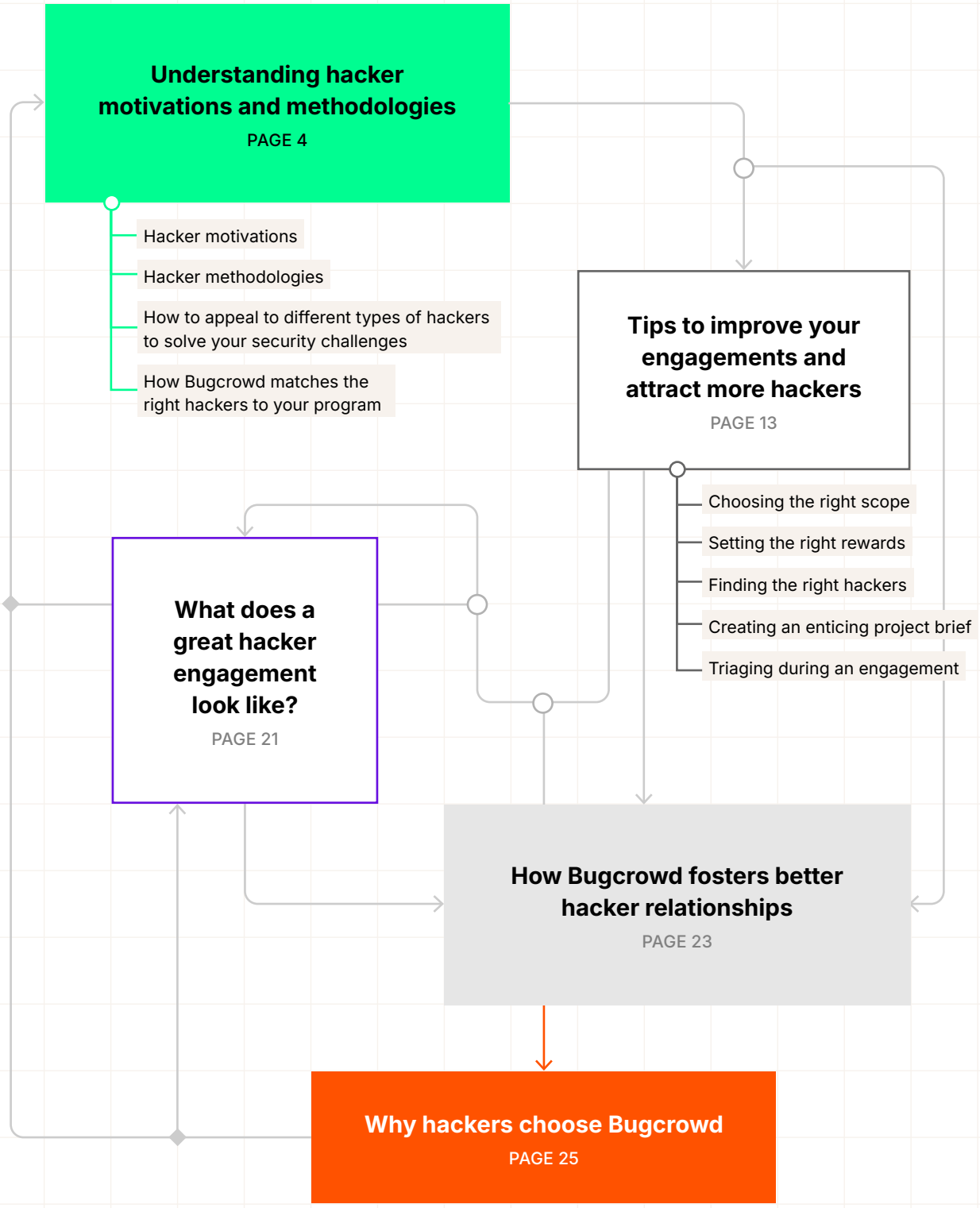
bugcrowd

Guide to working with hackers

Guide to working with hackers



The cybersecurity skills gap widens every year, according to industry reports, news articles, and analyst blogs. Security risks are changing too quickly for teams to adapt. 88% of security leaders think there are more security risks now than before 2020. Internal training programs aren't bridging the growing gap between security teams and threat actors. Companies are seeking to overcome this by hiring but face a skills shortage. The consequences: **a ballooning attack surface, stagnating security, and a feeling that there's no solution.**

We don't agree.

The cybersecurity skills gap disappears if you look at the issue from the right perspective. The talent exists; it's just a matter of accessing it. Some of the world's best security talent is no longer looking for full-time security jobs. They recognize that they can have more impact, find more bugs, and earn more by working with multiple companies under a crowdsourced security model. This security talent comprises a range of related personas, including ethical hackers, pentesters, and red team operators—but in this guide, we'll use the term "hacker" as a catchall to simplify things.

This new paradigm—crowdsourced security—makes sense for companies too. You can work with the hackers who have the exact skills you need. You probably don't need the expertise of an API hacker every single day, but when you do, you want the best. And if you need API, cloud, and AI expertise, you can find three experts as easily as you can find one.

In essence, you can set your team on autoscale to ensure your attack surface stays deflated.

Crowdsourced security is a good solution to some of the most pressing cybersecurity needs and issues. However, we acknowledge that it's not always easy to shift your thinking from a "full-time hire mindset" to a "skills-as-a-service mindset." How do you find the hackers with the skills you need? How do you vet them? How do you make sure hacker engagements are productive?

We wrote this guide to answer those questions and help you take full advantage of crowdsourced security. We'll cover the basics of crowdsourced security, how to work with hackers (including hacker motivations and methods), and ways to make your engagements as enticing and effective as possible.

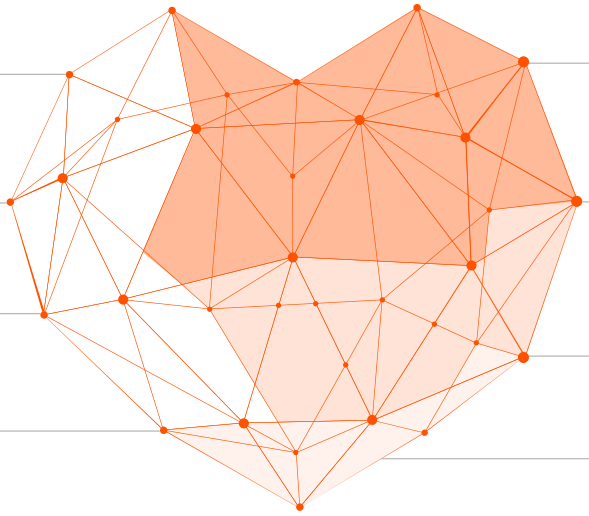
Understanding hacker motivations and methodologies

Years ago, hackers were almost exclusively assumed to be criminals. Now, most security professionals not only understand the difference between threat actors and hackers, but they actually have personal experience with ethical hacking. Whether you're currently working with ethical hackers via a crowdsourced security solution like Bugcrowd or are just wanting to learn how to maximize an investment in working with hackers, a key first step is understanding hackers.

Hacker motivations

Hackers are driven by a unique blend of personal and altruistic motivations. Over the course of their careers, individual hackers often experience each of these motivators at different times. While no hacker can be slotted exclusively into one category, understanding the intrinsic and extrinsic factors that drive them can provide some insight.

The security industry is full of some pretty amazing experts who helped us develop the research around hacker motivations and methodologies. Shoutout to Beau Woods, Senior Advisor with CISA, and Michael Skelton, VP of Operations at Bugcrowd, for their help with this research!



3%
For reasons I'd rather not share

4%
For something to do

8%
For my livelihood

11%
For the greater good

28%
For my personal development

18%
For financial gain

15%
For the excitement

14%
For the challenge

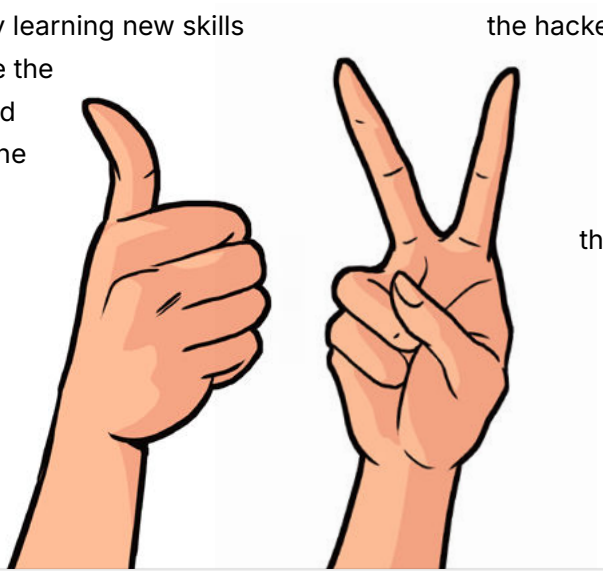
Intrinsic motivators

The greater good

Many hackers are motivated by a desire to make the internet a safer place. Whether it's protecting user data, helping organizations secure their assets, or giving back to the community, they're truly driven to defend organizations against adversaries.

Tinkering, puzzling, and learning

For many hackers, the joy of solving complex puzzles and continuously learning new skills fuels their passion. Inside the Mind of a Hacker revealed that 28% of hackers on the Bugcrowd platform cited "personal development" as their primary reason for hacking.



Extrinsic motivators

Financial compensation

For some hackers, the pursuit of financial stability or a better quality of life is a strong motivator. This often drives talented individuals to specialize in high-demand areas of cybersecurity and earn significant rewards for their skills.

Fame and reputation

Recognition plays a significant role in the hacker community. While "fame" might be too strong a word, many hackers seek acknowledgment of their talents in the public arena through Hall of Fame listings, speaking opportunities at security conferences, and opportunities to build their professional credentials.

How do we vet hackers?

At Bugcrowd, trust isn't assumed, it's earned. Every hacker on our platform undergoes a rigorous, data-driven vetting process that extends beyond what most organizations require for their own employees.

Furthermore, trust is earned incrementally through a proven track record of skill, professionalism, and ethical behavior. Our platform's CrowdMatch AI technology incorporates these trust signals to intelligently match the right hackers with the right opportunities based on their expertise, performance, and alignment with the overall program.

Hackers progress through a "trust journey," starting with public programs and advancing to private and restricted engagements as they demonstrate consistent success. For customers with specific needs, such as geolocation restrictions, security clearances, or certification requirements, we offer additional vetting options, including ID verification, background checks, and white-glove sourcing. Our platform enforces these requirements through built-in controls, including compliance screening against global watchlists and traffic control technology for managing access to sensitive targets. By combining scalable technology with a human-centric approach, we create a secure, collaborative environment where hackers can thrive and organizations can confidently address their security challenges.

Hacker methodologies

Motivations aren't the only way we categorize hacker personas—we also look at hacker methodologies. As you saw in the section on motivations, no two hackers are the same. However, in general, we can categorize hackers by five different methodologies that take into account their experience and expertise. Programs generally need a few different types of hackers, and those needs change over the lifespan of a project.

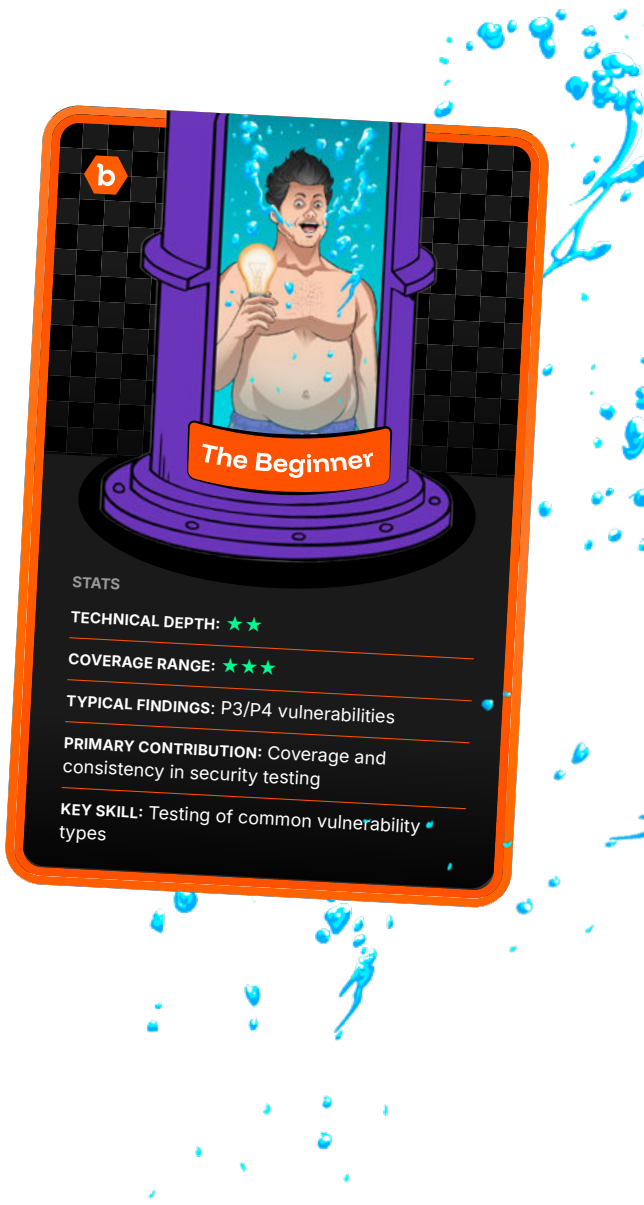
Let's explore the five different types so you can see how to best engage various hackers.

The Beginner

They may be called "Beginners," but don't underestimate their value– beginners are indispensable to well-rounded security testing. The term "Beginner" here specifically refers to researchers new to crowdsourced security, not necessarily those new to security work overall. They may have experience from other areas of security or IT, and in some cases on the platform, we label them as Beginners if we don't have additional information about them. They often identify P3/P4 vulnerabilities in authentication, authorization, and infrastructure configurations.

> **Their approach fosters comprehensive coverage of common security issues that require attention.**

Beginners often bring fresh perspectives to established programs, questioning assumptions that others take for granted. Many are actively expanding their skills through structured learning, making them highly motivated to thoroughly test everything they can think of. Their findings are often similar to those revealed by traditional penetration tests, providing baseline security coverage that's important to any organization.

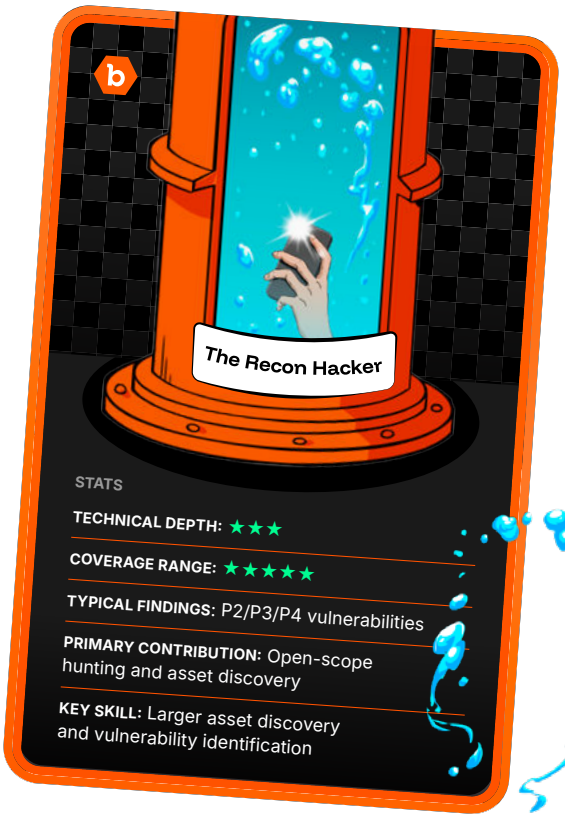


The Recon Hacker

Recon Hackers focus on identifying issues across the largest possible scope, using automated tools and techniques to map and analyze broad attack surfaces. These researchers excel at discovering P2/P3 issues that traditional penetration testing might miss.

> **They help larger organizations especially by discovering previously unknown assets and potential security gaps.**

These researchers often focus on specific types of vulnerabilities that can be identified at scale and likely appear in multiple programs they engage with, such as cloud misconfigurations or exposed assets. While many recon-focused hackers are highly skilled, they often specialize in refining their toolkits to exploit specific types of vulnerabilities at scale rather than diving deep into individual programs.

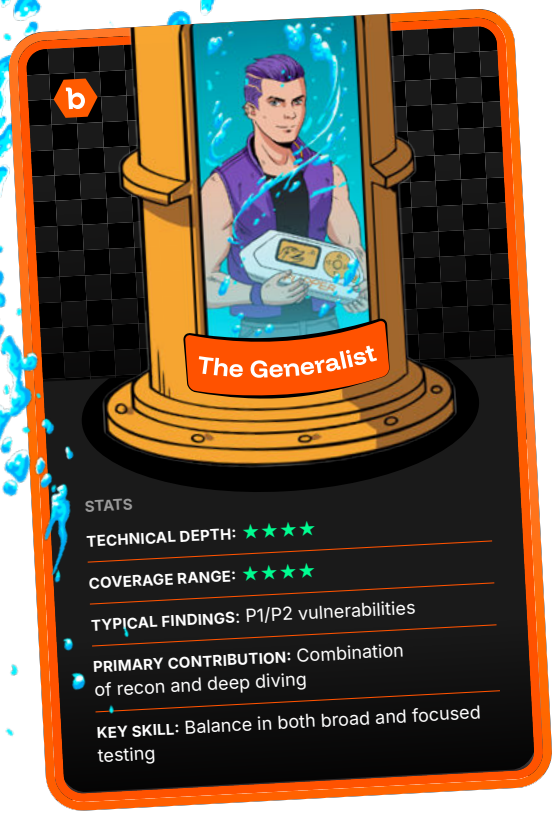


The Generalist

> **Generalists blend different security testing techniques, using both recon and deep-diving tactics in their role as all-around solid hackers.**

These versatile individuals maintain balanced toolkits that include both automated scanning tools and manual testing techniques. They quickly understand new systems and identify the most promising areas for detailed investigation.

Their strength lies in their adaptability, switching from broad scanning to focused testing as opportunities arise. These researchers usually work across multiple programs, building experience through many different security contexts and technologies. Rather than specializing in one approach, they maintain diverse skill sets that help them identify and investigate potential vulnerabilities using various methods. Since they can help out almost anywhere, it's no surprise that these hackers are highly valued at Bugcrowd.

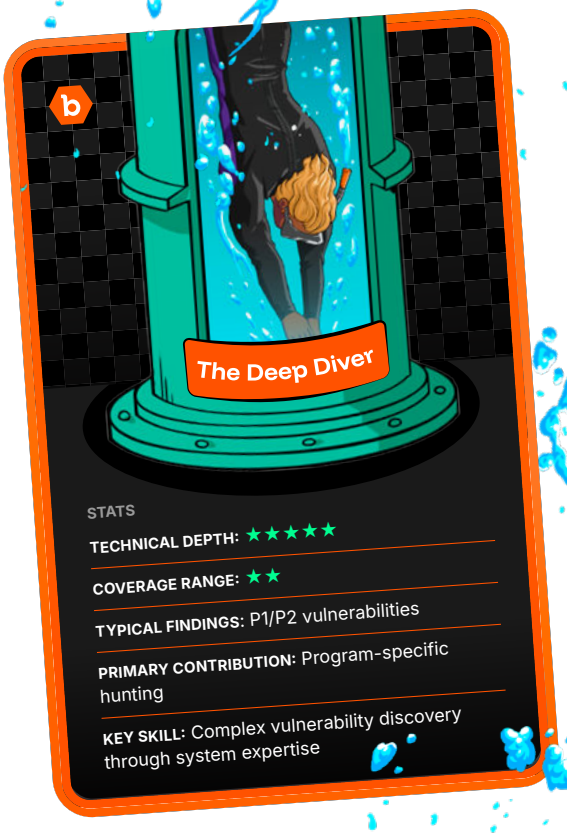


The Deep Diver

Deep Divers tend to focus on particular programs, going deep and learning as much as they can about them. Their hard-earned knowledge of how a program operates enables them to uncover vulnerabilities that others might miss. They're particularly valuable for mature programs where the obvious issues have been found, as they are masters of uncovering sophisticated vulnerabilities through their continued engagement.

> **To identify Deep Divers, Bugcrowd looks at the quality of these researchers' submissions rather than quantity alone.**

What sets them apart is the originality and depth of their findings—these hackers deliver insights that reflect both their persistence and specialized knowledge of the program they're testing. They may know your program better than you do, and that's exactly what you want.

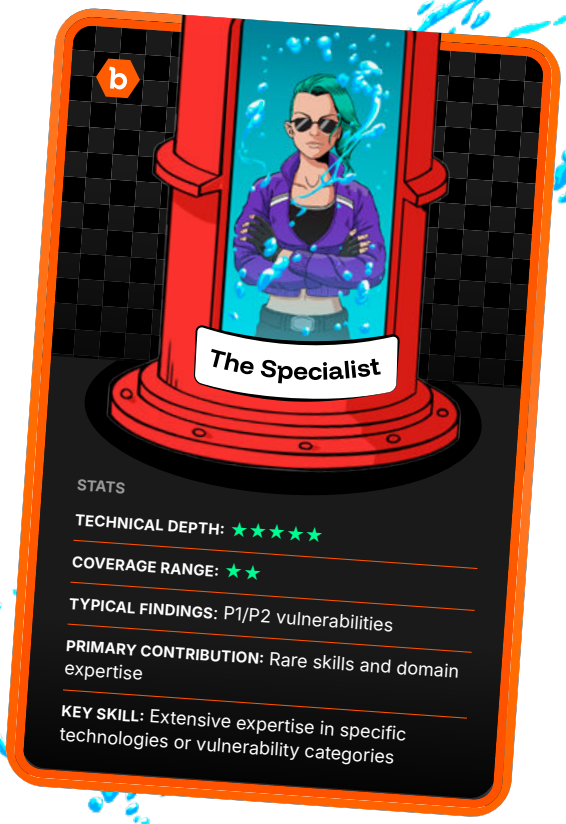


The Specialist

Specialists are the rare experts who have devoted years to mastering specific technologies or vulnerability types. They might be focused on emerging fields like AI security and Web3, complex domains like hardware security, or specific vulnerability categories like race conditions or cryptographic failures.

Their deep expertise allows them to find issues that other hackers might not even know to look for. Their specialized knowledge often extends beyond security into a deep technical understanding of their chosen domain, allowing them to identify subtle flaws that could be exploited. While they may participate in fewer programs, their specialized knowledge is particularly valuable when programs involve complex technologies or face unique security challenges.

> **Bugcrowd specifically sources and activates these rare experts when their unique skills are needed to meet a program's specific requirements.**



How to appeal to different types of hackers

Hacker motivations are the foundation of any crowdsourced security approach. Within any Bugcrowd program, many—if not all—of these motivations will influence the outcomes. Successful programs deliberately incorporate elements that resonate with different motivations to maximize reach and appeal across the hacker community.

Keeping our extrinsic and intrinsic motivators as focal points, Bugcrowd strives to architect engagements to meet those primary drivers. A healthy engagement will have elements that speak to many, if not all, of these motivations.

Here are some approaches that we recommend to create a compelling engagement that encourages hacker engagement:

Safe harbor

Establish a policy that allows hackers acting in good faith, as defined within the program, to provide security feedback without fear of legal repercussions.

Coordination disclosure

There is a shift in the security industry where we are collectively moving to be more transparent when it comes to vulnerabilities. Everyone has them. Many hackers like to speak about their techniques and approaches to discovering these vulnerabilities. This is actually a really beneficial practice for organizations, because when hackers openly share their processes, it helps the whole community improve. Once the issues have been remediated and are no longer a threat, giving approval to the community to share their success helps hackers build notoriety and educate other hackers.

Broad scope

Most engagements start very targeted, but most hackers look to fulfill their curiosity and expand their skillset by looking for specific types of scope. Having a wide and well-communicated scope for testing will allow those Specialists to engage directly.

Competitive rewards

Being competitive in your reward ranges will put you in the best position to compete for talent within that arena. We'll discuss this more later in the guide.

Solving your security challenges with hackers

Now that you have a better understanding of hackers and what makes them tick, you may be wondering, “How does all of this help me reach my security goals?”

Crowdsourced security encompasses a vast spectrum of offensive capabilities and approaches. Organizations tend to seek answers to questions such as:

How do I secure all of my assets within my budget?

How do I demonstrate security due diligence to my customers?

How do I simulate the approaches an adversary will use?

How do I find more critical vulnerabilities before an adversary does?

How do I validate that my existing protections are working?

These questions have given rise to various specialized security practices: penetration testing, red teaming, vulnerability disclosure, attack surface management, vulnerability assessments, and bug bounty programs. Each offers distinct advantages in addressing specific security challenges.

Let’s follow the security journey of an organization that starts with only a few assets and grows over time. We’ll see how security testing and hacker engagement evolve to match each stage of growth.

The security journey

Early stage and establishing a baseline

1 **Imagine an organization with seven new business-critical assets: a mix of web applications, APIs, an IoT device, and a mobile application.** While these assets have received some basic security scanning, their overall risk is largely unknown.

At this early stage, the priority is understanding basic security risks. The security team decides to hire a Generalist to help with the first steps:

- → Vulnerability assessments
- → Penetration testing
- → Establishing a security baseline
- → Compliance validation and due diligence
- → Set up regular engagement (quarterly or annual)

With their well-rounded expertise and a proven testing framework, a Generalist helps establish an assessment of the security posture of the assets and discerns easily identifiable vulnerabilities and their potential impact if exploited. However, as initial vulnerabilities are addressed, the organization naturally progresses toward working with Specialists and Deep Divers to uncover more complex security issues.

Growth stage and diversification

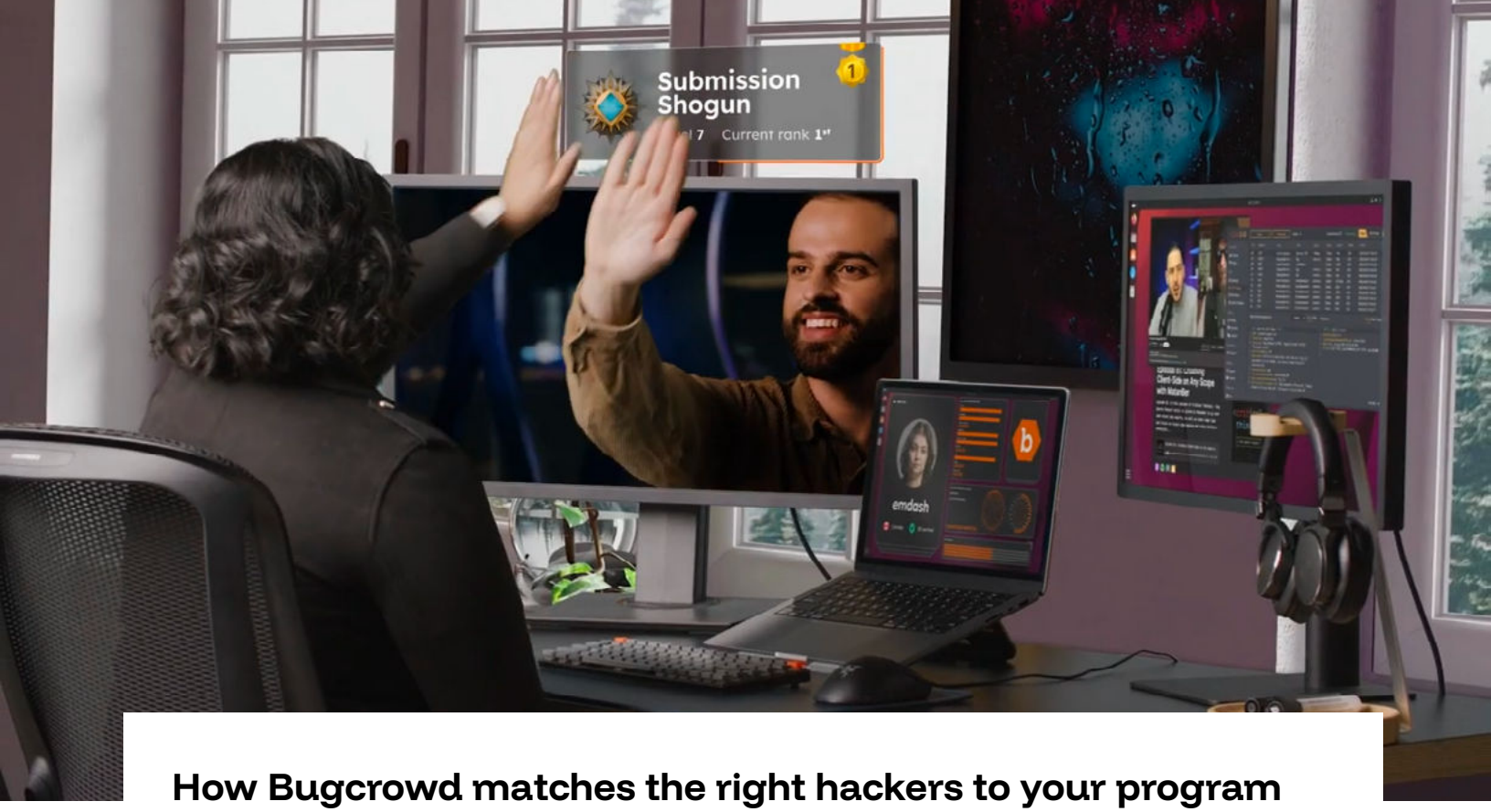
2 **As assets mature, security testing evolves to incorporate mixed teams and varied approaches.** The organization will likely want to start leveraging both Generalists and Beginners, moving beyond the initially defined methodologies into more exploratory testing. At this stage, security teams start seeking specialists based on asset type.

They also start to look for Specialists with deep expertise in specific areas like IoT, mobile, APIs, or particular tech stacks. This shift coincides with a move toward continuous testing to keep up with frequently changing assets.

Mature stage and advanced security

3 **At the most mature stage of testing, the focus shifts from methodological approaches to creative, adversarial thinking.** Continuous testing programs become the norm, engaging all hacker personas in a collaborative environment. Robust incentives and a strong emphasis on teamwork drive these engagements, mimicking the tactics of real-world adversarial groups, where individuals share approaches and iterate through them to achieve their objectives.

In this stage, organizations often use advanced testing models such as bug bounty programs, objective-driven testing, and red teaming.



How Bugcrowd matches the right hackers to your program

As you can see, organizations are inundated with choices when it comes to what type of hacker to apply to their use cases. Bugcrowd helps customers take a strategic approach to sourcing and engaging with hackers by matching customers to the appropriate roles based on program maturity and results.

For example, adding Beginners to a program that has been running for three months may lead to frustration and a high number of duplicates, while adding Generalists too early dilutes the ability of Beginners to up-level themselves through their findings. Our engineered approach helps maximize the contributions of each hacker role.

The answer to the question of which crowd to engage, and when, is something we've been refining for years. At the core of our platform is an AI model designed to map hacker performance, skill sets, accomplishments, and more to specific engagements.

This system ensures the right hackers are matched with the right programs at the right time. Our matching methodology serves two purposes: It helps organizations build resilient security programs while ensuring hackers receive opportunities that align with their skills, motivations, and goals.

Tips to improve your engagements and attract more hackers

Smooth and efficient collaborations with hackers are worth more than their weight in gold. Hiring full-time offensive security staff is time-consuming and expensive. Forrester Research's Total Economic Impact of Bugcrowd Managed Bug Bounty report found that working with hackers "improved security operations efficiency and helped the composite organization avoid hiring two full-time employees." An even more expensive burden is the cost of a breach.

In 2024, the average cost of a data breach was $4.88M. The cost of a hacker engagement is far lower than both of these outcomes. Even small, unoptimized hacker engagements can reap rewards. After all, you only pay for results in a crowdsourced model.

But, a few simple changes (e.g., in rewards, scope, and triage) can greatly increase the effectiveness of your engagement. We want to give you a clear list of changes to make your next hacker engagement even better. We'll cover:

1

Choosing the right scope

2

Setting the right rewards

3

Finding the right hackers

4

Creating an enticing project brief

5

Triaging effectively during an engagement

6

Other tips to maximize hacker engagement

1 Choosing the right scope

Setting a clear scope for an engagement is paramount. Without it, hackers may be confused on what is and isn't a target. Up front, this means fewer hackers will want to work on your engagement. Down the road, this means wasted time if a hacker works on the wrong part of your system.

In general, we recommend having as wide of a scope as possible. Vulnerabilities can hide in even the most innocuous parts of your systems. Additionally, threat actors don't think about specific targets when trying to break into your systems; they simply try to find any way in. By allowing hackers to do the same, you can root out the vulnerabilities threat actors would be likely to exploit. There are many examples of companies breached by a small hole in their attack surface.

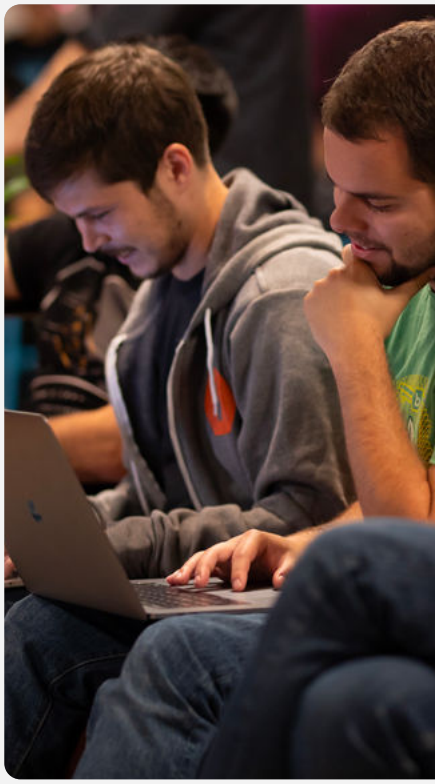
Hackers breached JP Morgan and compromised 83 million accounts via a single server that hadn't received an update to its MFA.

The numbers also support wider scopes. Engagements with a wider scope (with at least a wildcard) receive 250% more P1s than limited-scope engagements. Wider-scope engagements also get 2x the number of hackers, and these hackers stick around for longer. There are, understandably, concerns with a wider scope. Namely, people worry that hackers won't focus on the right targets. This can be solved with a good reward system, where vulnerabilities in desired targets pay more than vulnerabilities found in nontargets. For more information on wide scopes, check out this post.

What are the types of scope?

Three main types of engagement scope:

- **LIMITED SCOPE:** A limited scope only contains very specific targets. Including only "example.com" and "accounts.example.com" would be an example of a limited scope.
- **WIDE SCOPE:** A wide scope includes a wildcard in its targets. "*.example.com" would allow a hacker to test any subdomain under "example.com," including forgotten staging sites that often contain hidden vulnerabilities.
- **OPEN SCOPE:** An open scope has no restrictions on what hackers can target, as long as the target belongs to a specified company. For example, archived GitHub repos would be fair game (and may have secrets that should be scrubbed). Here, hackers can use their detection skills to the fullest to find vulnerabilities.



Ask a hacker

Scope

"Throughout my work, I've discovered significant and critical issues that, while outside program scope, posed immediate and impactful risks. If hackers like me aren't provided with a way to report these issues, it ultimately becomes a lose-lose situation: no bounty for me or other hackers and the real risk of a bad actor infiltrating your assets. Remember, no matter the scope of a bug bounty program, malicious hackers looking to steal data or plant ransomware are not limited to the defined scope.

> **Having flexibility in your scope gives you an opportunity to let the responsible hackers find these vulnerabilities and notify you before the malicious hackers have a chance to exploit them.**

This approach transforms a potential lose-lose scenario into a significant win-win opportunity. Putting your assets under the microscope might feel overwhelming at first, and I empathize with any concerns you might have. However, in the end, this openness will make your organization safer."

Todayisnew

2 Setting the right rewards

For bug bounties specifically, the reward structure has a significant effect on engagement success. The biggest obstacle we see in setting the right rewards is undervaluing caught vulnerabilities. A few thousand dollars can seem like a lot, especially to security teams with tight budgets. One way to think about this cost is to consider how much an uncaught vulnerability would cost. Earlier, we mentioned that the average data breach costs $4.35M. Relative to that, paying out a few P1s and P2s is not so bad. Additionally, only valid vulnerabilities get rewards, which promotes efficient searching on the part of hackers.

The other obstacle is figuring out how much to pay for each vulnerability. It's hard to quantify how much an individual vulnerability can affect the attack surface. We developed a reward recommendation framework to solve this problem.

Severity Level Per Vulnerability Rating Taxonomy (VRT)	P1	P2	P3	P4
Low Range ● (Attracts generalists)	$3,500-$4,500	$1,500-$2,500	$500-$750	$175-$225
Mid Range ● (Attracts experienced hackers)	$5,500-$7,500	$2,500-$3,500	$750-$1,500	$250-$500
High Range ● (Attracts P1 specialists)	$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

Low Range

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

Mid Range

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

High Range

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

We created these ranges based on the most successful bug bounties we've seen, adjusting for vulnerability types and security levels. We recommend these ranges for most bug bounties, unless you have very specific scopes or needs for specific hackers.

3 Finding the right hackers

Ordinarily, this would be one of the hardest parts of the whole security engagement process, but Bugcrowd actually handles this for our customers. Our security experts work directly with companies and source hackers for their specific needs and engagements. We also use our CrowdMatch feature (which draws on the mountain of data we have on engagement requirements and hacker skills) to find the best hackers for each engagement.

CrowdMatch-sourced hackers find 70% more vulnerabilities and twice the number of critical vulnerabilities. Finding the right hackers really pays off.

4 Creating an enticing project brief

At this point, if you have followed the outlined steps, you will have done a lot of the work needed to create a successful hacker engagement. Making this work evident to hackers is the final step to generating a lot of hacker interest. For pen tests, you'll correspond directly with specific hackers, and Bugcrowd will help convey the scope of your engagement. For bug bounties and VDPs, a clear and enticing project brief is the main tool to get hackers interested in your engagement. "Clear" and "enticing" are terms that can feel rather nebulous, so we've broken down what we've seen the best project briefs do. The best briefs:

- Have a recognizable name and a pithy tagline
- Clearly outlines the scope of a project
- Use a well-known vulnerability prioritization taxonomy
- Provide clear instructions on accessing the relevant targets
- Explicitly mention safe harbor
- Detail the reporting recommendations.

We break down all six of these tips in depth here.

Anatomy of a Bug Bounty Brief

A handy infographic that guides you when developing your brief

1 Organization name

3 Focus areas

This is a great opportunity to let hackers know what's important to you and draw attention to it.

Focus areas highlight:

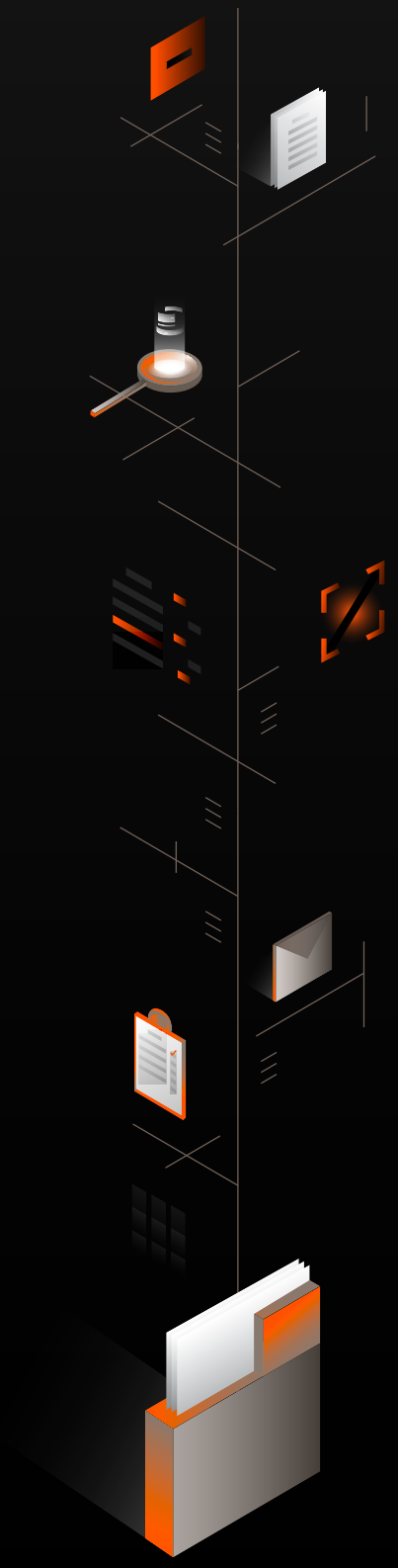
- Areas of concern or critical functionality
- New features/functionalities
- Overlooked or complex targets

5 Exclusions

Guide hackers in the right direction by clearly stating any exclusions to your engagement's scope. Bugcrowd's Vulnerability Rating Taxonomy (VRT) is a great resource for vulnerability best practices. We specifically recommend adding P5 vulnerabilities as the first line under your exclusions to reduce noise.

7 Disclosure and rules

Public disclosure is an important part of the vulnerability reporting process. While we respect each customer's specific disclosure policies and unique use cases, we nonetheless recommend collaborating with hackers to transparently share resolved vulnerabilities. This approach fosters goodwill and strengthens relationships within the hacker community. That being said, coordinated disclosure is the default policy for all new engagements. Hackers can request to disclose their submission once the vulnerability has been fixed.



2 Scope

It's critical to define a clear and available scope, leaving nothing open to interpretation. Ensure your engagement stands out by evaluating your attack surface and unique goals and creating a compelling bounty scope that motivates hackers. Design a compelling bounty brief by:

- Opting for a wide scope
- Offering large rewards
  (ideally with wildcarded domains)
- Answering questions before they can be asked; it's best to be as informative as possible

4 Out of scope

What is out of scope is just as critical as what is in scope. Mention:

- Third-party services
- Areas of your scope that may be exceptions to in scope
- Similarly named/geographically operated locations

6 Rewards

To meet your organization's unique goals, aim to pique hackers' interest—increase brand recognition, create interesting targets, build rapport with the community, offer leaderboard recognition, and of course, give cash rewards. We strongly encourage all customers to offer cash rewards, combined with a strong, well-thought-out scope, for an ideal engagement. Don't know where to start with reward payouts? Check out our recommended bounty reward ranges.

Ultimately, your bounty brief is a work agreement between you and the hacker. Make sure it's complete to ensure a successful engagement.

5 Triaging during an engagement

A smooth triage and reward process drives hacker engagement. Quick and clear bug triage gives hackers the feedback they need to maximize the impact of their work. In fact, 89% of hackers seek constructive criticism on their work. It also gives companies time to investigate and patch severe vulnerabilities.

With some upfront work, triage can be easy. If you use a well-defined vulnerability rating system, such as Bugcrowd's VRT, you don't need to spend much time scoring vulnerabilities. A hacker will submit a bug report, and the VRT will determine the bug's severity. We also have our own triage team that will de-dupe, reproduce, and rate every single vulnerability in a Bugcrowd engagement. Hackers get quick feedback from known, trusted members of our triage team. The VRT leaves no room for ambiguity on a vulnerability's severity either.

The result is a clear, quick triage—hackers get on the right track and get rewarded, and companies find vulnerabilities with little back-and-forth.

6 Other tips to maximize hacker engagement

There are so many levers an organization can pull to improve hacker engagement on their crowdsourced security programs. Here are a few more that are important to keep in mind:

Regularly review your program

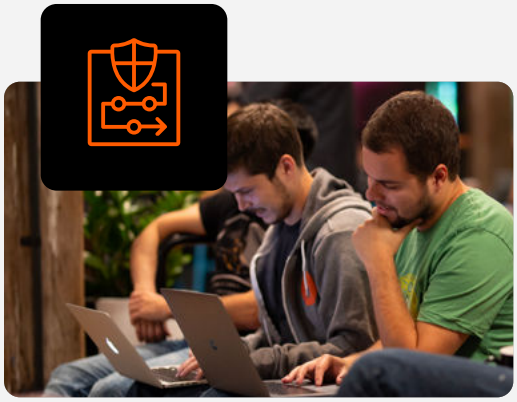
With a good crowdsourced security engagement, you want to regularly review your progress and adjust certain levers. As your program matures, you should review and adjust every 6–12 months to bring long-term success.

Adding incentives

Setting the right rewards is important, but an additional way to help your engagement attract hackers is by introducing new incentives. For example, you could run competitions, offer bonuses, or have challenges on your engagement.

Communication

Good communication is a simple but crucial way to help your engagement stand out. Hackers love working on engagements that provide prompt responses and updates on inquiries, give kudos for good work, and pay on time.



These simple tips foster better long-term relationships with hackers so they're more likely to deep-dive into your engagement and flag it as one of their favorite engagements to work on.

Ask a hacker

Triage

darkieduck

"Bugcrowd's Triage team is exceptional to work with.

The team has grown significantly, to the point where P1s now get triaged within the hour. Their communication is excellent, and I've encountered very few problems getting my reports triaged."

What does a great hacker engagement look like?

To start, organizations need to choose the right engagement type—whether VDPs, bug bounty programs, penetration testing, or red teaming. Whether a specific type of engagement is right for your company depends on your company's security experience, system complexity, and attack surface. This blog post will help you decide between common engagement types.

From there, you want to start measuring hacking engagement. A successful hacker engagement will feel more productive. It will seem like it's easy to communicate with hackers. Furthermore, you'll get the sense that they're focusing on the exact targets you really care about. Triaging vulnerabilities will follow a clear priority list, and payouts will feel really worth it.

We can't rely exclusively on qualitative measures, so here are five key metrics that will tell you you're on the right track.

Number of critical reports accepted and rewarded in the last month/ quarter/year

Everyone, especially hackers, loves to see P1s and P2s. When hackers find one and it's triaged as valid (and the hackers are then rewarded quickly), this is likely to motivate hackers to hunt for more. It's rare that a hacker finds a P1 on a target and decides to change engagements out of the blue. More often than not, they stick with an engagement for long enough to familiarize themselves with its targets before moving on to the next.

1

Rewards given in the last month/ quarter/year

What you have spent in a given period is going toward valid reports that are useful and valuable to you. If you are topping up the reward pool on a regular basis, that's usually a good sign that your program is doing well. This is also the easiest and quickest way to get a pulse on your engagement success.

2

Hacker consistency

You are probably already familiar with a few names on your engagement, which is a good thing! This means you have acquired the loyalty of a few top hackers in the crowd. Hackers display greater loyalty when they feel respected and well-treated when submitting reports. As such, it is essential that you respond quickly, reward fairly, and are looking for a collaboration and not just a service.

3

Hacker variety

The opposite can also be true from a different perspective, especially on public engagements. When many different hackers are hunting on your targets and submitting vulnerabilities, it usually means that your brief is enticing and attracting talent. It stands out among other engagements, and hackers want to test their skills against your assets. You want this variety of talent in your engagement, so embrace it. Maybe you can turn them into loyal testers in the future!

4

Processing queue > 0

Submissions simply don't stop coming in! They may or may not be exactly what you want or expect, but it's a great indicator of engagement from the crowd. If this happens as a consequence of a recommendation your TCSM gave you, even better! This means that it's working and that you can apply the recommendations again in the future to try and achieve the same or better results.

5

In addition to these metrics, you can also track:

- **Submissions per month**
- **Valid P1/P2 findings per month**
- **Dollars awarded per month**
- **Valid submissions per month**

Our Metrics that Matter guide shares more details around these metrics and best practices to define bug bounty program goals.

How Bugcrowd fosters better hacker relationships

As you can see, many things factor into a great engagement. A clear scope, good rewards, and detailed briefs are just a few of the things you should consider. Bugcrowd makes the process a lot easier by helping you draft your brief, finding your perfect hackers (via CrowdMatch), and triaging all your bugs quickly. But the most crucial thing Bugcrowd does is get great hackers on our platform. Only then can we help you get these hackers working on your engagement.

To attract—and retain—great hackers on Bugcrowd, we do the utmost to help hackers reach their full potential in three ways:

We listen to hackers constantly

We host a variety of events

We help hackers upskill

Bugcrowd's Creators Program

Bugcrowd's Creators Program is a place where talented hackers bring together their collective expertise to strengthen the cybersecurity industry. Selected creators receive financial rewards for contributing their hacking mastery, technical proficiency, and community education. This collaborative approach between Bugcrowd and hackers allows the broader security community to harness diverse hacker perspectives while providing hackers unique and legitimate opportunities to get paid and grow in their field.

Opportunities include:

- **Written thought pieces**
- **Technical blogs**
- **Technical videos**
- **Interviews**
- **Podcasts**
- **Event presentations**
- **Q&A sessions with customers**

We consistently talk to hackers about their Bugcrowd experience to improve our products. We invite some of the most engaged and skilled hackers to serve on our Hacker Advisory Board (HAB). Our HAB meets frequently to provide feedback on Bugcrowd and improve the hacker experience. Quarterly, we send a survey to our large hacker base to better understand their experiences. We combine the focused feedback from our HAB with the quantitative data from the survey to improve our hacker products.

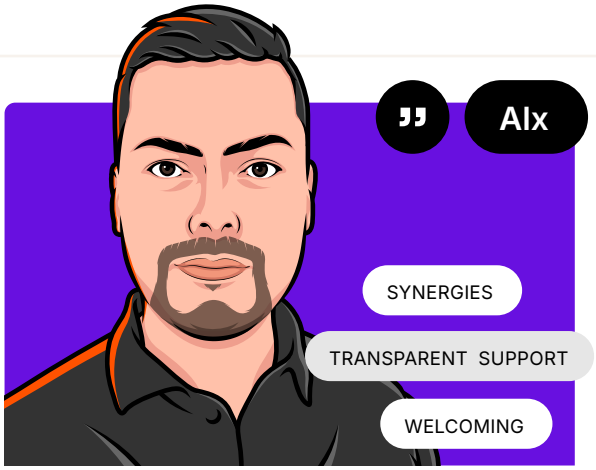
78% of hackers are self-taught, and they want to learn more. We publish LevelUp, a series of educational resources, to help these hackers become more skilled. With LevelUp, hackers can learn from some of the most experienced hackers in the field to improve both their foundational skills (e.g., programming) and advanced hacking techniques.

We host in-person and virtual competitions year-round for hackers to team up and outdo one another in digging up vulnerabilities. We also host bug bashes. In 2024, we hosted a bug bash with T-Mobile where hackers got an exclusive chance to root around with T-Mobile hardware. At these events, hackers bring their friends, meet other hackers, and become a part of the Bugcrowd community. Additionally, we host live and virtual CTFs for hackers to test their skills at a variety of levels. Each Bugcrowd CTF requires unique strategies, an eye for detail, and often team collaboration, if participants are serious about taking home the prize!

All this effort means great hackers work with Bugcrowd (and, by extension, you). But don't just take our word for it. Hackers can put their experiences into better words than we can:

Why hackers choose Bugcrowd

See what sets Bugcrowd apart from the rest and why hackers continue to work with Bugcrowd project after project.



Bugcrowd has a structured and transparent support system for hackers when it comes to submissions.

Neither evaluation nor handling is volatile, which is very different compared to my experiences with other platforms. Bugcrowd also welcomes and guides people who show promise, giving them the ability to grow. Through events, I've had the chance to work with people who became friends, and together, we've created amazing synergies.
I strongly believe that this kind of teamwork always outperforms the lone-wolf approach."

A big reason I hunt with Bugcrowd is that it's where I had my first real success in bug bounty, and that win kept me coming back. Over time, Bugcrowd has built an experience that keeps things engaging and motivating, especially with the gamification aspects. Staying in the top 60 on the platform has been a fun challenge that pushes me to keep honing my skills. But what's really kept me with Bugcrowd, even after trying other platforms, is the way it treats hackers.

It genuinely respects the work we do, and that makes a big difference.

godiego

What I really appreciate about Bugcrowd is how familiar it feels and how well the team takes care of hackers.

You can always message people directly, and it feels much less corporate than other platforms, where you're treated as just another number. This personal touch is especially evident during in-person hacking events.

PERSONAL TOUCH
LESS CORPORATE

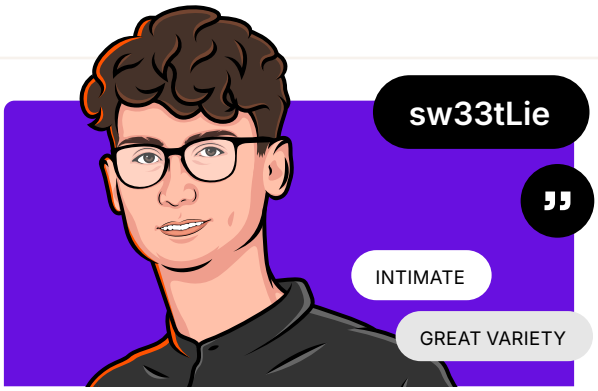
Why hackers choose Bugcrowd

There are many reasons why I choose to hack on Bugcrowd. First, its reporting form is clear and easy to understand, and the VRT is exceptional. The way programs are sorted and displayed is impressive, and I particularly appreciate how easy it is to access previous reports and keep separate reports for each program. The Triage team stands out for being fast, smart, and most importantly, cooperative—something that's rare on other platforms.

You can communicate with Support immediately through multiple channels, and the team members are consistently responsive. The challenges, events, and swag are amazing.

I love how the Bugcrowd team is always first to congratulate hackers on Twitter when they report bugs or receive bounties.

EASY TO UNDERSTAND



Bugcrowd's triage time, especially for P1s, is better than that of any other platform. They offer solid programs with great variety, including many high-paying ones with an extensive scope.

It's also easy to communicate with the Bugcrowd team on Slack and through support tickets. The Request a Response feature is particularly useful, and the platform works well overall. I especially like the VRT. While these might seem like small things, they're actually the key elements that make a platform great.

Bugcrowd offers a more private and intimate experience—you can see this in how the platform is designed, where you can hide your profile and stats, unlike on other platforms.

I chose Bugcrowd because it's the best platform when it comes to bug bounties. The programs are amazing, and the Triage team is really helpful whenever a hacker submits a report.

HELPFUL

bugcrowd

PLATFORM TOUR

See the Bugcrowd Platform in action

Take a 5-minute tour to get an overview of how the Bugcrowd Platform connects you with trusted hackers to help you take back control and stay ahead of attackers.

Unleash Human Creativity for Proactive Security

Try Bugcrowd