What's a Vulnerability Worth?

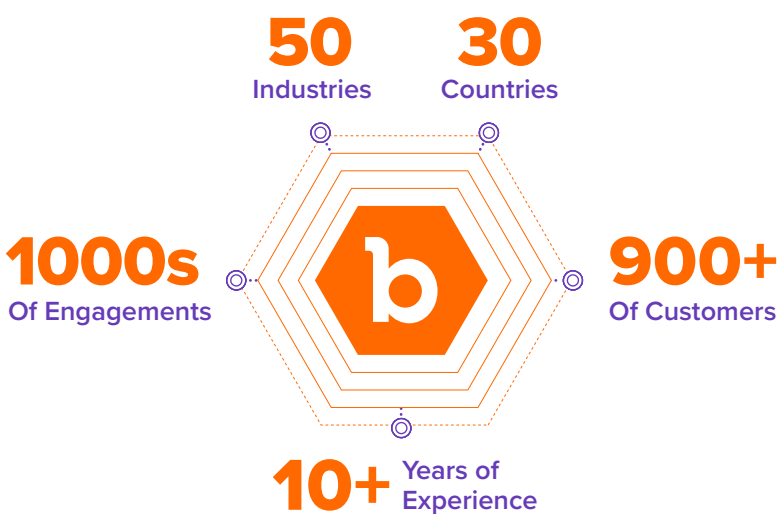
Recommended reward ranges
for your Bug Bounty program

bugcrowd

Contents

Background

Bugcrowd's customers include organizations across every industry, managing some of the world's largest and most successful bug bounty programs.



This long track record -- created over a decade of experience and 1000s of engagements -- gives Bugcrowd unique insight into the vulnerability and risk economics underpinning successful bug bounty reward structures.

Based on that experience, we can provide recommended bug bounty reward ranges to help program owners motivate the right hackers to work on the right targets, as well as ranges for specific industries that have unique needs. With this information, program owners will know the baseline incentives for motivating hackers to deliver the best results, and have an expectation of budget impact as their program matures.

Bug bounty solutions on the Bugcrowd Platform can be open to the public, with no restrictions on participation, or private, with only invited participants. They can also be continuous or time-limited.

Questions & Answers

The questions most often asked by security decision makers interested in bug bounty programs include:

1. **What is a vuln "worth" on an economic basis?**
2. **What should my organization budget for a successful program?**
3. **Was that payout I read about too low? Too high?**

$4.35M

Avg. cost of a data breach for companies in 2023

Source: Ponemon Institute

The answers to them — and the solutions needed to address the underlying risks at issue — will, inevitably, continue to develop as the market evolves.

The key to reaching a positive outcome, however, remains the same: to run a successful bounty program, you need to attract the right hackers to the right targets with the right reward. The Bugcrowd Platform's CrowdMatchTM AI technology uses data to match the right trusted hackers to your program across 100s of dimensions, but it's still important to design incentives that will keep them active and motivated.

At Bugcrowd, we strongly believe that:

1. **Appropriately rewarding hackers is an absolute requirement for all-around success in bug bounty (especially in the face of dark net incentives), and**
2. **The economic benefits of generous payouts far outweigh their cost.**

Furthermore, we understand that different organizations are at different points on their bug bounty journey, and that requires some flexibility for budgeting and ROI calculation.

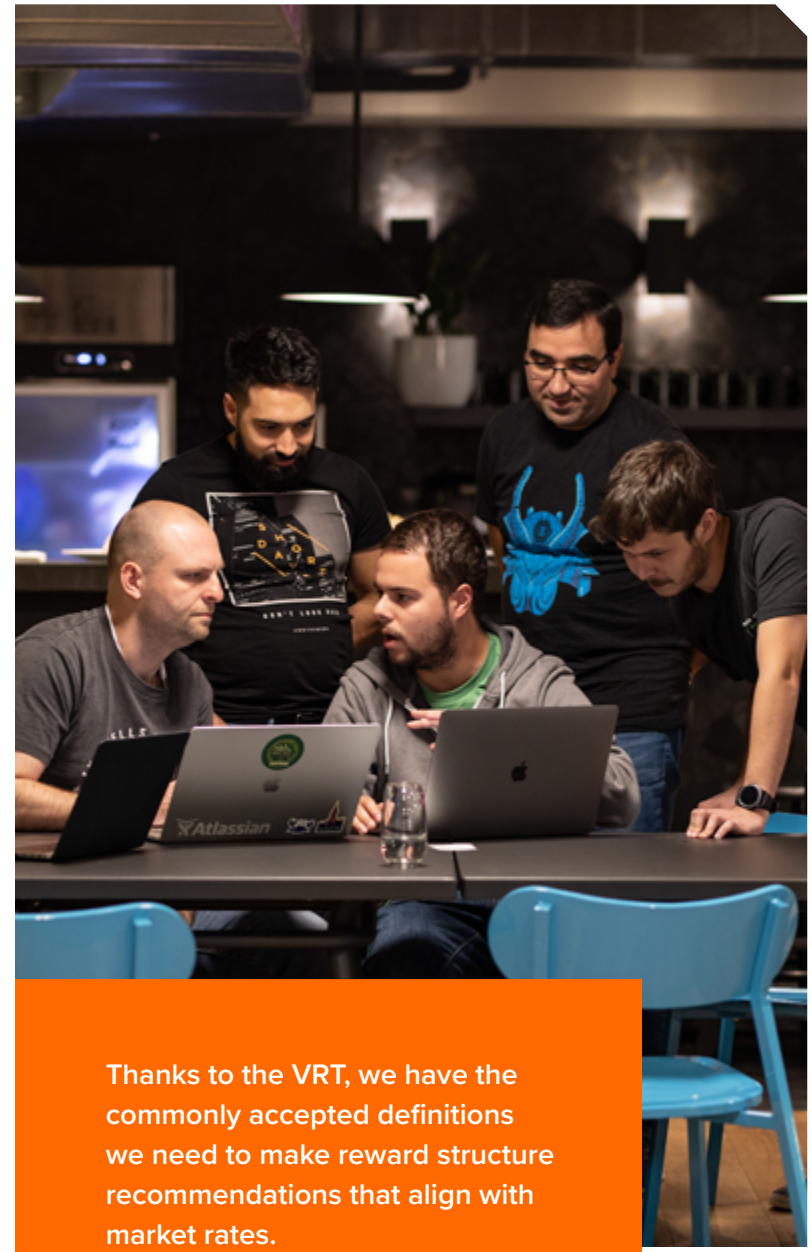
Prioritizing Vulnerabilities

Rewards structure should be based on alignment between commonly accepted vulnerability definitions, severity levels, and market rates.

Our bounty reward recommendations provide a clear, consistent pricing framework that aligns with market rates, helping program owners understand budget impact while enabling them to confidently design programs that will incentivize hackers to work on the right things.

To determine appropriate reward ranges, it is first necessary to define severity levels for prioritization purposes. Prioritization is important in an incentives-based system because higher priority problems can be more difficult to identify and require more time, effort, and expertise--and hence deserve higher rewards.

Since 2017, Bugcrowd has been the maintainer of the Vulnerability Rating Taxonomy (VRT), an open-source effort to classify and prioritize submissions on the Bugcrowd Platform in an industry-standard way. The VRT is a simple-to-use, non-prescriptive, and evolving method for assigning severity levels to specific vulnerability classes. Since the VRT's creation, hundreds of thousands of vulnerability submissions on the Bugcrowd Platform have been created, validated, triaged, and accepted by program owners under this rubric.



Thanks to the VRT, we have the commonly accepted definitions we need to make reward structure recommendations that align with market rates.

We've discovered that assigning a "P1" designation to the most critical vulnerabilities and a "P5" label to vulnerabilities that pose acceptable risks works well for this procedure. The baseline priority matrix below is a starting point for setting expectations between hackers, the Bugcrowd Triage Team, and program owners.

P1
Critical

Vulnerabilities that cause a privilege escalation from unprivileged to admin or allow for remote execution, financial theft, etc.

- Remote Code Execution
- Vertical Authentication Bypass
- XML External Entities Injection with significant impact
- SQL Injection with significant impact

P2
High

Vulnerabilities that affect the security of the platform, including the processes it supports

- Lateral authentication bypass
- Stored XXS with significant impact
- CSRF with significant impact
- Direct object reference with significant impact
- Internal SSRF

P3
Medium

Vulnerabilities that affect multiple users and require little or no user interaction to trigger

- Reflective XXS with impact
- Direct object reference
- URL redirect
- CSRF with impact

P4
Low

Vulnerabilities that affect multiple users and require little or no user interaction to trigger

- SSL misconfigurations with little impact
- SPF configuration problems
- XSS with limited impact
- CSRF with limited impact

P5
Acceptable Risk

Non-exploitable vulnerabilities in functionality. Vulnerabilities that are by design or are deemed acceptable business risk to the customer

- Debug information
- Use of CAPTCHAs
- Code obfuscation
- Rate limiting, etc.

Reward Recommendations

The reward ranges below are suggestions, not absolutes. Some targets may call for higher rewards, and others, lower rewards. When designing your program, we recommend starting at the lower end of the range initially. That will provide the flexibility needed to increase rewards over time if added incentives are needed.

Severity Level Per Vulnerability Rating Taxonomy (VRT)		P1	P2	P3	P4
Low Range (Attracts generalists)	Best for: Untested web apps that are new to crowdsourced testing with basic credentialed access and no hacker restrictions (e.g. geolocation, etc) – for any target with restrictions in place, rewards should default to one range higher	$3,500-$4,500	$1,500-$2,500	$500-$750	$175-$225
Mid Range (Attracts experienced hackers)	Best for: Well-tested web apps that have been part of longstanding crowdsourced programs, moderately tested APIs or mobile apps, presumed-to-be-vulnerable thick clients/binaries and/or embedded devices	$5,500-$7,500	$2,500-$3,500	$750-$1,500	$250-$500
High Range (Attracts P1 specialists)	Best for: Extremely hardened and sensitive web apps, APIs, and mobile apps - as well as moderate-to-highly secured thick clients/ binaries and/or hardened embedded devices	$11,000-$20,000	$3,500-$7,500	$1,000-$2,500	$300-$600
Hardware Providers		$5,000-$10,000+	$2,000-$4,000	$600-$900	$200-$400
Cloud Providers		$5,000-$15,000+	$3,000-$5,000	$1,000-$2,500	$250-$700
Financial Services		$8,000-$20,000+	$3,000-$8,000	$600-$1,500	$250-$350
Cryptocurrency		$50,000+	$10,000-$20,000	$2,000-$3,000	$500-$750

Additional Considerations

Target Criticality

If the company handles mission-critical, highly sensitive, or valuable data (e.g., PII, PHI, financial data, etc.), it's a good idea to explore increasing pay to attract and retain top people.

Target Accessibility

If your targets necessitate large test setups or other complex or scarce situational knowledge, it's a good idea to adjust the pricing to account for the ramp time and attract the right kinds of talent.

Program Maturity

If a firm has a high level of security maturity and/or wants to attract the highest level of security expertise, all basic payouts should be multiplied by a factor of two or more. This approach will keep you on par with some of the most well-known companies that are now conducting bounty programs.

Marketing Your Program

If a business wants to use the program to market its security capabilities, it can choose to increase payouts to present a clear indicator of security maturity to the general public.

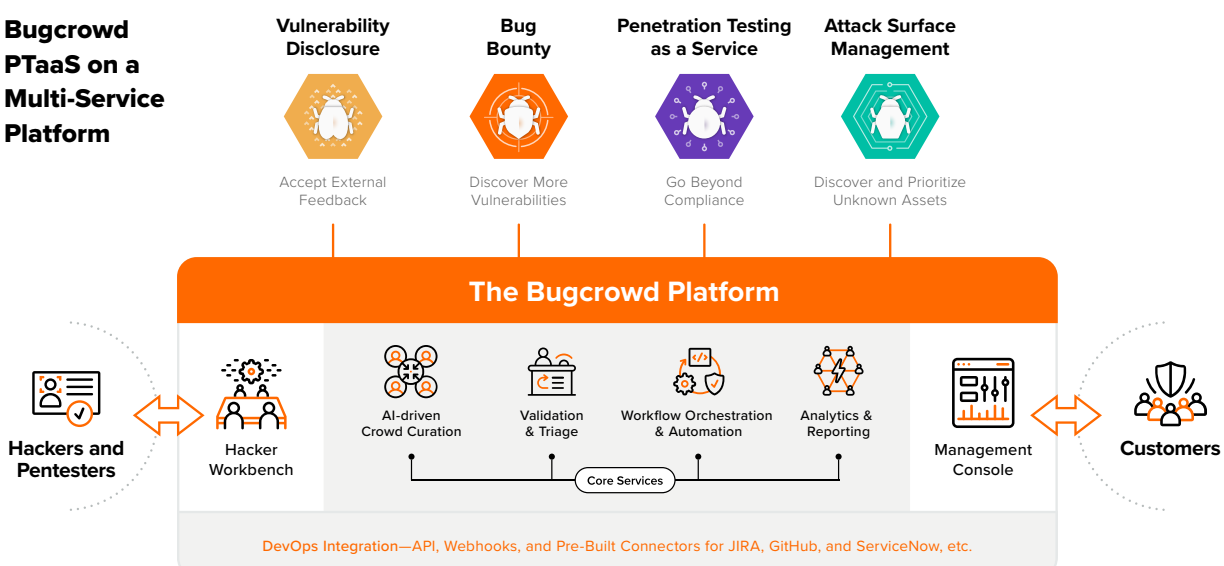
Unleashing Human Ingenuity: The Bugcrowd Platform

Are you unsure which pricing model your company should use? That's one of the many ways the Bugcrowd Platform can help.

Bugcrowd unleashes the ingenuity of the global hacker community for consolidated pen testing, bug bounty, vulnerability intake, and attack surface management needs – for any risk reduction/ compliance goal, scope, asset, and environment, and backed by extensive trust engineering. And all with SaaS scaleand efficiency and one-to-many integration with existing DevSec processes.

Please contact us for a free, no-obligation consultation on what range your organization should establish for a bounty program and how much you can expect to pay in the coming year.

Bugcrowd PTaaS on a Multi-Service Platform



Multi-solution Platform

Multi-solution platform for meeting multiple security goals and supporting long-term innovation

Right Crowd, Right Time

Activates the right trusted hackers, with the right skills, at the right time–for 2x better results

Engineered Triage At Scale

Best-in-class triage, powered by specialists armed with the best triage toolbox in the industry

Security Knowledge Graph

Data-driven insights from a rich Security Knowledge Graph developed over a decade

bugcrowd

Get in touch to learn more about how Bugcrowd can help you unleash hacker ingenuity to find vulnerabilities that traditional approaches miss

Get Started