bugcrowd

BUGCROWD REPLACES TRADITIONAL PEN TEST FOR INSTRUCTURE'S SECURITY AUDIT

Next Gen Pen Test uncovers 5X more critical vulnerabilities

Security & Transparency for eLearning

Instructure, the provider of the leading cloud based Learning Management System (LMS), Canvas, from its inception has proactively published the results of its annual security survey to add full transparency to its security posture. Initially the survey was based on traditional penetration testing, but realizing this approach offered limited value and was not a comprehensive method to identify critical vulnerabilities, Instructure turned to Bugcrowd to provide a more leading-edge and thorough crowdsourced based assessment.

The Value of a Next Gen Pen Test

The private, managed Bugcrowd Next Gen Pen Test has delivered to Instructure the highest quality researcher talent pool available, carefully selected for their knowledge and specialized skills, all ready and able to test the Canvas application within the allotted multi-week testing window. Unlike customary penetration testing with its focus on predefined scenarios, the Bugcrowd approach employs the creativity, cleverness, and broad-based expertise and scope only a crowd of researchers can offer, with a magnitude of results to match. Bugcrowd manages all of the back-end logistics, including submissions, ratings, payment, methodology, and reporting. Additionally, Bugcrowd ensures vulnerabilities are properly validated and operationalized into the SDLC so the development team knows what vulnerabiltiies to fix and how to fix them.

Working with Bugcrowd

As an online education enablement organization, Instructure is slated with delivering instruction and training to thousands of students in groundbreaking ways, all while protecting curriculum content and individual learner information. Instructure desired to affirm its commitment to its user base with a meaningful, actionable way to uncover and repair security issues, all while validating a publicly proactive security stance.

Working together with Bugcrowd, Instructure was able to incorporate the Crowdcontrol bug tracking platform into an ongoing security program, using the most innovative and effective technology available. This moved them beyond checkbox boilerplate pen tests to the results delivered by a cadre of human researchers with vast experience, knowledge and purpose.

Year after year, Instructure has acknowledged the ROI the Bugcrowd solution provides and the collaborative effort in which they excel, and is investing in additional Bugcrowd programs to expand the

INSTRUCTURE

As the basis of Instructure's annual security audit, Bugcrowd's Next Gen Pen Test Program ensures maximum security for its users.

"The cybersecurity landscape is an ever evolving one, so we knew we had to do something different, something innovative with this year's audit, and that is what Bugcrowd offered us. We've continued with the Bugcrowd program because it consistently delivers quantifiable results and practical reports, tools that we then can use to internally remediate issues before they become customer problems. We now know what to tackle first."

Q. Wade Billings,
VP, Technology Services

canvas

"Bugcrowd came on the scene and we experienced a dramatic shift in our security awareness. Even after the first Bugcrowd report, we were able uncover a 5X growth in findings. Our team of researchers could fan out, cover more surface area, find new vulnerabilities and then effectively report back. Once we had our Bugcrowd verified and rated results reports, we could easily create a Jira ticket and turn them over to our engineering team, confident they were high priority items on the way to swift resolution.'

Leading Edge

Annual penetration testing had long been the basis of Instructure's published security profile, and part of the organization's core philosophy to make their proactive stance well known. Results from these legacy engagements were predictable and limited, pushing Instructure to look for new solutions.

Bugcrowd offers innovative ways to uncover critical issues that traditional methods do not reveal or efficiently categorize. Bugcrowd's leading edge security approach is a crowdsourced testing model that breaks old process paradigms in favor of a newer and more thorough attitude toward security vulnerability detection and disclosure. It leverages the skill sets of the world-wide researcher community, ensuring maximum creativity and scope in the effective remediation of flaws in software, hardware, operating systems and code.

Comprehensive

Instructure had implemented annual pen tests using a major external vendor, but because of marginal year over year results and their own internal desire for more in-depth insights, the security team intuitively felt that they needed to shake it up with a more offensive support strategy, one that delivered both deeper and wider outcomes.

With the ability to engage Bugcrowd researchers globally, Instructure had far more reach in its investigations, with the discretion to select those individuals that most closely understood their application and its potential for breach. Instead of point-specific, predictable outcomes, Instructure was able to use the human intelligence Bugcrowd researchers delivered to successful understand and meet their security challenges.

Collaborative

Instructure found themselves with the need to reinvigorate synergies between their security team and their internal engineering staff, who had the actual job of problem remediation. Previous efforts delivered marginal insights into issues, and left the engineering staff with little motivation to categorize and engage on what had been both redundant and low priority findings.

Bugcrowd employed its unified platform, Crowdcontrol™ to improve Instructure's SDLC integration and remediation program, providing the vehicle to unify the efforts of both the security team and the development team. Using Bugcrowd's accurate categorization, VRT, escalation capabilities, and SDLC integrations, the Instructure engineering group was re-energized to tackle the most critical and well-defined issues, confident they were working on problems that would deliver value to the customer and the organization.

Bug Bounty Learnings

Instructure has experienced ongoing success and has adopted Bugcrowd's Next Gen Pen Test Program as an essential part of its annual security survey. The newly realized collaboration between the vulnerability detection group and the remediation process engineering team has expedited faster bug remediation.

Instructure and its learning management system Canvas have continued to lead in the tech-ed space, a vertical market where security concerns loom large. With Bugcrowd's assistance, Instructure has been able to attract, engage and retain researchers who have a growing and ongoing understanding of the product and the intricacies of their customer's needs. This association adds long-term brainpower, cumulative value and better results for Instructure and the ongoing security of its users.

Learn why hundreds of companies have turned to Bugcrowd.

www.bugcrowd.com/get-started

Bugcrowd.com
sales@bugcrowd.com | (888) 361-9734