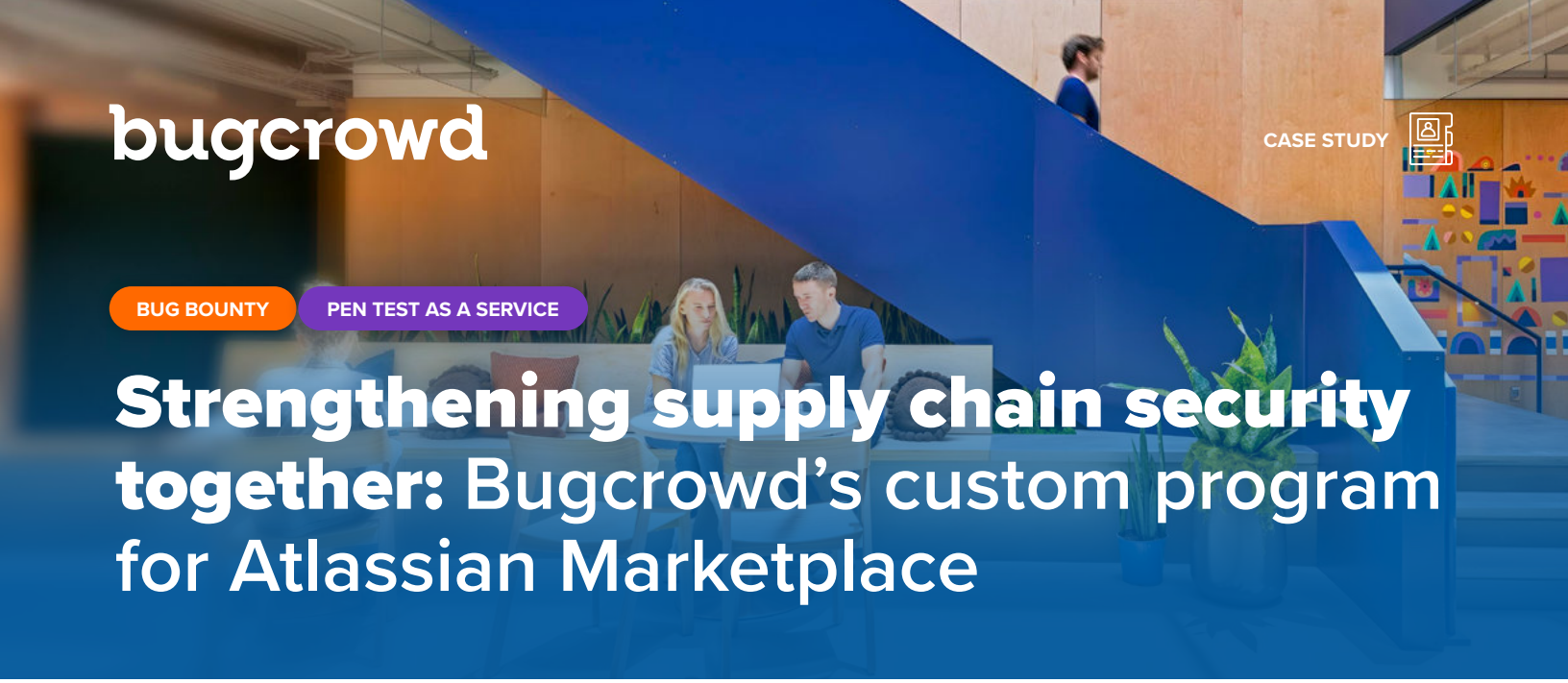


bugcrowd

CASE STUDY

BUG BOUNTY | PEN TEST AS A SERVICE

Strengthening supply chain security together: Bugcrowd's custom program for Atlassian Marketplace

ATLASSIAN

Industry Software

Founding Date 2002

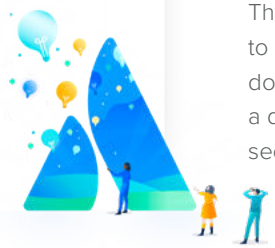
Website atlassian.com

# of Employees 10K+

Headquarters Sydney, Australia

RESULTS OVERVIEW

- **116 vulnerabilities reported**
  Bugcrowd reported 116 vulnerabilities across all applications tested in the bespoke methodology assessments.
- **21% critical vulnerabilities**
  21% of the 116 vulnerabilities were identified as critical or high severity.



The Situation

Collaboration is central to Atlassian's mission, as evidenced by products like the Atlassian Marketplace. This platform connects external developers with Atlassian customers, allowing them to purchase third-party apps that extend the functionality of Atlassian tools such as Jira and Confluence. Since its launch in 2012, Atlassian Marketplace has grown to host thousands of apps for 260,000+ users, generating over 4 billion dollars in lifetime revenue.

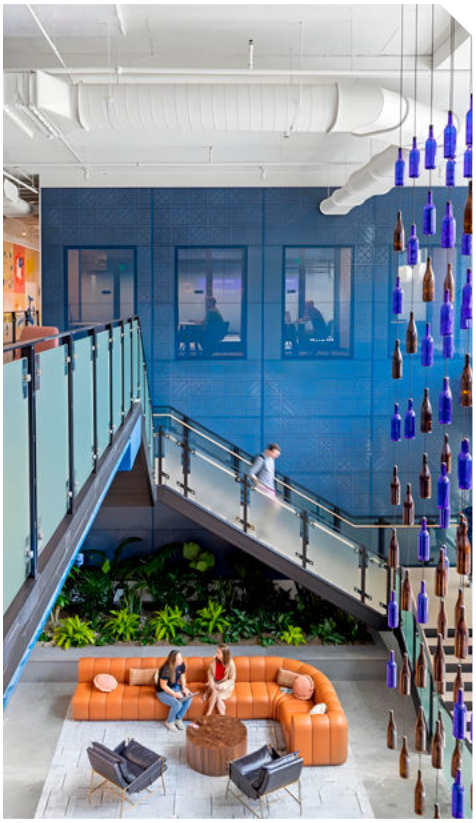
Given its scale, Atlassian Marketplace needs to take a proactive approach to safeguarding its ecosystem. If customers install an application from Atlassian Marketplace that compromises their data, it would create ripple effects across their business and lead to significant reputational risk for Atlassian. Furthermore, vendors relying on Atlassian for distribution could see their businesses affected. Ultimately, such security incidents can hinder the growth potential of both Atlassian and its vendor partners.

The Challenge

To solve this security challenge, the Atlassian Marketplace introduced a special badge in its user interface, highlighting apps that met Atlassian's privacy and security standards. For verification of these crucial criteria, Atlassian turned to a trusted ally: Bugcrowd, their long-standing security partner. Since 2016, Bugcrowd has managed successful bug bounty programs across Atlassian's web properties and APIs, making them well-suited for this task.

As Atlassian Marketplace grew, so did the complexity of its security landscape, which introduced new risks. To mitigate these issues, Atlassian updated its security requirements for badge eligibility. However, the standard web app methodology failed to capture all possible edge cases necessary to verify the new requirements. Simultaneously, the platform's expansion attracted a new wave of vendors. Many were small businesses, often lacking the resources to prioritize security.

The evolving situation led to an unexpected paradox. Some programs failed to uncover any vulnerabilities, while those that did left Atlassian with lingering doubts due to the limited scope of the assessments. This inconsistency created a dilemma: how could Atlassian design a tailored solution to address its unique security challenges across its rapidly growing Marketplace?



The Bugcrowd solution

After brainstorming, Atlassian and Bugcrowd aligned on a solution: quarterly bespoke methodology assessments. In this approach, Bugcrowd's in-house team spent a day evaluating each app with zero reported vulnerabilities, using a jointly-defined methodology. The team repeated this process every quarter to catch new issues.

"This approach allowed us to focus on areas of highest risk and the flexibility to customize evaluation criteria over time. Bugcrowd performed the assessments and delivered findings in their characteristic collaborative way—while our partners benefited from the additional insights," explained Vlad Yastreboff, Senior Manager, Security at Atlassian.

To execute this solution, Bugcrowd and Atlassian identified the partners and applications that needed to be tested, along with the methodology of test cases and triaging criteria. With this groundwork laid, Bugcrowd assembled a team of researchers to test each application. Results were reported to Atlassian in real-time via a shared tracker. Once the testing was completed, Bugcrowd delivered a comprehensive report of vulnerabilities across all applications.

Vlad said, "Bugcrowd hit the ground running and partnered with us throughout the process. We saw the first batch of vulnerabilities just a week after finalizing our approach. We reviewed the results in our biweekly catch-up and gave feedback, which they promptly incorporated. Before we knew it—nine weeks later—we had a full report across all our high-risk partner apps!"

"Bugcrowd hit the ground running and partnered with us throughout the process. We saw the first batch of vulnerabilities just a week after finalizing our approach."

— VLAD YASTREBOFF
Senior Manager, Security at Atlassian

The Outcome

Over the ten weeks of testing, the bespoke assessments revealed 116 vulnerabilities across the Marketplace apps, of which 21% were crucial or high-severity. Atlassian immediately began working with each partner to investigate and fix the issues, strengthening customer trust in Atlassian's Marketplace apps and ecosystem.

"The great thing about Bugcrowd's ability to rapidly deliver a variety of distinct, but complementary, security assessment services, is that we can rapidly mix and match to achieve the right level of technical security assurance, while leveraging Bugcrowd's proven service delivery model. It's been a great experience," Vlad said.

The success of this initiative underscores the benefits of partnering with security experts to tackle complex ecosystem challenges. "This bespoke solution showcases the power of Bugcrowd's multi-solution crowd-sourced security platform," Julian Brownlow Davies, VP of Advanced Services at Bugcrowd, explained. "By truly understanding Atlassian Marketplace's unique situation and bringing our expertise, we delivered a solution that provided Atlassian customers and vendor partners the security assurance and coverage they needed."