hackerone

THE BEGINNER'S GUIDE TO

Hacker Powered Security for Financial Services

WHAT IS HACKER POWERED SECURITY?

Hacker Powered Security is simply the act of engaging with the external hacker community to find unknown security vulnerabilities and reduce cyber risk. Common examples include private bug bounty programs, public bug bounty programs, time-bound bug bounty programs and vulnerability disclosure policies. With hacker-powered security testing, organisations can identify high-value bugs faster with help from the results-driven ethical hacker community.

WHY DO I NEED HACKER POWERED SECURITY?

In a survey of 600 European security leaders across a number of industries including financial services and retail, 83% considered software vulnerabilities a significant threat to their organisation and 86% said that software projects are stifled due to fears of inevitable security issues.

Reduce risk, launch products faster and strengthen your brand by incentivising third party researchers to review your assets and find weaknesses that might otherwise have been missed, posing a risk to the security of your business. Every 5 minutes, a hacker reports a vulnerability on HackerOne's platform. In 77% of the cases, hackers find the first valid vulnerability in the first 24 hours.

The benefits of hacker-powered security are many, from improving on traditional pen tests by identifying 10-times the number of critical vulnerabilities to identifying dozens or hundreds of vulnerabilities in a few days to spending just a fraction of a security engineer's salary while paying only for validated results.

Even government regulators and industry groups are imploring organisations to use hacker powered security, publish VDPs, and consider bug bounty programs. The practice has been outlined by the European Union Agency for and in ISO 29147.

LIVE TALK

"We need to move to a world where...all companies providing internet services and devices adhere to a vulnerability disclosure policy."

JULIAN KING,
SECURITY UNION COMMISSIONER,
EUROPEAN COMMISSION

WHO ARE THESE HACKERS?

57% of security leaders would rather accept the risk of software vulnerabilities than invite unknown hackers to find them. The cyber criminals are going to hack you anyway, we say you may as well invite the ethical hackers to find vulnerabilities first.

We know that the hacker community is filled with smart, curious, collaborative human beings. Over 80% of hackers are under the age of 35, eight out of ten are self-taught and 40% are IT professionals. They come from over 90 countries including the US, India, Russia. The biggest takeaway of the 2020 Hacker Report was that the ethical hacking community is eager to do good in the world. They are already finding vulnerabilities. Hackers are motivated by opportunities to learn, be challenged and have fun more than money. While money definitely still attracts hackers to different programs, it's not the key driver of what they do.

79% of programs on HackerOne are private, meaning that select hackers are invited to participate so you can retain control over who is actively hacking.

LIVE TALK

"I'm a good guy. I don't want to hurt anybody. I just like breaking stuff and helping people. That's what HackerOne allows me to do without legal risks which is awesome. I want to hack companies to help them, and it's so rewarding to see that they finally learned to appreciate the work of ethical hackers. I love it."

@INTIDIC,
HACKER

WHO IS ALREADY DOING THIS?

Adoption of hacker powered security is growing in every sector from government departments and large enterprises to tech start-ups and online retailers. Goldman Sachs, PayPal, Starling Bank, Lending Club, Coinbase, The Department of Defense, The European Commission and Microsoft are just some of the organisations that have embraced hackers to help them shore up their defences.

LIVE TALK

"In addition to some amazing, creative submissions, we've received some incredible feedback from researchers. In just a few short months, we've used that feedback to make substantial changes to our scope, payments, and transparency. We want hackers to challenge and educate us, and build a trusting and respectful relationship that goes both ways."

PAX WHITMORE,
SECURITY ENGINEER AT PAYPAL

RESPONSE

A VDP is usually the first step to working with hackers. A Vulnerability Disclosure Policy simply provides a mechanism for anyone to report a potential vulnerability; it is table stakes for security in today's digital world. It can be as simple as a monitored email address, but even a detailed VDP need not be more than a page or two of rules, scope, and expectations. The intent is to give discoverers a clear and concise path to follow when they find a potential bug, and also let them know what you expect from them (report details, disclosure limits, etc.) and what they should expect from you (response time, disclosure timing, communication frequency, etc.).

Internally, a VDP will also help you create your process for monitoring, managing, vetting, responding to, and fixing reported vulnerabilities. It's a great first step to dealing with incoming bug reports and building a team and a process for handling those reports.

5 Critical Components of a VDP

1. **PROMISE:** Demonstrate a clear, good faith commitment to customers and other stakeholders potentially impacted by security vulnerabilities.

2. **SCOPE:** Indicate what properties, products, and vulnerability types are covered.

3 **"SAFE HARBOR":** Assures that reporters of good faith will not be unduly penalized

4. **PROCESS:** The process finders use to report vulnerabilities.

5. **PREFERENCES:** A living document that sets expectations for preferences and priorities regarding how reports will be evaluated.

Featured Case Studies

General Motors: Learn why hackers have become an essential part of their security apparatus.

AlienVault: Read how they moved from an email-driven VDP to a holistic program that helps them realize response times of 48 hours or less.

CHALLENGE

Next, short-term hacker-powered programs can be used to replace or augment your existing penetration tests by having hackers focus on a specific attack surface for a limited time. It's a great way to evaluate the benefits and impact of a broader bug bounty program and get more from your pen test budget. How you set bounty values can also help you manage report volumes or aim attention at specific areas of concern.

In the survey of security leaders, 45% admitted that pentests don't provide sufficient results to keep up with the pace of development. However, one organization detailed how hacker-powered pentests helped them eliminate $156,784 in total costs and save an additional $384,793 over 3 years by reducing internal security and application development efforts.

A typical HackerOne Challenge lasts just 4 weeks. In week one, the project's scope is defined and hackers are invited. Hackers then test the target properties and applications in weeks two and three while internal security teams and/or HackerOne experts triage incoming reports. Finally, in week four, the results are reviewed and a final, formal report is delivered.

Featured Case Studies

European Commission: Read how hackers helped fix a 20 year old bug as part of the EC's EU-FOSSA initiative.

Oath: Learn how their bug bounty challenge resulted in bounty awards of over $400,000 in a single day.

BOUNTY

Moving to a private, targeted bug bounty program is the next step in the hacker-powered security journey. A private program allows you to further hone and test your internal processes while limiting the number of hackers involved, the volume of incoming reports, and public awareness of the program. A private program also lets you view the potential size and cost of a broader bounty program, giving you time to scale your internal teams and processes to match and enabling you to build an accurate bounty table that works for your organisation. After running a private or time-bound bounty program, you're ready to open your technology up to a continuous public bug bounty program.

No matter how you choose to structure your bug bounty program, it can be entirely private, public, or anywhere in between. Here's how they differ.

Private programs are known only to those hackers you specifically choose to invite based on skills, experience, location, or other attributes. But, every report, participant, bounty, and other aspect of the program is totally private.

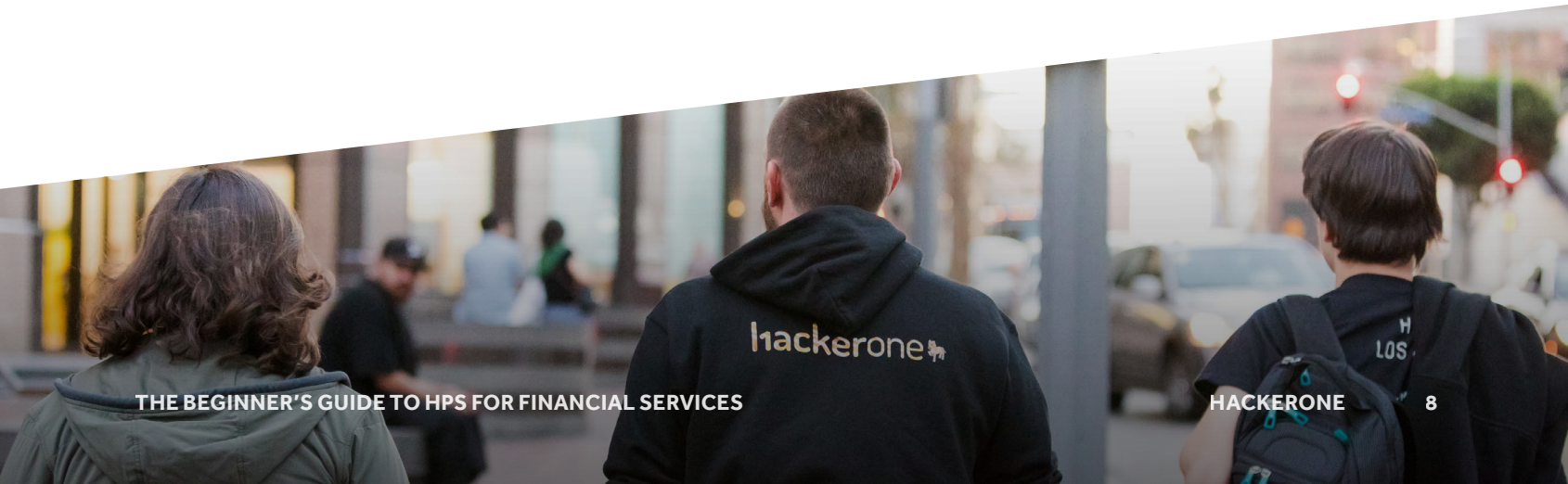
Public programs are open to all hackers and can maximize both your program's visibility and the volume of participants and their varying skills. It gives you better coverage and exposure to hackers, and can also be publicized to show your customers how much effort you're putting into security. But even with a public program, bug reports can remain private and redacted, disclosure timeframes are up to you, bounty values are yours to set, and many other elements can be controlled as you wish. On average, public programs engage 3.5 times the number of hackers reporting valid vulnerabilities.

Private bug bounty programs currently make up 79% of all bug bounty programs on HackerOne. For those who want more control over their programs, HackerOne Clear provides access to only vetted, background checked hackers.

Featured Case Studies

ABOUT YOU: Learn how they saved money on security testing and supplemented their internal teams with hacker powered security.

PayPal: Read about how with a public program they resolved over 300 vulnerabilities thanks to 1,000+ hackers.



ABOUT US

HackerOne is the #1 hacker-powered security platform, helping organisations find and fix critical vulnerabilities before they can be exploited. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security alternative. With over 1,600 customer programs, including The U.S. Department of Defense, General Motors, Google, Goldman Sachs, PayPal, Hyatt, Twitter, GitHub, Nintendo, Lufthansa, Microsoft, MINDEF Singapore, Panasonic Avionics, Qualcomm, Starbucks, Dropbox, Intel, HackerOne has helped to find over 140,000 vulnerabilities and award over $74M in bug bounties to a growing community of over 570,000 hackers. HackerOne is headquartered in San Francisco with offices in London, New York, the Netherlands, France and Singapore.

Do you require strict finder verification capabilities or secure VPN technology to satisfy legal requirements? Download the datasheets to learn about HackerOne's Advanced Vetting or VPN.

hackerone

Contact us to get started.