hackerone

THE SHOPIFY HACKER-POWERED SECURITY STORY

Shopify uses bug bounties to safeguard their merchants and turn the tables on vulnerabilities...and criminals.

CUSTOMER STORY

shopify

Customer Data

PRODUCT TYPE

HackerOne Bounty

Public Program

COMPANY SIZE

3,000+

NO. REPORTS RESOLVED*

759

INDUSTRY

Commerce

HACKERS THANKED*

300+

since 2015

CUSTOMERS

600,000+

merchants in 175 countries

TOTAL BOUNTIES PAID*

$850,000+

TOTAL PLATFORM SALES

$55 Billion

**Program data as of 3/15/18. Total bounties paid includes the Shopify+Scripts program and the h1-415 2017 live-hacking event*

Shopify's ecommerce platform helps more than a half-million merchants spread across 90% of the world's countries design, set-up, and manage their online stores.

In 2012, Andrew Dunbar left his role as an IT security specialist in the Canadian government to take a role as Shopify's one-person security team. Now, not quite six years later, Andrew leads Shopify's roughly 50-person security team. He's not only worked to build a stellar team of relentless security professionals, he's become a leading voice touting the benefits of hacker-powered security.

But it's not easy, especially while supporting so many merchants and giving them the freedom to customize their shopping experience as they like. It forces you to take a different approach to security. **"For companies to think their app isn't going to have an unknown vulnerability, it's kind of short sighted," said Andrew. "Our goal is to make sure the same vulnerability doesn't happen twice."**

As Andrew has built Shopify's security team, he's also found that hacker-powered security helps them maintain the trust they've worked to build with merchants. And that trust is why they chose to work with HackerOne.

Stopping Shoplifters, Both Online and Offline

For Shopify, the risk of a vulnerability exploit is clear, and potentially huge. Their merchants deal with millions of customers, collect sensitive personal and financial information, and facilitate credit card transactions. Many of those merchants also use Shopify's technology offline, in their bricks-and-mortar stores or from wherever they do business. And just like criminals target banks because "that's where the money is," the money is also in the ecommerce transaction.

"We hear these stories about retail breaches all the time," said Andrew. "There are hundreds every year, and the risks are everywhere online and offline. From physical point-of-sale devices with weak encryption to malicious bots targeting online promotions, criminals are coming up with ways to beat security efforts just as fast as the industry is closing those gaps."

Shopify, like every ecommerce solution provider, has seen it all. What their security team does is work to mitigate those potential risks as much as possible. But a team of 1 or of 50, it's still nice to have help.

Doubling Down on Their Community of Developers

Shopify's platform has always relied heavily on APIs, so their community of thousands of developers serves as sort of extended security and quality control teams. "Developers are constantly using our published APIs, so it's a really great way to have your code tested in ways you never imagined," said Andrew.

When Andrew was Shopify's one-person security shop in 2012, he received a bug report from one of their external developers. As he worked with the developer to dig into the issue, he wondered how they could embrace this community, encourage bug report submissions, and reward them fairly for their efforts.

"These white-hat developers already have access to our APIs, can create test shops, can build payment systems. We try to give them the tools needed to find vulnerabilities across our platform," Andrew explained.

Their system was cobbled together and worked well, but they quickly recognized the need to have a more scalable program in place.

Quickly Scaling and Evolving Their Bug Bounty Program

As Shopify built their bug bounty program, they saw early the need to make a splash with the broader white-hat hacker community.

“We set out to have an incredibly competitive program,” said Andrew. “We wanted to establish credibility and and create a lot of visibility, so we made sure our payouts were high. We also wanted hackers to see that we were taking this seriously.”

Higher payouts brings more hackers, obviously, so Shopify also had to worry about scalability. They built a support system on their internal customer support app, developed canned email responses, and paid bounties via PayPal.

“We quickly decided that we wanted to have a bounty program at the level of Facebook or other leading companies,” Andrew recalled. “We knew we needed to improve beyond an email-based system and give our teams better visibility into reports and their status.”

Once they were introduced to HackerOne in 2015, they immediately saw it as a platform that would give their program a solid foundation from which to scale.

PRO TIPS FROM SHOPIFY

Andrew Dunbar, Shopify’s director of risk and compliance, has this advice for those considering a bug bounty program:

- **Be consistent.** Hackers are detail-oriented people, and they’ll quickly spot inconsistencies in your program.
- **Recognize the value hackers bring to the party.** You know bugs are out there, and they won’t be found without hackers.
- **Have a willingness to reward and communicate budget needs internally.** Whether you need higher-quality hackers or you want to direct them to certain areas, be flexible on your bounties.

"The biggest challenge our program faced was visibility," said Andrew. "For the bug bounty program, we had to show ethical hackers that we have a robust platform with unique problems to make it worthwhile."

Engaging with HackerOne's large community of hackers was of obvious importance, but Shopify was also competing for visibility with many, many other bug bounty programs.

"We wanted to take advantage of the visibility and scalability that came from HackerOne," said Andrew. "The platform helped improve the quality of submissions. We got much more transparency into the report submissions and the process they went through."

An Executive-Level Investment in Security

In under two years, Shopify's core program had paid out more than $500,000 in bounties. In late 2016, Shopify expanded their HackerOne program to cover critical new mRuby functionality. In just one day, Shopify paid out more than $300,000 in bounties, bringing a lot of attention to the program. According to their CEO, it was worth every penny.

"What you have to realize is how important Security is to Shopify," said Shopify CEO, Tobi Lutke, on a Hacker News discussion thread at the time. "We are a trust based business to an extreme extent. One of the best ways for us to augment our internal security team is to work with the white-hat community. This was a pain before HackerOne but now is significantly easier."

> “ One of the best ways for us to augment our internal security team is to work with the white-hat community. This was a pain before HackerOne but now is significantly easier.
>
> TOBI LUTKE, CEO, SHOPIFY

Tobi goes on to explain that, in the early days of their bounty program, they "overspent as a kind of marketing investment" aimed at building interest in their program from more of the top-tier hackers.

"We want to be known for being one of the most responsive companies and also pay top dollars for top findings," Tobi added. "It should be more fun and more lucrative to make Shopify-related discoveries than (for) other companies."

Andrew knew that getting CEO and CTO support for their bounty program was important from the very beginning, but that was easy. From the top down, Shopify recognized the need to maintain the trust of their merchants. Any exploit, big or small, would be damaging to both their merchants and their brand. Their bounty program gave hackers an easy path for reporting bugs and being incentivized to do so, rather than exploiting it or selling it to someone else. It also shed some light on their security efforts, further cementing trust with their merchants.

SHOPIFY SECURITY:

Fast Action During the Holiday Rush

Shopify recently paid a bounty of $15,000, plus a $250 bonus, for a critical bug that, if exploited, would have allowed unauthorized access to merchant accounts. The hacker, @cache-money, reported the vulnerability as the busiest shopping period of the year was winding down.

Within 12 hours, *on Christmas Eve*, Shopify's security team implemented a fix, Within 6 weeks, Shopify publicly disclosed the issue and paid the bounty.

"It was a pleasure to work with a team that takes security as seriously as they do," said @cache-money in the report's summary.

Read the full report here.

"Internally, we had lots of support," Andrew explained. "Our leadership team has worked hard to build security into the company culture and stood firmly behind having a bug bounty program. Because our leadership team understands the value and impact of security, budget talks were typically: How can we pay more to have more eyes working on our program? With the bug bounty program, we've found a scalable way to continue building trust in our platform."

As their bounty program took off, Tobi described being "thrilled" with their early experience on HackerOne. He also said that, even if individual bugs would've been otherwise found, the point was to get some diverse, talented humans looking creatively at their security.

"As everyone who does security knows - lots of exploits, even if superficially contained, can sometimes combine into 'the big one'," Tobi concluded.

All in the Name of Better Security

As their bug bounty program continued, so did Shopify's surprise and delight at the types and volumes of incoming reports. What helped was making it easier for hackers to build their own shops to test, download scripts, and tinker with APIs. It fostered a level of trust with hackers in order to increase the trust from their merchants.

"We wanted to make it easy for people to find things," Andrew explained. "Until you have a robust set of eyes on your stuff, it's really hard to know what you're missing."

"Until you have a robust set of eyes on your stuff, it's really hard to know what you're missing.

ANDREW DUNBAR, DIRECTOR RISK & COMPLIANCE, SHOPIFY

One example Andrew provided was a potential vulnerability which would have allowed unauthorized access to merchant invoices. If they missed that, Andrew thought, what else might they have missed?

The speed and efficiency bounty programs have in finding vulnerabilities is why Andrew has become an outspoken proponent of bug bounties and has been featured in many articles and interviews about the topic. Bounty programs are, according to Andrew, a great way to get in front of an issue before a vulnerability can be exploited. And security is an issue confronting every company.

Success is More Than Just Financial

With most programs, in most organizations, the results are frequently measured financially. But at Shopify the importance of security to their customers outweighs the typical metrics. So demonstrating and following-through on their dedication to security is what's really important.

"This is part of Shopify's investment and dedication to the overall security of our platform," says Andrew.

But metrics are, still, a part of every program. So Shopify tracks the monetary value of bounties and the number of valid vulnerabilities. At the executive level, results are also measured by the scope of reach or how many hackers are participating, and how their program compares against industry peers.

Shopify Engages Top Hackers in Live-Hacking Event

Live-hacking events bring security teams and hackers face-to-face. Long-term relationships are built, and lots of bugs discovered in 1-day of hacking.

Shopify participated in the inaugural live-hacking event at our San Francisco Headquarters, in scope was their successful MRuby program and they targeted a specific shopping cart product to get more critical vulnerabilities on these valuable assets.

Andrew said, "Some of the top hackers in the world are in the same venue as you, meeting your security team. Just being able to have those face-to-face conversations has been really valuable."

You can watch the full h1-415 2017 Live-Hacking event recap video and see #h1415 on twitter.

An Unforeseen Success Metric: Turning Hackers into Employees

In 2017, Shopify hired one of HackerOne's top 100 hackers, Pete Yaworski, for an in-house role on their security team (a relationship that was established at their h1-415 live-hacking event). Pete had been working for the Ontario government as a cybersecurity specialist, but Shopify has turned out to be a perfect fit.

"There's so much value in being part of a team," says Pete, reflecting on his internal role at Shopify. "From a micro perspective, I'm surrounded by amazing security experts from whom I'm learning a ton. At a macro level, you have an entire organization behind you supporting your growth, development, and success."

But just as Shopify's overall security efforts aren't easily measured, Pete sees his own experience at Shopify also defined by the intangible.

"At Shopify, I get to work with incredibly smart people who are driven by a larger cause," Pete said. "There are real-world impacts I see as a direct result of my work, not only for Shopify but for everyone who interacts with our platform."

PETE YAWORSKI (@YAWORSK)

Learn more about HackerOne Bounty or reach out to start a conversation today.

About HackerOne

HackerOne is the #1 hacker-powered security platform, helping organizations receive and resolve critical vulnerabilities before they can be exploited. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security partner. Organizations, including the U.S. Department of Defense, U.S. General Service Administration, General Motors, Google, Twitter, GitHub, Nintendo, Lufthansa, Panasonic Avionics, Qualcomm, Starbucks, Dropbox, Intel and the CERT Coordination Center trust HackerOne to find critical software vulnerabilities. HackerOne customers have resolved over 65,000 vulnerabilities and awarded over $26M in bug bounties. HackerOne is headquartered in San Francisco with offices in London, New York and the Netherlands.

GM Lufthansa European Commission

Spotify HACK THE U.S. AIR FORCE airbnb

WordPress LendingClub HACK THE U.S. ARMY Google Play

New Relic Nintendo Adobe Dropbox

coinbase shopify YAHOO!