bugcrowd

Evaluating Your Security Posture:

ATLASSIAN'S FULLY MANAGED BUG BOUNTY

PROGRAM DETAILS

Launched: November 2016

Type: Bug Bounty (Private to Public)

Scope: Atlassian web properties, JIRA and Confluence REST APIs, Bitbucket Atlassian

Rewards: $100 – $3,000 per vulnerability

Security at Atlassian

Collaboration is core to Atlassian, exemplified in everything from its products to the company culture. Teams at more than 107,000 companies, large and small - including Citigroup, eBay, Coca-Cola, Visa, BMW and NASA - rely on Atlassian for project tracking, content creation and sharing, real-time communication and service management products in the cloud.

With collaboration, comes trust. And trust begins with security. At Atlassian, security is baked into the product development lifecycle. Having secure and trustworthy software is of utmost importance to Atlassian's business and customers. The entire team of security engineers is dedicated to building more secure products. Building and maintaining products that keep their customers safe is a team effort.

Seizing the Opportunity

For a number of years, Atlassian was running its own incentivized vulnerability reporting program. While very successful, the team was finding that it was too hard to manage the sheer number and varying quality of incoming reports.

The global security community is becoming more familiar with the bug bounty model and more creative in finding flaws. New types of systems are emerging, presenting additional opportunity for even more security concerns. Even with a fully dedicated security team, the Atlassian security team wants to invest in building more secure products rather than triaging and validating incoming vulnerability findings. For Atlassian, it became apparent that the balance between improving security and handling incoming vulnerability reports wasn't quite right – paired with the increased need for quicktime to action – which highlighted the need for managed bug bounty programs.

ATLASSIAN

Implementing a fully managed bug bounty program has empowered Atlassian, instilled confidence in the security of their products, and provided unmatched ROI.

Daniel Grzelak, Head of Security

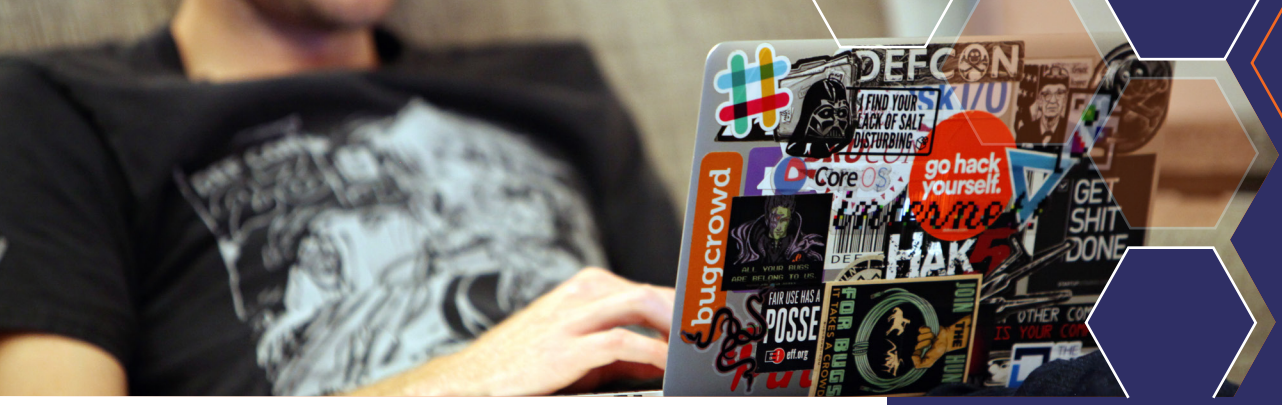
"Our traditional application security practice produces great results early in the lifecycle and deep in our services, but the breadth and depth of post-implementation assurance provided by the crowd really completes the secure development lifecycle. Multiplying the specialization of a single bounty hunter by the size of the crowd creates a capability that just can't be replicated by individual organizations."

135
TOTAL VALID SUBMISSIONS

2.82*
AVERAGE VULNERABILITY PRIORITY

$82,550
TOTAL PAID OUT

*average priority is based off a scale of 1, being highest, to 5 being the lowest.



Program Management Relies on Collaboration

Atlassian believes that collaboration is fundamental to any software or business team's success, and leveraging the power of the crowd for security testing is a natural extension of this. Moving away from the self-managed model, Atlassian turned to Bugcrowd to leverage its fully managed bug bounty solutions, as an opportunity to offload much of that work and focus on more sensitive areas within their environment.

Atlassian launched private bug bounties with Bugcrowd in November 2016, and in July 2017, launched its first public bug bounty. Implementing a fully managed bug bounty program has helped Atlassian uncover vulnerabilities faster than ever, freeing up their security team to allocate more time to finding anti-patterns and implementing broad mitigations.

Bug Bounty Program Results

With Bugcrowd, provider of crowdsourced security testing, Atlassian's security team adds tens of thousands external cybersecurity researchers. This highly capable community is constantly testing Atlassian's products, using well-defined guidelines and a safe testing ground to perform their research. Their results are shared through a standardized reporting platform, and Bugcrowd's application security engineering team handles the initial triaging and vulnerability validation.

Over the course of their programs, they have been able to maintain strong engagement across targets.

Working with Bugcrowd - Measuring Results

Bugcrowd architects security expertise into the design, support and management of every program. Atlassian leavered this experience while tapping the world's best security researcher community to help keep their products and customers secure. By demonstrating their security posture, Atlassian is not only instilling confidence in the security of their products, they're upholding one of the company's core values: Openness, and demonstrating a position of true leadership when it comes to the security of their customers.

Atlassian's success is indicative of their commitment to product security and their bug bounty program has enabled them to measure their application security program in a way they were previously unable to. What does the future hold?

Improve SDL Coverage

The breadth and depth of post implementation assurance provided by the crowd completes Atlassian's secure development lifecycle.

Strengthen Security Posture

The economics of bug bounty programs with Bugcrowd allow Atlassian to measure how confident they are in their security posture based on their payout amounts.

> "The effect and the impact of an external person reporting a vulnerability or lots of vulnerabilities is very different to your own internal AppSec team reporting some vulnerabilities. The impact is just different, and everyone around an organization looks at this with a very different set of eyes when these things get reported externally."

Daniel Grzelak, Head of Security

Learn why hundreds of companies have turned to Bugcrowd.

www.bugcrowd.com/get-started

Bugcrowd.com
Sales@Bugcrowd.com | (888) 361-9734