bugcrowd

CASE STUDY

BUG BOUNTY

BigCommerce Proactively Reduces Risk with Bugcrowd

About BigCommerce

BigCommerce (Nasdaq: BIGC) is a leading open software-as-a-service (SaaS) ecommerce platform that empowers merchants of all sizes to build, innovate, and grow their businesses online. BigCommerce provides merchants sophisticated enterprise-grade functionality, customization, and performance with simplicity and ease of use. Tens of thousands of B2C and B2B companies across 150 countries and numerous industries use BigCommerce to create beautiful, engaging online stores, including Ben & Jerry's, Molton Brown, S.C. Johnson, Skullcandy, Solo Stove, Ted Baker, and Vodafone. Headquartered in Austin, BigCommerce has offices in London, Kyiv, San Francisco, and Sydney.

Background Information

A bug bounty is a monetary reward for security researchers who find legitimate security flaws in software. Payments are allocated for each vulnerability found, depending upon various factors including the risk, impact, and exploitability of the vulnerability.

BigCommerce has run a private bug bounty program as a major pillar of the company's cybersecurity program since October 2020, before launching the public bug bounty program with Bugcrowd. Nearly 500 researchers participated in the private program, and within two years, more than 75% of the vulnerabilities identified were validated within four days of each submission. BigCommerce has since rewarded researchers for finding more than 100 vulnerabilities through their program.

BIGCOMMERCE

Industry

Technology

Challenges

Identifying security vulnerabilities across the company's IT platforms, applications, and devices.

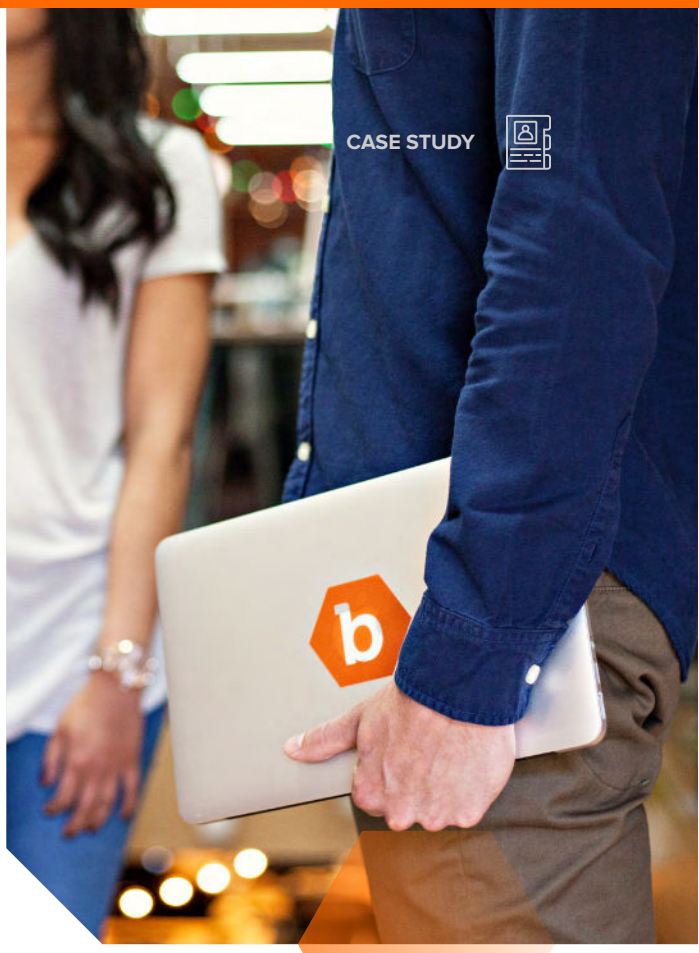
Solution

BigCommerce launched a new public bug bounty program with Bugcrowd that allows any security researcher around the world to submit vulnerabilities to the BigCommerce security team.

Outcomes

After running a private program for two years, BigCommerce made their bug bounty public. Now, anyone can report potential vulnerabilities, attracting more security researchers to help. This move, along with ongoing penetration testing and their private bug bounty, has reduced risk and become crucial to their cybersecurity strategy.

BUGCROWD BUG BOUNTY



Overall, why did BigCommerce choose Bugcrowd as its bug bounty vendor platform over the self-managed program?

Bugcrowd oversees crucial steps including vetting and triaging each claim and managing the researchers' expectations. In addition, if a vulnerability qualifies for a bounty, all rewards are paid and managed through Bugcrowd. This process allows BigCommerce to focus its resources on remediating the vulnerability as quickly as possible.

Any security researchers with a Bugcrowd account are eligible to submit a vulnerability. Every reported vulnerability is first triaged by application security engineers at BigCommerce to evaluate the validity, risk, and impact of the vulnerability. Once verified, the company immediately pays the researcher, and the ticket gets added to an internal queue of bugs to be fixed. Based upon the severity of the vulnerability, BigCommerce enforces an internal remediation policy that allows the product and engineering teams to prioritize each finding.

What benefits have you realized from your usage of the Bugcrowd platform?

BigCommerce has a strong security culture that allows them to work in a collaborative manner. Their engineers are well trained on security fundamentals and are always willing to work with Bugcrowd to ensure we ship a secure product. BigCommerce engineers are also trained on how to prioritize the vulnerabilities that are received through Bugcrowd. The fastest vulnerability fix ever pushed to production was less than 30 minutes, which was also a bug reported by a researcher.

"The cybersecurity landscape constantly evolves, demanding fresh approaches to identifying and addressing unique vulnerabilities. This bug bounty program allows BigCommerce to expand diversity beyond our global workforce. By partnering with external researchers who have different backgrounds and experiences, we are confident that we can mature our company's security practices and better protect our employees and customers," said Brian Dhatt, chief technology officer at BigCommerce.

The bug bounty program is not a replacement for traditional security reviews—it provides an additional layer of defense to supplement code reviews, penetration testing, and red team engagements.

"No technology is perfect, and that is why BigCommerce believes working with skilled security researchers around the globe provides crucial protections to identify any potential security weaknesses," concluded Dhatt.