bugcrowd

CODE.ORG ADOPTS AN ALWAYS-ON APPROACH TO SECURITY WITH BUGCROWD

Continuous crowdsourced security testing helps secure student and educator information

The Value of Student Information

Code.org is a nonprofit dedicated to expanding access to computer science in schools and increasing participation by women and underrepresented minorities. Code.org's vision is that every student in every school has the opportunity to learn computer science, just like biology, chemistry or algebra. Code.org believes computer science and computer programming should be part of the core curriculum in education, alongside other science, technology, engineering, and mathematics (STEM) courses, such as biology, physics, chemistry and algebra.

While cybersecurity standards and best practices are unique to every industry, those that store personally identifiable information are connected by a universal concern for protecting customer and employee data. EdTech (education technology) is one such industry. EdTech platforms often provide personalized programming for the individual user, meaning that information initially input about each student is always evolving and expanding. And while great care is taken to collect and store this information, it should also be noted that malicious attackers exert equal effort to find and exploit it. Unfortunately when it comes to data exploitation, the identities of children are far more likely to be targeted for tax, medicare, loan, and other types of fraud. This can have exceptionally long-lasting and sometimes irreversible consequences.

Security at Code.org

Code.org, like many other education platforms, maintains compliance with several international, US federal, and state laws for data security and privacy including GDPR, FERPA, COPPA, PPRA, SOPIPA, and HB 5469, amongst others. But it's the progressive practices that extend beyond compliance requirements that have really positioned Code.org as **a leader amongst their peers**. That's why their Software Development Cycle includes an embedded security review process for every proposed platform change, automated testing to ensure that assertions about the security of the platform do not lapse or regress when new features are shipped, and as of last year, a continuous security testing program.

Previously, Code.org utilized other security programs to supplement internal security audits. These were found to be costly and lacked sufficient return on investment. As Code.org began offering a steady stream of new features and services to users, they decided an 'always-on' approach to security was the only option for effectively securing student and educator information. That's when Bugcrowd entered the picture.

C O
D E

Launched: December 2018
Type: Private Managed Bug Bounty

"We have used other security programs in the past to supplement our internal security audits but these were costly and happened one to two times per year at best. With Bugcrowd, we've added an always-on approach to security."

Anthony Suarez
CTO, Code.org

Bugcrowd for Code.org

Code.org launched an independent investigation into available security testing platforms with the goal of leveraging a global network of security researchers to find and help process more priority vulnerabilities, faster. Based on a comparative review of platform features, Bugcrowd was selected as the platform of choice. After nearly a year of service and counting, Code.org stated the following key benefits:

- Bugcrowd's ability to match a diverse group of skilled and experienced researchers that bring actionable expertise on state-of-the-art attack vectors
- The ability to reduce time to market for new features and products with always-on testing
- Comprehensive program management including managed triage which helps scale security without draining limited internal resource
- Bugcrowd's clear Vulnerability Rating Taxonomy to quickly assess submissions and subsequently pritize work based on risk and impact
- Remediation advice and SDLC integrations to help Engineers fix quickly
- Transparent crowd payouts via a reloadable bounty pool, with expert advice from Account Managers on predicting future budget based on past results

Cybersecurity & EdTech

While Financial, Health, and Government sectors vie for space at the top of the 'most likely to be exploited' list due to either archaic security architecture or the value of data stored, it's the emerging industries like IoT, BioTech, and EdTech that face some of the most prolific threats due to lack of precedent, standards, or legislative requirements. Many EdTech platforms sit at the intersection of new technology and critical data storage, putting them squarely in the crosshairs of malicious attackers. As classrooms become increasingly networked environments, how do educators and technology providers keep up with the growing risk of attack?

> "Having real-world external testing of our platform has helped us keep up to date with security industry trends and tooling, which in turn improves our team's ability to protect the Code.org platform."

Anthony Suarez
CTO, Code.org

Code.org is part of a significant cultural movement in the education technology space — one that brings security and privacy front and center and raises the expectations parents, and educators have for the technology platforms entrusted with their children's information.

The impact of student data loss is grave, with an average cost to remediate a breach in the education industry valued at more than $300 per affected record, second only to healthcare worldwide according to a Ponemon Institute Study. In an effort to avoid such outcomes, several government and non-government bodies have taken action to elevate awareness around EdTech security. The California Attorney General's office issued a guide entitled, "Recommendations for the Ed Tech Industry to Protect the Privacy of Student Data," which details both preventative and reactive data security practices including employee training and breach notification plans. The FBI issued a public service announcement warning educators and parents on the specific data protection challenges facing EdTech platforms. And the International Conference of Data Protection and Privacy Commissioners issued a draft resolution on best practices outlining ways to minimize risk and exposure.

Though notably, many of these targeted guides lack practical ways to bake security best practices into your existing Software Development Lifecycle. That's why in addition to following more comprehensive, vertical-agnostic best practices like NIST, Code.org also expends equal effort developing a detailed data security plan tailored to their business goals, organizational structure, and development workflow. With millions of students and educators relying on their platform every day, Bugcrowd's ability to seamlessly integrate continual security assessments into existing security workflows has been a critical value add for the organization.

Working with Bugcrowd: The True Value of Crowdsourced Security for EdTech

Over the course of their crowdsourced security program, Code.org has seen consistent engagement across their applications and assets to surface more vulnerabilities than ever-before possible. Additionally, they've proved that the value of crowdsourced security testing extends beyond vulnerability discovery into risk reduction, resource efficiency, and workflow integration to reduce friction between Security and Development lifecycles. Perhaps more importantly, Code.org is part of a significant cultural movement in the education technology space — one that brings security and privacy front and center and raises the expectations parents, and educators have for the technology platforms entrusted with their children's information.

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