How Kuna works with hackers to enhance their security

HACKEN PROOF

One of the largest crypto exchanges in Eastern Europe, which launched the development of basic infrastructure for the innovative fintech-projects both in Ukraine and in foreign markets.

- **Product type:** Managed Bug Bounty
- **Start Date:** 21/01/2018
- **Reports submitted:** 84
- **Vulnerabilities resolved:** 24
- **Hackers participated:** 38

How Hackers Stole $1B From Cryptocurrency Exchanges In 2018

Due to the sharp rise in popularity of cryptocurrencies (i.e. high demand to trade crypto), we saw a sharp rise in the number of exchanges. From the point of view of cybercriminals, this was a perfect storm - you have entrepreneurs wanted to exploit the market opportunity, creating a large number of crypto exchanges, that are trading in assets which aren't controlled or governed by any institution. This meant that security was not the main priority for founders who were building exchanges. Hackers quickly recognized the lucrative opportunity to earn easy money by exploiting vulnerabilities in crypto wallet software and servers. It's no surprise that around **$1.1 billion** worth of cryptocurrency was stolen in 2018 alone.

Reducing Risk by Using Crowdsourced Security Testing

The security team at Kuna recognized early the need to get in front of potential security issues.

Let's hear directly from Roman Cherednik, CTO at KUNA Exchange:

1. How did you make the decision to start a bug bounty program?

We operate a platform that is extremely sensitive to vulnerabilities. Sometimes even a small mistake in implementation may cost a lot. So Bug Bounty program is an extra measure for us that improves our security by leveraging the community of white hackers.

2. Why did Kuna choose to host a managed bug bounty program with HackenProof? Why not just self-host and manage it by yourselves?
We tried. It appeared to be quite a time-consuming task to engage the engineering team to process and manage the Bug Bounty inbox. So we decided to use BugBounty-as-a-Service to delegate this task to HackenProof and let professionals process, triage and validate the incoming reports. They forward us the only requests that we need to focus on. As a bonus, the issues are now unified and go with precise reproduction steps using the terminology of our platform that we use ourselves.

3. How has launching a bug bounty program impacted Kuna's cybersecurity strategy?
We have already fixed multiple issues that white hackers reported to us and we expect this collaboration to expand further-going as we continuously update our platform with new integrations and features.

4. Any highlights of hacker interactions so far?
Probably, the ones that ask for money upfront :)

5. What advice would you give other organizations on launching their bug bounty program?
Just do it and it will pay off.

REACH OUT TO US TO LEARN MORE ABOUT RUNNING A MANAGED BUG BOUNTY PROGRAM

Contact Sales

About HackenProof

The HackenProof platform connects its customers with the global hacker community to uncover security issues in their products. By running custom-tailored bug bounty programs, HackenProof helps their customers significantly reduce the risk of losing their data to cybercriminals. HackenProof is a part of Hacken Ecosystem, with products fueling cybersecurity industry from all sides: bug bounty platform, crypto exchange analytical ranking platform, cybersecurity conference HackIT, and a cyber school. HackenProof is headquartered in Tallinn, Estonia.

HACKEN PROOF

sales@hacken.io