program expanded over the years, and are there any upcoming areas or products you plan to include?

Initially, we focused on our core platform but the scope of our bug bounty program has grown to include our mobile applications, API services, and newer product offerings. We continuously assess and expand the program to cover all facets of our ecosystem as it evolves. Looking ahead, we're planning to include upcoming products to ensure comprehensive security coverage.

## What strategies have helped maintain high engagement from researchers and foster long-term participation in the program?

Maintaining high engagement has been achieved by fostering a collaborative and rewarding environment for researchers. We offer competitive rewards, provide clear and detailed guidelines, and ensure prompt communication throughout the vulnerability assessment process. Recognizing and crediting researchers for their contributions has also been key to building strong, long-term relationships within the security community.

## How do you foresee the program evolving in the next few years, particularly in terms of scope, reward structure, or collaboration with the security community?

In the coming years, we anticipate further expanding the scope of our bug bounty program to include all new services and technologies we adopt. We plan to adjust our reward structure to stay competitive and to incentivize the discovery of more complex and impactful vulnerabilities. Additionally, we aim to deepen our collaboration with the security community by promoting events, workshops, and possibly mentorship programs to nurture new talent in the field.

## Anything else that you would like to share with the community?

To celebrate our bug bounty program hitting four years on Intigriti's platform, we're giving all valid submissions of medium and above an extra €1,000! This initiative will take place from **Monday, October 21st at 5 PM UTC to Friday, November 1st at 11:59 PM UTC**.

We want to extend our heartfelt gratitude to all the security researchers who have contributed to our bug bounty program. Your expertise and dedication are vital to our mission of providing a secure platform for our users. We encourage both seasoned and aspiring researchers to participate in our program and join us in our commitment to enhancing the security of the digital financial ecosystem.

Researchers can participate in Uphold's bug bounty program via Intigriti's platform. We look forward to receiving your submissions!