bugcrowd

CASE STUDY

Platform-powered bug bounty helps Wise innovate payment security

How the team discovered a critical vulnerability just 24 hours after launch

WISE

Industry:
Financial services technology

Founding date:
2011

Number of employees:
5000-10,000

Headquarters:
United Kingdom

Website:
wise.com

The situation

Wise, formally Transferwise, a global fintech company building the best ways to move money worldwide, needed to adapt its security processes from a traditional compliance-oriented penetration test model to something more innovative.

The challenge

Wise's use of traditional penetration testing solutions were not providing sufficient depth and breadth for their testing use cases. As Chief Information Security Officer Shan Lee explained, "We wanted to do something more focused around genuine security than just about checking a box for some audit. We needed a process that offers a more real-world approach."

As a result, Wise's journey to crowdsourced security began. Lee understands the power and value of the crowdsource model, stating, "I've always been a fan of the crowdsourced security model. I've had experience using this methodology in past roles and have seen the value and operational impact it can have on a security organization."

Key takeaways

Improved risk reduction

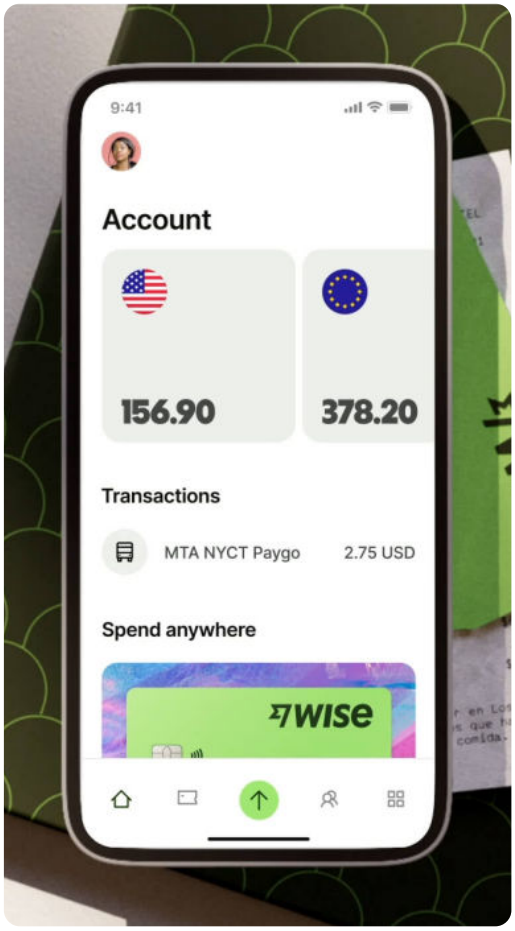
Expedited threat mitigation

More secure applications

The Bugcrowd solution

Having analyzed various crowdsourced security vendors, **Wise turned to Bugcrowd to help launch its first private bug bounty program.** Bugcrowd's program provided them with continual testing, greatly reducing risk and better mitigating threats. With its bug bounty program, Wise gained more insight into potential threats and vulnerabilities across its applications. This private program also introduced bug bunting to the company with a scope that would expand alongside their increasing operational bandwidth.

> **"The number of findings is a true measure of our maturity as a company. I want to get to a point in the not too distant future where I am showing a graph at every board meeting that shows a meager number of Bugcrowd findings and not for lack of attention, but due to our focus on enhancing our application security," Lee said.**



> The number of Bugcrowd findings is a true measure of our maturity as a company. I want to get to a point in the not too distant future where I am showing a graph at every board meeting that shows a meager number of Bugcrowd findings and not for lack of attention, but due to our focus on enhancing our application security.
>
> **Shan Lee, CISO, Wise**

The outcome

The private bug bounty program helped to streamline the vulnerability management lifecycle and its associated remediation workflows before going public, ensuring scalability of these newly found security efficiencies.

Within just 24 hours of launching the private program, Wise received its first valid 'P1 Business Critical' vulnerability. These rapid results highlight the risk reduction provided by the program, helping to keep threats like fraud and e-skimming at bay. Discovering a considerable threat so quickly proved the concept that crowdsourced security works.

> **As CISO Lee explained, "The finding we received would not have been discovered in a traditional penetration test, so by having a more expansive scope and the support from the crowd, we were able to focus on areas we didn't realize needed the attention."**

Over time, **Wise scaled its vulnerability management processes, allowing them to broaden the scope of its private program.** As the scope continued to expand, the program was at a point where it made sense to convert to a public program. With a public program, Wise opened the scope in a way that anyone from the Crowd could be activated. This allowed the security team to accept bug bounty submissions at a higher volume and velocity and has helped to standardize submissions for repeatability, while accelerating the vulnerability management lifecycle.

As Security Engineer Ando Roots described, "Over time, we were able to effectively address and manage the number of submissions we were receiving and now have developed a workflow that is scalable and efficient. It exemplifies our security maturity as a team and an organization."

Adopting crowdsourced security has transformed vulnerability management at Wise and helped to create a security-focused culture. With Bugcrowd, Wise can test and defend real-world scenarios using a crowd of ethical hackers to safeguard their customer experience.