hackerone

Case Study

shopify

# Secure ecommerce X 300,000 How Shopify shares with Hackers

Does sharing security holes with hackers make Shopify more secure? That's what Shopify wanted to learn with their unique approach to a bug bounty program.

Dissatisfied with the software options available to build their snowboarding store, alpine enthusiasts Tobias Lütke and Daniel Weinand founded Shopify in 2004. Security was a top priority as user growth skyrocketed to a community of over 300,000 entrepreneurs trusting Shopify to power their businesses. They chose an unconventional tactic: revealing fixed security vulnerabilities to the world to increase trust. Here's how they did it.

## Getting Better Vulnerability Reports in Less Time

Back in September 2013, Shopify used standard issue tracking software to track vulnerability reports. This resulted in Shopify's team spending time on manual processes, including creating tickets, proofs of concept, reproducing issues, assigning severity, and then later submitting it to GitHub. Ticket management and maintaining a hall of fame were becoming a burden. Still, just having a vulnerability response put them ahead of 94% of the Forbes 100.[1]

To decrease the time that the internal team spent on tracking vulnerabilities, Shopify researched other companies who had successfully offered bug bounty programs, such as Twitter, Square, and more. Then Shopify evaluated bug bounty companies for their features, expertise, and hacker network.

*"It puts Shopify on par with top software companies that attract top researcher talent. If you are not on HackerOne, you're competing for the attention of researchers and facing an uphill battle. If you are Microsoft you can offer $100k all on your own. If hackers don't know you from 15 years of vulnerability management...it's hard."*

**- Andrew Dunbar**
Director of Risk and Compliance, Shopify

## Sharing Security Holes

Lütke, Shopify's CEO, drove the effort to implement a bug bounty program to fix these problems. He realized offering payments would draw the attention of the best hackers, but gaining the trust of repeat hackers was paramount as they found the most vulnerabilities. In fact, repeat hackers have provided 64% of valid Shopify bugs ever found. The top 20 Shopify hackers (of 145) alone provided 41% of their valid vulnerabilities.

### About Shopify

Shopify is the leading cloud-based, multichannel commerce platform designed for small and medium-sized businesses. Merchants can use the software to design, set up, and manage their stores across multiple sales channels, including web, mobile, social media, marketplaces, brick-and-mortar locations, and pop-up shops. The platform also provides merchants with a powerful back-office and a single view of their business. The Shopify platform was engineered for reliability and scale, using enterprise-level technology made available to businesses of all sizes. Shopify currently powers over 300,000 businesses in approximately 150 countries and is trusted by brands such as Tesla Motors, Budweiser, Red Bull, LA Lakers, the New York Stock Exchange, GoldieBlox, and many more.

[1] A 2015 HackerOne study showed only 6% of Forbes 100 companies have a process for responding to and closing security vulnerability reports from outside their organization.

shopify

On HackerOne, organizations have the option to take closed security holes and make them public as a teaching tool. Shopify realized that this was also valuable to encouraging repeat hackers. That's why Shopify has publicly shared 120+ security vulnerabilities - more than 99% of HackerOne customers. Public reports encourage hackers to look for vulnerabilities to report.

Shopify quickly gained a reputation for disclosing reports publicly, and hackers loved it.

"After resolution, we aim for full public disclosure of issues. It has helped by creating a great reputation on our platform. We've even had researchers apply for jobs," said Dunbar. "A lot of companies don't want to expose or disclose vulnerabilities, because it's seen as a weakness, but we don't see value in that. In addition, we work very hard to explain why something is or isn't an issue, because it's an educational opportunity." On top of that, Shopify currently offers a $500 minimum bounty, the highest on HackerOne.

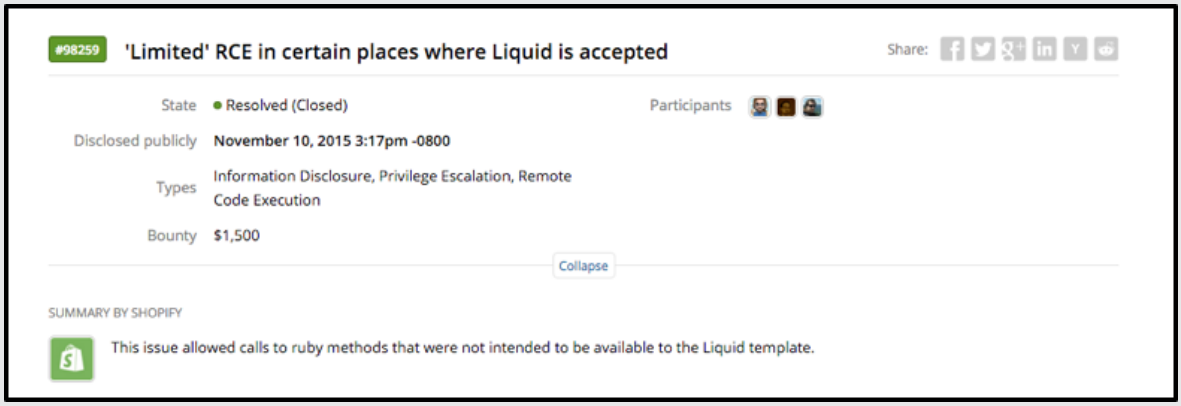
*"It's about maintaining trust with our merchants. Entrepreneurs are running their businesses and they don't want to worry about security, so we have to ensure any issue gets addressed. HackerOne provides a return on our investment through its large community of talent and by taking care of administration, vetting researchers and handling payments."*

**- Andrew Dunbar**
Director of Risk and Compliance, Shopify

## Results

The results of openly communicating with hackers were very positive. In the first month, Shopify received 600 reports. After 3 months, they had 1,000. In the last quarter of 2015, the number of participating researchers had grown to 272, reporting an average of 200-300 vulnerabilities monthly. Since launching on HackerOne, 269+ vulnerability reports have been closed with more than 100 hackers thanked. Hackers earned $8,500 in their launch year of 2014 and $80,000 more in 2015. Hackers continue to hack and protect Shopify, drawing inspiration from each public report.

## What did Shopify Get? Great reports.




Other valid reports include: "Fetching external resources through svg images," "VG parser loads external resources on image upload," and "XSS at importing Product List."