bugcrowd

OUTREACH.IO STREAMLINES VULNERABILITY DATA WITH BUGCROWD'S JIRA INTEGRATION

Bugcrowd's bi-directional Jira integration helps get the right vulnerability data to the right developer team

Security at Outreach.io

Outreach is a leading sales engagement platform, that automates and prioritizes customer touch points throughout the customer lifecycle, resulting in increased productivity for revenue teams. Thousands of customers rely on Outreach to increase efficiency and effectiveness of reps, drive collaboration between sales, marketing, and success, and deliver revenue lift.

At Outreach, users' security is paramount. The company takes every precaution to protect their information so that they can focus on bringing innovations to market through their products and services. Not only does Outreach build world-class features, but it also has a laser-focus on building a secure engagement platform to house customer data.

Outreach runs a private bug bounty program with Bugcrowd, as well as on-demand programs to ensure the company gets as much security vulnerability coverage as possible. To ensure those vulnerabilities get communicated to the right stakeholders at the right time with the right instructions, Outreach benefits from Bugcrowd's bi-directional Jira integration.

Seizing the Opportunity

Outreach does a number of things to help secure its platform. The company starts with mandatory peer reviews and enforces that through its repositories. The developers don't get to check-in code until it's been reviewed and signed off by a peer. Outreach also runs a couple of static analysis tools as part of its regular task pass, so if it fails anything from performance, compatibility, insecurity, it's the developer's job to go and fix that problem.

Outreach leverages Bugcrowd as the last line of defense. The company runs a successful, continuous private bug bounty program with Bugcrowd, as well as on-demand programs when there is a big new feature release upcoming. Especially when a new feature needs a lot of customer input or is manipulating customer data, the on-demand bug bounty program helps Outreach uncover a lot of great vulnerabilities that they can go back and fix before putting it into production for customers.

Integrating Bug Bounty Findings into SDLC with Jira

Outreach understands the need for crowdsourced security for application testing, but the feature teams are broken out into what they call tribes, made up of product and engineering. These teams own different feature sets and customer pain points end-to-end, which gives them a sense of ownership over that part of the Outreach platform, but also gives them a sense of responsibility when things are going wrong with that part of the platform.

Outreach

About the Outreach Program

Launched: February 2017

Type: Private bug bounty

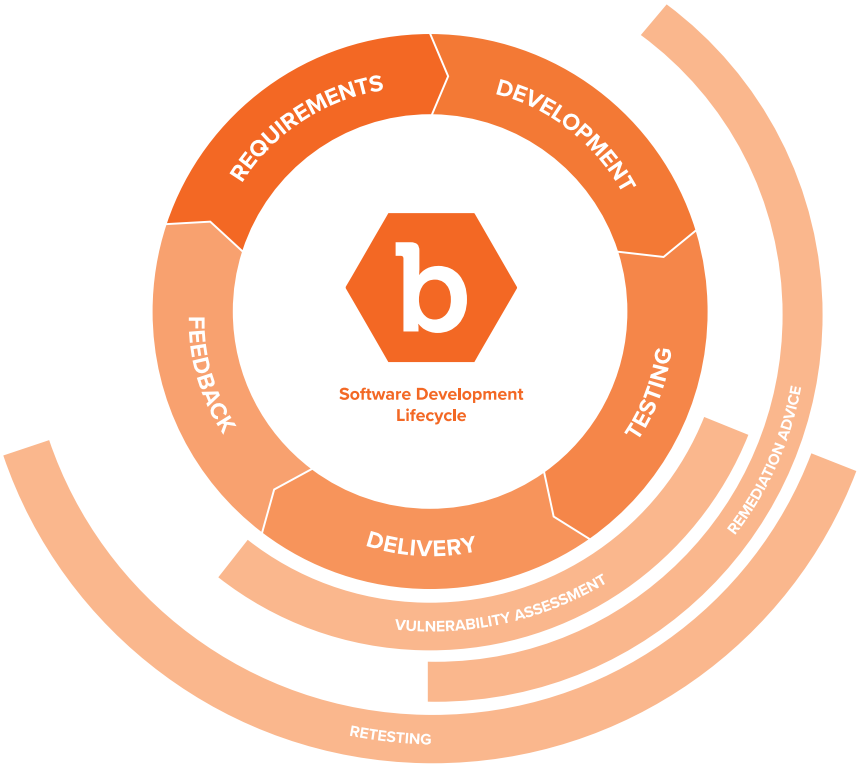
Scope: Private

Rewards: $100 – 6,000

Vulnerabilities Rewarded: 54

Paid Out: $33,650

> "One of the biggest benefits of Bugcrowd for us is the Jira integration. When we first started with Bugcrowd, we didn't have Jira in place. Then as we moved to Jira, I got really excited because Bugcrowd had an integration that allowed me to push issues and bugs directly into a Jira ticket.
>
> **Martin Rues, CSO Outreach.io**



Since Outreach has different teams owning different features of the platform, the company needed a way to filter each incoming vulnerability report coming in from Bugcrowd to the specific team owning the code. Outreach utilizes Bugcrowd's bi-directional Jira integration for multiple projects to get the right information to the right developer group, so they can focus on what is important to them and take action fast.

Bugcrowd offers the most scalable and robust Jira integration for crowdsourced security platforms. This integration enables security teams to streamline application security into development's day-to-day workflow. With highly customizable configurations, automated workflow, and remediation advice, the Crowdcontrol Jira integration ensures vulnerabilities are fixed quickly and effectively while maintaining code velocity.

Bug Bounty Program Results

Outreach.io has been able to maintain strong engagement across targets. Early on in the program, the program received a P1.

The P1 was a chained vulnerability that posed a threat deep into the infrastructure. For Outreach, it was incredible to find that up front and be able to fix it quickly. It gave a boost not only to the bug bounty program, but also bolstered a positive relationship between the security and engineering teams who were quick to respond.

Additionally, Bugcrowd's bidirectional Jira integration lowered developer overheard for Outreach, expediting time to remediation and secure code production.

54 vulnerabilities rewarded

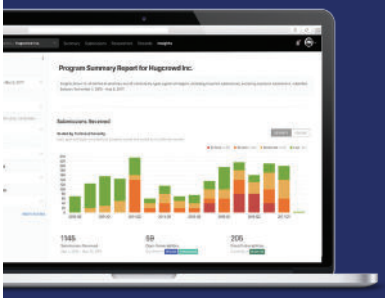
3.91 average priority

$33,650 total paid out

"It's huge to be able to directly push vulnerabilities into our Jira queue. We don't have to treat it any differently, dependent on what part of our application is affected, a ticket is created and tasked to the team responsible for building it."

"Our engineers looked at it and went, 'I would've never thought that was possible.'"

Martin Rues, CSO Outreach.io



Learn why hundreds of companies have turned to Bugcrowd:
www.bugcrowd.com/get-started