



Financial services enterprise delivers secure Web3 wallet management with Bugcrowd

How a FinServ enterprise bolsters its API security measures, meets compliance requirements, and addresses vulnerabilities.

The situation

A French financial services enterprise (who wishes to remain anonymous) develops a secure wallet-as-a-service infrastructure in web3. Their API-first wallet management system makes it easy for organizations to provide access to all blockchains with a single integration.

As a provider of financial services infrastructure, API security is very important to the organization. In addition to regulatory compliance, continuous testing is required to ensure its APIs are free from vulnerabilities, hardened against attacks, and reliable under stress.

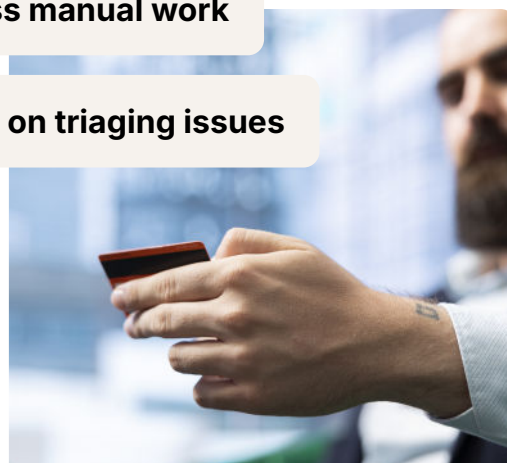
Since a secure API was so important to its platform, they decided to evaluate and purchase a dedicated solution for identifying API risk. Of particular importance was finding a solution that would minimize unnecessary noise and seamlessly integrate with their delivery pipelines, making API security easy to deliver at rapid speed.

Key takeaways

Prove SOC2 compliance with less manual work

Reduced time developers spend on triaging issues

Faster remediation





The challenge

The organization needed:

A specialized tool dedicated to API testing as part of a comprehensive security solution

To build robust security measures to prevent unauthorized financial access and potential vulnerabilities

A solution that seamlessly integrated into their system and offered a streamlined process for identifying real issues while minimizing unnecessary noise

To move fast and focus on real vulnerabilities

The solution and outcome

Bugcrowd's quick setup and noise-free results impressed the team when evaluating solutions.

Thanks to Bugcrowd's intelligent testing, the team is now confident that critical vulnerabilities are identified for rapid remediation.

The organization has integrated Bugcrowd with their OpenAPI spec. This combined with conducting regular scanning helps streamline its compliance reporting and allows the team to prove SOC2 compliance with less manual work.



Bugcrowd's built-in analysis and triage ensure that only real results are delivered, reducing the time developers spend on triaging issues. With Bugcrowd, the organization remediates faster and spends more time delivering features to their user base.