GITLAB'S APPROACH TO SECURITY:

AN INHERENT FOCUS ON TRANSPARENCY AND COMMUNITY

The openness of this DevOps software company extends to security, and steered their hacker-powered security program from a small vulnerability disclosure policy (VDP) to one paying more than $1 million in bounty awards.

GitLab | hackerone

CUSTOMER DATA

PRODUCT TYPE

HackerOne Bounty

LAUNCH DATE

June 2014

TOTAL BOUNTIES PAID

>$1,200,000

AVERAGE RESPONSE TIME

1 Hour

REPORTS RESOLVED

>550

COMPANY SIZE

>1,250 Employees
>3,000 Contributors

INDUSTRY

Software

HACKERS THANKED

297

TOP BOUNTY AWARD

$20,000

AVERAGE BOUNTY AWARD

$1,000

GitLab takes a transparent, community-driven approach to security, so **100,000 customers** can trust them to protect their software projects.

GitLab calls themselves an "open core company," working to create software to help companies manage their own software development lifecycle. Their software is used to manage the entire DevOps lifecycle, and is used by more than 100,000 organizations around the world. Their unique open source development approach has built an active community of more than 3,000 contributors who've helped build a product suite that fundamentally changes the way development, security, and operations teams collaborate and build software.

With their commitment to the global community of code contributors, it's no wonder GitLab readily embraced the idea of hacker-powered security. Their idea of creating "a world where everyone can contribute" aligns perfectly with the goals of the global security research community. But even as GitLab started their hacker-powered security program with a simple VDP, they eventually ramped up to become one of HackerOne's largest programs by increasing average bounties, quickly paying awards, and openly communicating with security researchers. Fast forward to today and GitLab has paid out more than $1 million in bounty awards.

SCALING SECURITY FROM SCRATCH

The GitLab security team began with a vision to align security with the company's open source strategy. Leveraging the expertise and resourcefulness of the community was an effective way to compliment the security team and achieve this goal. Simply adding more members to the internal team at the rate of rapid growth they were experiencing wasn't feasible.

In addition to their open source commitment, GitLab also had a core set of security tenets, which they called their "basic truths." First, a strong security posture required a balance of people, process, and technology. Second, security must also enable the business. And, third, nothing is ever fully secure and only a multilayered approach can effectively reduce risk. Those points combine to guide both their proactive and reactive security measures. As their security team grew and learned, they built programs to educate developers on secure coding and development and employed industry-leading static and dynamic vulnerability scanners. However, no single method is foolproof, hence the need for reactive readiness.

GitLab believes everyone can contribute, including efforts to secure and strengthen their product and company. When the company's growth began to scale, the global hacker community was seen as a valuable extension of their reactive security strategy, and gave their security team the flexibility to focus on building out areas like application security and security operations. But even with the way they embrace open source, GitLab opted to start small with a vulnerability disclosure policy (VDP), which first opened in 2014, then grew slowly over time. It's deemed the "crawl, walk, run" approach, and it helped GitLab scale in a manageable and methodical way.

GitLab's Core Security Tenets:

1. **A strong security posture requires a balance of people, process, and technology.**
2. **Security must also enable the business.**
3. **Nothing is ever fully secure and only a multilayered approach can effectively reduce risk.**

VDP AS EDUCATION

VDPs are a security best practice for every organization, regardless of size or industry. They're also a great way to start engaging with the hacker community and ramping up internal security team efforts around triage, communication, and management of internal processes required to evaluate and route incoming reports to resolution.

VDPs need not be expensive or difficult to create. Initially, GitLab's public VDP didn't offer bounties, as most don't. Recognizing the value of the community's efforts, however, the team started offering GitLab swag in exchange for bug reports. It was a smart and simple move that endeared the company to the hacker community.

"Fostering relationships with the hacker community is similar to fostering relationships with the development community," said James Ritchey, security manager at GitLab, who leads their Bug Bounty program. "Key points include transparent communication, building trust, respecting and valuing their input, and showing appreciation by rewarding contributions. Using the HackerOne platform helps us cultivate those relationships, and complements the GitLab mission that everyone can contribute."

> **"Using the HackerOne platform helps us cultivate (hacker) relationships and complements the GitLab mission that everyone can contribute."**
>
> **JAMES RITCHEY**
>
> **SECURITY AND BUG BOUNTY PROGRAM MANAGER, GITLAB**

The slower pace and smaller scale of a VDP gave the team time to build the processes and policies that would eventually support a more incentive-driven bug bounty program.

"Ensuring you've established the appropriate staffing levels and support structure are key to success when starting a bug bounty program," says Johnathan Hunt, VP of security at GitLab. "This includes security engineers to review, validate and triage the findings who can work across the development groups to test and mitigate."

GitLab used the VDP as an evolutionary step towards a future bug bounty program, and learned to effectively manage and resolve reports while building much goodwill with the hacker community. It also provided learnings on hacker expectations, yet cost them a little more than some GitLab swag.

GRADUATING TO A BUG BOUNTY PROGRAM

After a couple years growing and improving their VDP and learning how to better engage with the hacker community, GitLab launched a small, private bug bounty program in December 2017.

"We were ready for a private program, open to a small pool of researchers, where we were able to get our feet wet, build out our AppSec team and develop and establish our bug bounty triage, response, and disclosure processes," recalled James Ritchey, security and bug bounty program manager at GitLab.

As GitLab continued to develop and strengthen their internal processes, they also looked to improve the way they engaged with hackers by starting an invitation-only bug bounty program. Offering bounties let hackers see that they were valued; it also increased hacker expectations around communications and response times. However, GitLab was able to rely on HackerOne's expertise to support their program's growth.

"Pairing with HackerOne to manage our bug bounty program gave us immediate access to deeply talented security researchers, helping us hit the ground running, " said Ritchey. "It also allowed us to focus on other areas required to rapidly scale up our security department."

> **"Pairing with HackerOne to manage our bug bounty program gave us immediate access to deeply talented security researchers, helping us hit the ground running."**
>
> **JAMES RITCHEY**
>
> **SECURITY AND BUG BOUNTY PROGRAM MANAGER, GITLAB**

Combined with their VDP, GitLab's private bounty program helped identify and resolve nearly 250 vulnerabilities with the help of over 100 hackers. The private program paid out $194,700 in bounties and gave them the confidence to expand even more with a public bug bounty program.

"Overall, we consider our private bug bounty and public VDP quite successful," adds Johnathan Hunt, VP of security at GitLab. "It allowed us to foster relationships with several hackers we still work with today and to iterate on our program and processes including triage, response times and the use of automation so we can ensure a positive experience for the hackers that contribute to our program."

GOING PUBLIC WITH BUG BOUNTIES

As GitLab's private bug bounty program continued, they focused on key metrics and lessons learned to improve the program. Looking at the number of reports received per month, for example, helped them determine the appropriate level for bounty awards. They also used feedback from hackers to adjust and accelerate the payment schedule on awards, build automated responses and updates using GitLab APIs, and refine their internal triage process.

However, GitLab thrives on transparency, a core value of theirs, and something which is limited in a private bug bounty program. What's more, hackers themselves use public vulnerability reports as a way to showcase their techniques and share valuable learnings with one another. So, exactly one year after launching their private bounty program, GitLab decided it was time to open it up to all hackers as a public program.

"As we grew our security and appsec teams and seasoned our processes around how we prioritize reports and collaborate internally to define and implement fixes, we quickly understood we'd want an open, public program where an entire community of security researchers could contribute," said Ritchey. "HackerOne was able to provide us with relevant metrics and logistics to consider so we could ensure success and make an informed decision around timing."

In the program's first year, 513 hackers from around the world submitted 1,378 reports. GitLab paid more than $565,000 to the 171 hackers who reported valid vulnerabilities that year.

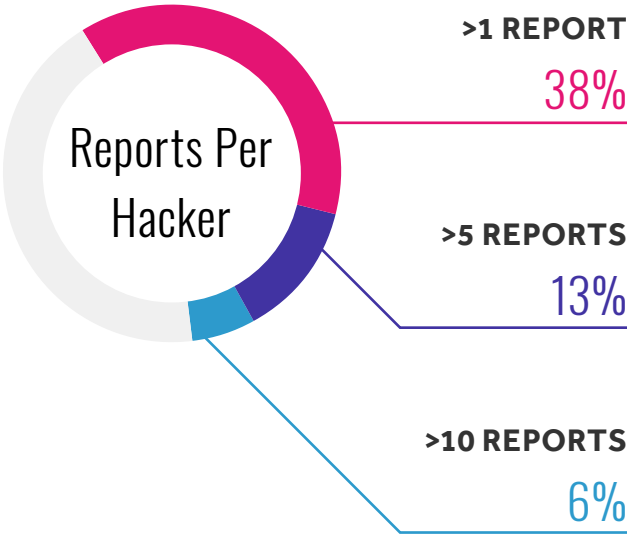
"The program kept our engineers on their toes, challenged and surprised our security team and helped us keep GitLab more secure," wrote Juan Broullon, GitLab senior application security engineer.

KEEPING HACKERS ENGAGED

It's been shown that repeat hackers find the majority of valid reports, so getting them, and keeping them engaged is good for security. GitLab understands the importance of community and the value of hackers who submit multiple vulnerability reports. Ritchey saw it as "a sign that our processes were working and the way that we were incentivising and engaging with our hackers was appreciated."

Looking at a snapshot of their combined private and public bounty programs across one year, GitLab found that 38% of hackers involved in their programs submitted more than one report, while 13% submitted more than 5 and 6% submitted more than 10. It showed that GitLab's commitment to hacker satisfaction was paying off and prompted them to do even more to keep reporters incentivized, motivated, and engaged to find bugs on their platform. GitLab's team even attended HackerOne's H1-702 live hacking event in Las Vegas in September 2019 to meet in-person with their top hackers, recognize their contributions, and thank them for their hard work.

But their outreach to hackers didn't stop there. As the one year anniversary of their public bug bounty program approached, GitLab didn't just increase their bounty award values, they launched a hacking contest to offer hackers some special rewards. The challenges ranged from best bug report to most impactful finding, with winners receiving a custom mechanical keyboard in the GitLab giveaway.



SURPASSING $1,000,000 IN AWARDS

Moving from a simple VDP in 2014 to one of the top bug bounty programs in 2018 was no small feat. And since GitLab's hacker-powered security efforts paid out more than a half-million dollars in its first year, it was clear they ran a popular program that was well-prepared for continuous growth. So it wasn't surprising that, in January 2020, GitLab announced they had surpassed the milestone of awarding out $1 million in bug bounties to hackers on HackerOne for discovering and disclosing valid bug bounty reports.

"There's no denying that a million dollars in bounties paid is a big milestone for our program, but what makes this especially meaningful to us is that it clearly demonstrates GitLab's commitment to building a strong and secure product," said Ethan Strike, security manager at GitLab.

GitLab's engagement with the hacker community paid dividends not only in bug reports, but in attracting dedicated hackers who returned to help again and again.

"We're proud that our journey to a million in paid bounties includes contributions from 768 reporters (since Jan 2014) including several of HackerOne's all time leading reporters," added Strike. "We also have 227 repeat reporters, meaning that we're finding ways to engage and incentivize reporters to continue to contribute to our program."

Even hackers outside of GitLab's sphere have taken notice. In the first 13 months of their public program, 541 new-to-their-program hackers submitted reports. That shows significant participation growth and, again, reflects GitLab's mantra that everyone can contribute.

COMMUNITY FOR SECURITY

GitLab is built around a community, so it makes sense that they extend that community approach to their security program. Hacker-powered security gives them access to hundreds of thousands of hackers with broad, deep, or pinpoint experience, around-the-clock efforts, and the creativity only a human can apply to a security challenge. After more than five years of hacker-powered security, they have no plans to pull back now.

"Our bug bounty program is a key, final step in a holistic approach to securing our platform from code creation to customer use," says Johnathan Hunt, VP of security at GitLab. "This program ensures our platform is continuously tested by the world's top security researchers to detect and mitigate vulnerabilities that would otherwise impact our customers and business."

> **"This program ensures our platform is continuously tested by the world's top security researchers to detect and mitigate vulnerabilities that would otherwise impact our customers and business."**
>
> **JOHNATHAN HUNT**
>
> **VP OF SECURITY AT GITLAB**

It's clear that no organization or technology is ever 100% secure. That's why it's important to take a multi-pronged approach, even within hacker-powered security. GitLab recognized early on the need for a VDP, slowly expanded that to a small, private bounty program, then a larger public bounty program. The progressive stage programs all work in conjunction with GitLab's broader security efforts for continuous coverage and a constant set of outside eyes.

"Our bug bounty program ensures GitLab achieves the highest standard in continuous security coverage," adds Hunt. "It solidifies our defense-in-depth approach to securing our customers and their data through continuous testing by experts across the globe."

CRAWL, WALK, RUN WITH HACKERONE

GitLab's experience launching, improving and growing their hacker-powered security program is a good model for organizations and security teams of any size. Their crawl, walk, run approach helps teams understand how hacker-powered security can augment and extend their programs to reduce risk and improve security. The key is starting small and growing, or iterating (another core GitLab value) at your own pace.

First, every organization needs a VDP. It's the "see something, say something" of the internet and it's crucial for giving everyone from random website visitors to seasoned hackers clear guidelines for alerting you to a potential security gap. It also helps your internal teams better route any incoming reports, which a contributor might send to your support team, social media accounts, or a sales email address. There are many guides and templates to help you create your own VDP, so there's really no excuse not to have one.

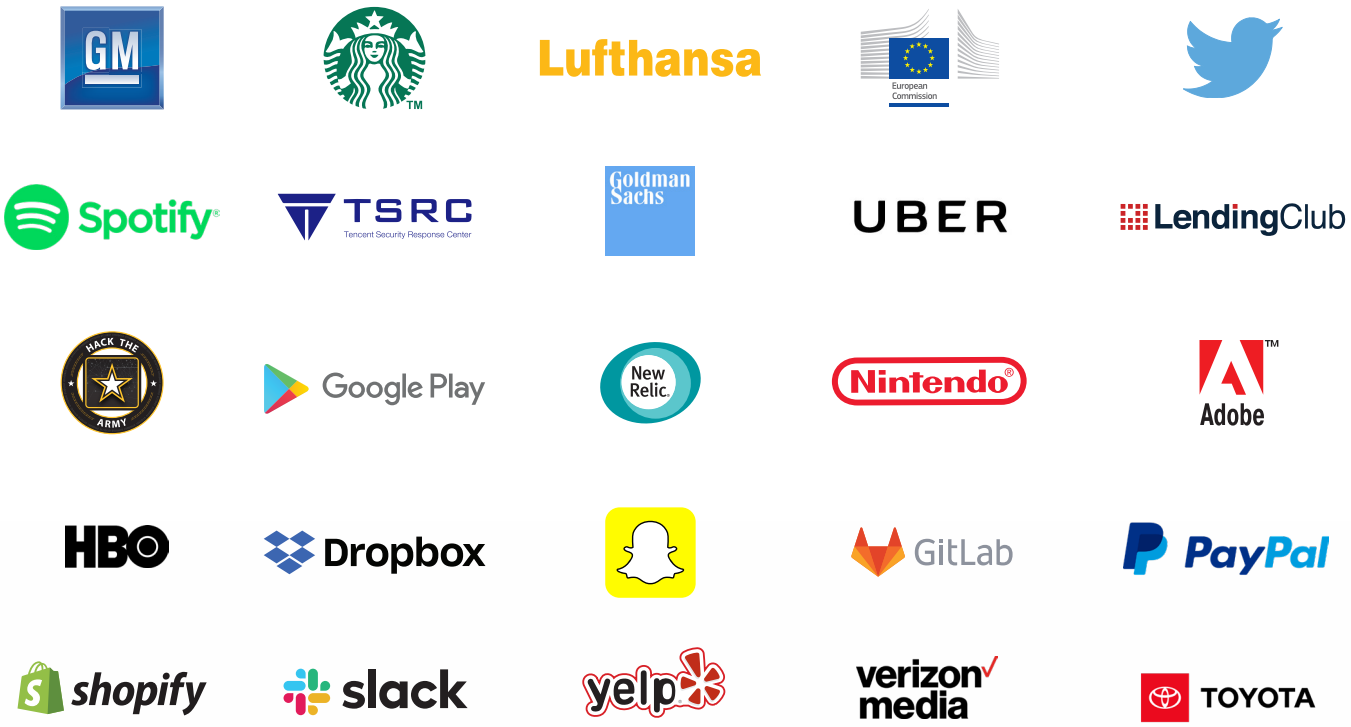
As your program matures, moving to a private or public bug bounty program lets you take full advantage of the power of the hacker community. These programs can plug directly into your existing SDLC and security apparatus, and can be self-managed or turnkey to include assistance for hacker communications, report triage, and more. It's also cost-effective, since the costs are directly related to validated bug reports. Every dollar you spend is the result of a hacker finding a real security threat.

Are you ready to put the power of the hacker community to work for your organization?

With hundreds of thousands in the HackerOne community ready to help, you don't have to go it alone.

hackerone

HACKERONE HAS VETTED HACKERS FOR HUNDREDS OF ORGANIZATIONS INCLUDING:



With Over 1,800 Customer Programs,
More Companies Trust HackerOne
Than Any Other Vendor.

CONTACT US