bugcrowd

Crowdsourced Security:
The Next Generation of Penetration Testing

Highlights

- Traditional penetration testing is not an effective method for reducing the risk of cyber attack.
- The next generation of pentesting is based on crowdsourcing.
- Crowdsourced Security uses a diverse set of highly skilled researchers incentivized to find high priority vulnerabilities.
- Crowdsourced Security delivers valuable results 80% faster than a traditional penetration test
- Crowdsourced bug bounty programs are proven to find 7x more critical issues than traditional pentesting methods and security solutions.
- Crowdsourced Security creates less operational overhead than traditional pentesting, and supports agile development environments.

Common Challenges with Penetration Testing

Traditional penetration testing suffers from numerous shortcomings that lessen its effectiveness for risk reduction. The biggest issue is that pentesting is usually performed by one or two people using a rote, standardized methodology. Given the vast number of adversaries and their diverse skill sets and creativity, it is unrealistic to expect that this approach will reliably find the most serious application vulnerabilities.

> ***"New security assessment approaches such as crowdsourcing pen testing and bug bounty programs are emerging as alternatives to single-sourced black- and gray-box testing."***
>
> Gartner, How to Select a Penetration Testing Provider, Toby Bussa, Claudio Neiva, Prateek Bhajanka, 14 September 2017

Second, pentests are periodic "point-in-time" exercises. In today's agile DevOps environment, applications are continuously changing, so testing once or twice a year will leave new application code untested for months. And because many pentest firms are relatively small, there may be a long delay between scheduling a test and actually getting it done.

Pentest results also lack true insight into actual risk, and are hard to action. The typical output is a long report of potential vulnerabilities. For a developer, it's no easy task to sift through thousands of findings with no context or remediation advice, nor do they have the ability to interact with the tester to understand the potential exploits. Furthermore, there's no integration into the software development workflow, adding operational overhead and slowing the pace of both remediation and application development.

Lastly, pentests are not cost effective. The incentives of pentesters focus on quantity, not quality of results. The reality is that organizations continue to spend money on pentests because they are well-understood and accepted by auditors and compliance regulations, but they are not effective for reducing risk or controlling costs.

David Kosorok,
Director of Application Security, SAP Concur

"SAP Concur has truly appreciated the service and security hardening that has come about because of Bugcrowd's private and public bug bounty programs."

bugcrowd

The Next Generation of Penetration Testing

Crowdsourced Security is replacing traditional pentesting as the most effective and efficient way to reduce risk at the application level. Services such as bug bounty and vulnerability disclosure programs leverage human intelligence at scale to deliver rapid discovery of high-risk vulnerabilities across attack surfaces such as web front-ends and APIs.

Crowdsourced security is fundamentally better than penetration testing because the goal of the program is to find high risk vulnerabilities, and not to complete a simplistic set of tests that do not reflect the way advanced attacks actually work. It is clearly superior for modern agile development, because the program can run continuously, consistent with the rapid pace of code release into production.

	BUG BOUNTY	TYPICAL PENTESTING
Access to vetted, trusted, and experienced security researchers	✓	✓
Access to thousands of the world's best researchers to address the entire scope of the security assessment	✓	✗
Testing for complex modern day exploits and attack vectors	✓	✗
Powerful integration with software development lifecycle tools	✓	✗
Pay only for validated vulnerabilities	✓	✗
Classification of vulnerabilities based on a standardized model with remediation advice	✓	✗
Continuous, human-powered security assessment	✓	✗

Why Choose Crowdsourced Bug Bounties

Bug bounty programs build a partnership with the world's best white hat hackers to assess overall risk. At any given time, hundreds of security professionals using their unique skill sets are able to uncover vulnerabilities across multiple attack surfaces. Each of these individuals bring their own strengths and methodologies, providing unparalleled coverage with deep technical expertise.

PENETRATION TEST

Standard penetration tests are performed by a small number of testers, fundamentally limiting the perspectives and expertise brought to a project.

BOUNTY PROGRAM

Bug bounties exponentially increase the testing talent available and are just as safe as standard penetration tests.

bugcrowd

Bug bounty programs utilize a pay-for-results model to deliver much better ROI than traditional pentesting.Researchers are incentivized to hunt for the more complex application logic bugs that are the most challenging to find and remediate. The crowdsourced model finds an average of seven times the number of high priority vulnerabilities as compared to pentesting, and uncovers an average of eight critical, unknown vulnerabilities within the first 30 days.

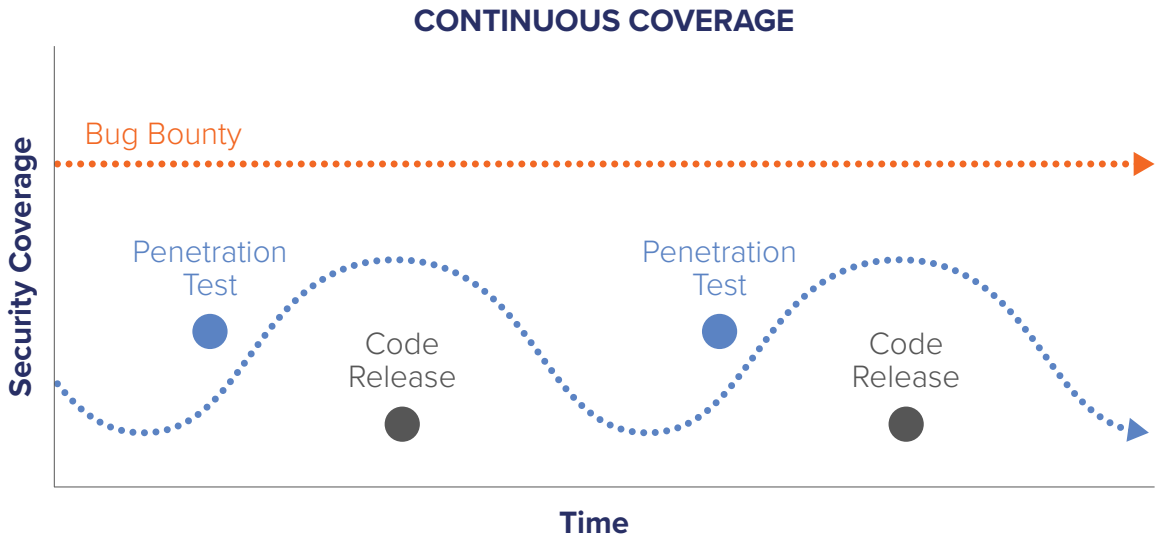
"Multiplying the specialization of a single bounty hunter by the size of the crowd creates a capability that just can't be replicated by individual organizations."

Dan Grzelak,
Head of Scurity at Atlassian

Bug bounty programs reduce the "noise" in the application security environment. Dynamic scanners and most pentest vendors produce reports full of false positives or no-risk issues. Parsing these reports takes time away from security teams and their mission of working on more pressing issues. However with crowdsourced security, each bounty submission is verified and risk-rated, and can include advice that aids remediation and developer security best practices training.

18 **distinct areas of hacking expertise within the crowd including web, Android, iOS, hardware, firmware, Linux, network, and more.**

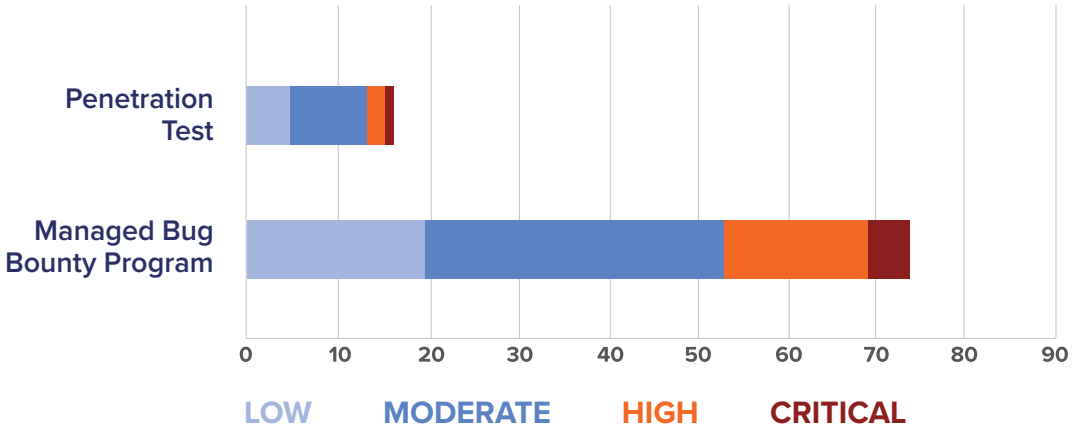
With bug bounty programs, organizations have the coverage necessary in today's modern software development life cycle. A bug bounty program can be time-matched with the development lifecycle of the target application. As organizations transition to agile, devops software methodology, security assessment should be continuous. Traditional penetration testing is inflexible and only offers point-in-time assessments. Bug bounty programs also provide integration with internal systems like JIRA or vulnerability management software. With powerful APIs and integrations, bug bounty programs align security with the DevOps process.



bugcrowd

Pentest vs. Bug Bounties

BUG BOUNTY PROGRAMS FIND MORE HIGH PRIORITY VULNERABILITIES

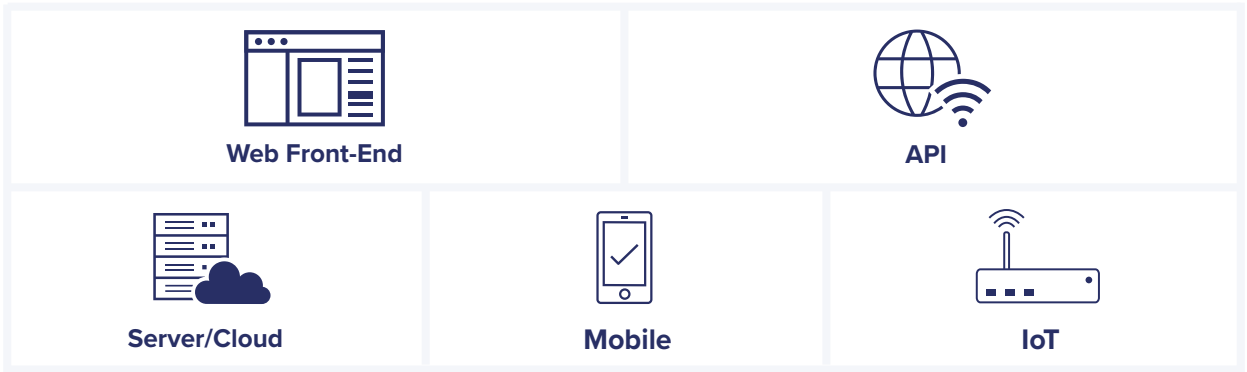


Benefits of a Bug Bounty Program

RAPID RISK REDUCTION	COST-EFFECTIVE	LOWER OPERATIONAL OVERHEAD
An incentive-based testing approach motivates researchers to think creatively and find high-impact vulnerabilities that present the most risk to the business.	A results-driven model ensures payment for the vulnerabilities that present a risk to the business, and not for the time or effort it took to find them.	A cloud-based, managed solution that seamlessly integrates into your existing SDLC delivering frictionless setup with zero maintenance.

ATTACK SURFACE COVERAGE

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



bugcrowd

Bug bounty programs are available in either a time-boxed or continuous model. Bugcrowd makes it easy to quickly launch either model based on security requirements and software development cycle.

On-demand Bug Bounties are a great fit for organizations looking for a Crowdsourced Security proof-of-concept or replacement for periodic penetrations tests.

Continuous Bug Bounties are best fit for high-value targets or agile development to continuously harden an application's attack surface.

Bugcrowd Makes Bug Bounties Easy and Effective

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

Researchers

Right hacker, Right

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)

Platform

Crowdcontrol™

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.

Management

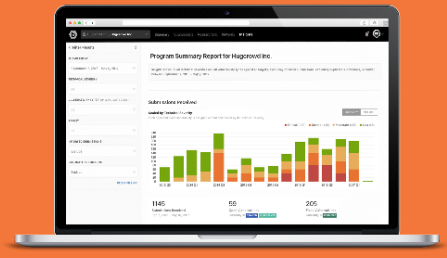
The Experts

Industry leading team with 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.

Trusted by Leading Companies Around the World

mastercard · ATLASSIAN · Square · CONCUR · TESLA · (ISC)² · NETGEAR · FCA FIAT CHRYSLER AUTOMOBILES · OWASP Open Web Application Security Project · cisco Meraki



Getting Started

Want to learn more about how your organization can leverage crowdsourced security to start discovering and fixing high-value vulnerabilities missed by traditional security testing? Bugcrowd offers a full line of crowdsourced security solutions.

www.bugcrowd.com/get-started