bugcrowd

BUG BOUNTY PROGRAM

Reduce risk with crowdsourced security

Think Beyond Traditional Security Solutions

Cybersecurity is fundamentally a people problem. Organizations rely on traditional security methods and staff that lack the creativity and motivations of black hat hackers. These methods continue to fall short leaving organizations vulnerable to cyber attacks. What's needed are innovative alternatives that leverage the creativity of human-intelligence at scale to combat the malicious motives of adversaries.

Bug Bounty Program: A Human-based Approach to Risk Reduction

Bug bounty programs level the cybersecurity playing field by building a partnership with a team of white hat hackers to reduce business risk. This competition-based testing model leverages human intelligence at scale to deliver rapid vulnerability discovery across multiple attack surfaces. With Bugcrowd's managed approach organizations receive prioritized vulnerabilities, program support, and remediation advice throughout the process to accelerate the discovery and remediation of vulnerabilities.

How It Works:

1

Engage Global Researchers:

Incentivize a global community of security researchers from around the world to find vulnerabilities.

2

Submission Triage and Validation:

Bugcrowd's application security engineers triage and validate all incoming submissions to ensure an organization's security team is focused on critical issues that present a real risk to the business.

3

Submission Acceptance and Payout:

Organizations review and confirm triaged submissions. At this time it is recommended to pay researchers for their findings.

4

Fix Vulnerability and Verify:

Bugcrowd's cloud-based platform integrates directly into software development offering seamless ticket generation to speed up the remediation process. Bugcrowd offers retesting to verify the patch was successful.

Highlights

- **Connect with tens of thousands of white hat hackers** to combat the imbalance between the creativity and motivations of cyber attackers and security defenders.

- Partnering with Bugcrowd to run a bug bounty program **accelerates the discovery and remediation of vulnerabilities to maximize risk reduction.**

- Bugcrowd seamlessly integrates vulnerability remediation into the software development lifecycle, largely **eliminating administrative overhead.**

- **Supports the most important attack targets**: web and API interfaces on cloud/servers, mobile, and IoT platforms.

- Unlike penetrations tests, bug bounty programs **significantly improve risk reduction** with an incentive-based testing model.

- Bug bounty programs find up to **7x more critical** issues than traditional security solutions.

"Bug bounty programs are going to become a baseline security control that you need to have."

onelogin

Testing Flexibility to Fit Business Needs

Bug bounty programs support the two key attack targets (web and APIs) across all core platforms. On-prem or cloud-based applications, IoT and mobile apps can all be secured, either in production or pre-production environments.

Web Front-End

API

x86 Server/ Cloud

Mobile

IoT

Bug bounty programs are available in both on-demand or continuous engagements. Bugcrowd makes it easy to quickly launch either type based on requirements.

On-demand

A single point in time or periodic testing engagement that is best fit for an initial proof-of-concept, or as a replacement for periodic penetrations tests.

Ongoing

An ongoing testing engagement that is best fit for high-value targets or agile DevOps cultures where the application is changing continuously.

Bug bounty programs can be run with either public or private researcher exposure. It is common for organizations to "crawl, walk, run" as they scale their bug bounty program. The best starting point is usually as a private program with a limited number of invited, trusted researchers. As the program matures over time, organizations may choose to increase the number of researchers, expand the targeted scope, or transition to a public program to heighten security awareness and increase the breadth and depth

Private Programs

- **Controlled** testing environment with a small set of highly vetted and experienced researchers.
- **Elasticity** to adjust researcher engagement and testing scope as needed.
- **Ideal for targets that are not publicly accessible** such as staging environments, applications that require credential access, or devices.

Public Programs

- **Scale** testing efforts to gain access to extensive skill set, diversity, and coverage at scale.
- **Heighten Security Awareness** and reassure stakeholders security is a priority to your organization.
- **Ideal for publicly accessible targets** such as web and mobile applications or more complex targets like client-side apps and IoT devices.

Bug Bounty Programs Drive Efficient Risk Reduction

Bug bounty programs are quickly gaining popularity because they combine effective risk reduction with efficient use of both capital and operating expense. Researcher payments are based on results: the more serious the vulnerability discovered, the bigger the payout. As the leader in managed bug bounty programs, Bugcrowd's program management team handles virtually all operational overhead, allowing our customers to focus on actually reducing risk by remediating the vulnerabilities identified.

Rapid Risk Reduction

An incentive-based testing approach motivates researchers to think creatively and find high-impact vulnerabilities that present the most risk to your business.

Cost-Effective

A results-driven model ensures you pay for the vulnerabilities that present a risk to your business, and not for the time or effort it took to find them.

Lower Operational Overhead

A cloud-based, managed solution that seamlessly integrates into your existing SDLC delivering frictionless setup with zero maintenance.

Bugcrowd Makes Bug Bounties Easy and Effective

Bugcrowd's industry-leading crowdsourced security offerings are based on three key elements:

Platform

Crowdcontrol™
The Nerve Center

An all-in-one platform for simplified vulnerability reporting and solution management.

- **Remediation acceleration** to reduce risk.
- **Visibility** into vulnerability lifecycle, bounty pool, and researcher activity.
- **Integration** into your SDLC and security systems and processes.

Researcher

Right hacker,
Right incentive

Quality, impact, coverage, and trust – harness the power of human creativity.

- **Trusted** through proven track record, ID verification, and background checking.
- **Thousands of members worldwide** provide 24x7 coverage.
- **Diversity** of backgrounds and attack methodologies supporting a broad range of platforms (web, API, IoT, mobile)

Management

The Experts

Decades of experience in enterprise security and hacker community engagement.

- **Vulnerability** triage, validation, and remediation advice.
- **Program** onboarding, SLAs, and ongoing health.
- **Researcher** selection, payout guidance, and dispute resolution.

Bug Bounty Programs: The Next-Gen Penetration Test

Penetration test are largely ineffective at reducing risk because they employ a small number of people with a limited skillset and timeline. Their goal is to complete the test plan, not find the biggest sources of risk. Bug bounty programs significantly improve risk reduction with an incentive-based testing model that introduces thousands of the top researchers to test your assets.

Additionally, bug bounties offer low operational overhead and costs, and if needed can be run as an ongoing program to support agile devops that is continuously rolling out new code. That's why more and more organizations are using bug bounty programs to supliment their penetration tests.

To learn more about how bug bounties can help your organization reduce its security risk visit **www.bugcrowd.com/get-started**

Trusted by Leading Companies Around the World

mastercard. ATLASSIAN Square NETFLIX CONCUR TESLA

(ISC)² NETGEAR FCA FIAT CHRYSLER AUTOMOBILES OWASP Open Web Application Security Project CISCO Meraki

bugcrowd

Bugcrowd is trusted by more of the Fortune 500 than any other crowdsourced security platform. Why? Because people need to strengthen their security program without all the extra work and chaos. Bugcrowd cracked the code on crowdsourced security through rock solid program management, top trusted researchers, and an integrative platform. That's how our vulnerability disclosure and bug bounty programs find seven times as many critical vulnerabilities as traditional testing. Based in San Francisco, Bugcrowd is backed by Blackbird Ventures, Costanoa Ventures, Industry Ventures, Paladin Capital Group, Rally Ventures, Salesforce Ventures and Triangle Peak Partners. Bugcrowd. Outhack Them All™.