bugcrowd

CASE STUDY

BUG BOUNTY | PEN TEST AS A SERVICE

Rapyd Takes Security to the Next Level with PTaaS and a Public Bug Bounty on the Bugcrowd Platform

Rapyd

- **Industry** FinTech
- **Founding Date** 2016
- **Website** Rapyd.net
- **# of Employees** 500+
- **Headquarters** London, UK

KEY TAKEAWAYS

- ✓ **15 Critical (P1 and P2) Vulnerabilities**
  Found Over the Past Year
- ✓ **Average Days-to-Fix Vulnerabilities is 18 Day**
  Compared to Industry Average of 31 Days
- ✓ **Public Program Successfully Planned and Launched**
  Including Implementing an Integrated Workflow

After switching to Bugcrowd, Rapyd securely and successfully launched an industry-leading public program.

The Situation

Rapyd is a cutting-edge FinTech leader focused on helping businesses create great commerce experiences anywhere. They develop technology designed to remove the back-end complexities of cross-border commerce while providing local payment expertise.

For about four years, Rapyd used crowdsourced security in various forms, including adopting HackerOne Bug Bounty. They also routinely performed traditional penetration testing.

The Challenge

As their organization grew, Rapyd wanted to step up their security posture by making security testing continuous. They have an interesting use case for crowdsourced security, since their core business is so API-focused. A thorough discovery of vulnerabilities in APIs requires specialized knowledge, skills, and experience.

Rapyd also needed help with security assessments during mergers and acquisitions, such as when creating asset inventories and understanding the attack surface risk involved.

The Bugcrowd Solution

About a year ago, Rapyd decided to turn to Bugcrowd to take their crowdsourced security programs to the next level. They started leveraging Penetration Testing as a Service and a private Bug Bounty program. The goal was to eventually launch a public program, which Rapyd did in six months.

“We quickly felt safe to take our program public with Bugcrowd. We value the way Bugcrowd finds the right hackers with the right expertise for our programs.”

—ACHIAD AVIVI
Applications Security, Rapyd

The Outcome

Rapyd is experiencing outstanding results with Bugcrowd. In this year alone, 15 critical vulnerabilities and almost 40 total vulnerabilities have been discovered. A key factor in taking their program public was preparing the right process. Rapyd wanted to be sure they had the right roadmap in place before launching, which they worked with Bugcrowd to build. The Rapyd team are currently working on integrating their bug bounty program with their SDLC and product security flow to allow for sustainable growth.

One reason for Rapyd’s success is how involved their team is. Their entire security team participates in the strategy and operations of their program with Bugcrowd. Their teamwork is also reflected in the success of the program. They’ve built workflows in Jira and Slack for tracking program findings and routing to the appropriate stakeholders. These integrations were key benefits for the team.

This dedication to the success of the program can be seen in Rapyd’s commitment to quickly remediating vulnerabilities. Rapyd’s average time-to-fix submissions is 18 days across all severity levels. The industry average is 31 days to fix, so it is clear that Rapyd’s security program is truly excelling in partnership with Bugcrowd.

Rapyd chose Bugcrowd in part because of the unique way Bugcrowd selects specialized hackers for engagements. Since their needs were very specific (for example, for API testing), they needed to connect with the right group of hackers with skill sets that matched their use case. **“Bugcrowd accommodates both hackers and organizations. By picking the right hackers for specific programs, it keeps researchers engaged,”** said Achiad Avivi, Applications Security, at Rapyd. Bugcrowd’s CrowdMatch technology, which enables precise crowd matching, allows organizations to connect with the right hackers at the right time, which was perfect for Rapyd’s needs.

Rapyd’s success can be considered impressive under any circumstance, and it’s important to note that they were achieving these amazing results all while undergoing a time of major growth and multiple acquisitions. By leveraging security testing through Bugcrowd during major acquisitions, they were able to understand a previously unknown attack surface.

“Bugcrowd is a win–win situation for hackers looking to make an impact on internet security while making money and for companies looking to improve their security by finding these security issues before they become bigger problems,” said Achiad Avivi.