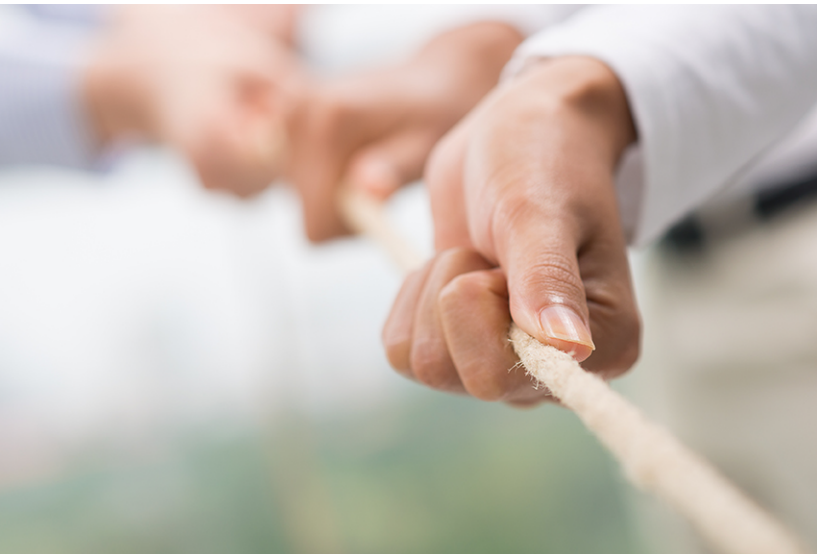
hackerone | BISHOP FOX | Case Study

Managed Security Through Collaboration



coinbase

By combining the HackerOne platform with Bishop Fox security consultants, Coinbase successfully implemented an effective bug bounty program to improve site security.

The task

Coinbase is the world's leading platform for buying and selling Bitcoin, a person-to-person digital currency. The Bitcoin network touches thousands of computers and millions of participants globally, which keeps the Coinbase platform diverse and driven. Security is extremely important for Coinbase in its mission to bring Bitcoin to the mainstream.

Founded in 2012, Coinbase focused on developing a solid security infrastructure, integrating security audits and penetration testing along the way. However, they wanted to take their security program to the next level — maximizing their effort, minimizing their time, and focusing on producing a quality product.

All they needed was the right solution.

A collective approach

Operating a bug bounty program was the natural next step in securing their service, but managing a new initiative within their already busy security program would take away time from progress on other projects.

Enter HackerOne and Bishop Fox.

Coinbase adopted the HackerOne platform to access top security researchers, manage vulnerability reports, and pay bounties; they engaged Bishop Fox to help oversee and validate the inbound report queue.

HackerOne provides a vulnerability coordination platform and workflow for interacting with and rewarding researchers. Their unique service introduced Coinbase to over 2,000 hackers within the HackerOne network, who increased the number of useful, valid vulnerabilities reported. Repeat reporters become an extension of the security team, often helping with remediation as they tried to hack the same issues after patches were released. HackerOne allowed Coinbase, Bishop Fox, and researchers to directly communicate and validate reports. HackerOne integration with common development issue trackers, such as JIRA and Phabricator, simplified Coinbase's remediation process for valid reports.

The Bishop Fox team of security experts have been managing bounty programs since 2011, before bug bounty became an established security norm. With bug bounty hall of famers on their team, they provide big picture insight into common patterns of reported bugs and have experience from both sides of the hunt.

Bishop Fox applied their security expertise and experience to evaluate, flag, and prioritize the most important vulnerabilities to Coinbase. "We provided initial triage and assessment of incoming bug reports, passing on the most useful to Coinbase's security team. We found the real threats and filtered out the fakes so Coinbase could focus on making improvements instead of validating findings," said a Bishop Fox security analyst.

Bishop Fox's curated lists of submissions increased the signal-to-noise ratio, reducing the amount of time that the Coinbase team had to spend on validation and remediation.

Proven results

"We strive to create an environment where our security team feels safe and doesn't worry about causing a problem or opening a hole. With a bug bounty program, the team is strengthened through continuous feedback and testing — not a single security checkpoint. As a result, they are able to work faster and be more responsive," said a Coinbase security engineer.

Since launching their Bug Bounty program, Coinbase has rewarded an average of two researchers a week.

HackerOne's practical and intuitive service combined with Bishop Fox's security smarts eliminated the stress of implementing a bug bounty program.

"With Bishop Fox managing our queue, our engineers have more time to focus on our core product. Hiring and optimizing time is a challenge in this industry. Bishop Fox helps improve the efficiency of HackerOne's already excellent service and focus of our team," said a Coinbase security engineer.

Coinbase realized that all companies can benefit from managing a bug bounty program – no matter the size or industry, stating, "We prefer to work with companies who have a bug bounty program. It ensures that a certain level of security is maintained. In a perfect world, bug bounty programs would be the norm. A product launch would automatically mean that security was considered.

"Audits are static. A bug bounty program means eyes are always on your product, seeking vulnerabilities." said a Coinbase engineer. "We want to see a world where a launch means something regarding security. Buyers banding together to require minimum mandatory bug bounties would send a signal to new companies that they have to secure their users before they can make a sale."

The combination of Bishop Fox expertise and the HackerOne platform simplified the act of receiving, confirming, and responding to reported vulnerabilities and provided a practical solution for Coinbase and its vendors to keep their users safe.

