SALESFORCE USES BUG BOUNTIES TO PROTECT CUSTOMER DATA

salesforce

hackerone

Salesforce disrupted the entire world of technology with their pioneering efforts to deliver enterprise software from the cloud. One of their biggest hurdles at the beginning was to convince skeptical customers' their data would be secure, especially as it was to be stored remotely and accessed over the internet.

Fast-forward 19 years and you'd be hard pressed to name a technology company that doesn't deliver products via the cloud. And, given that Salesforce revenue is more than $8 billion, it's clear that they've effectively gained the trust of tens of thousands of customers.

But that trust isn't taken for granted by Salesforce, and they've built a security apparatus that utilizes white-hat hackers as a key component of their overall strategy. Over the past 3 years, Salesforce has worked with HackerOne to accept thousands of bug reports and award bounties to more than 1,200 hackers. The results are nothing short of a resounding success.

BUG BOUNTY STATS: SALESFORCE

Average Bounty: $850

Highest Bounty Paid: $15,000

Average Response Time: < 5 hrs

Valid Reports Received: > 3,200

"The program has been successful because of the continued contributions from diverse, talented researchers, security engineers who triage and guide teams to remediate, and our engineering team that is always enthusiastic to learn from these bugs," said Vinayendra Nataraja, a senior product security engineer at Salesforce, in a recent blog post.

Salesforce also recognizes the work done by hackers by giving public thank you notes to those who help, working to maintain fast response times, offering bonus and bounty multipliers when appropriate, and keeping bounties inline with the effort.

"One of our core objectives is to keep our researchers happy and encourage responsible disclosure," said Nataraja. "We award bounties based on severity and complexity of the bug, and are always open to a discussion with the researchers about this."

We're excited that Salesforce trusts HackerOne to secure their tech and earn the trust of their own customers, and we're ready to help support their hacker-powered security efforts for the next 3 years—and beyond!

Celebrating 3 Years of Salesforce Bug Bounty

By: Vinayendra Nataraja, Product Security, Salesforce

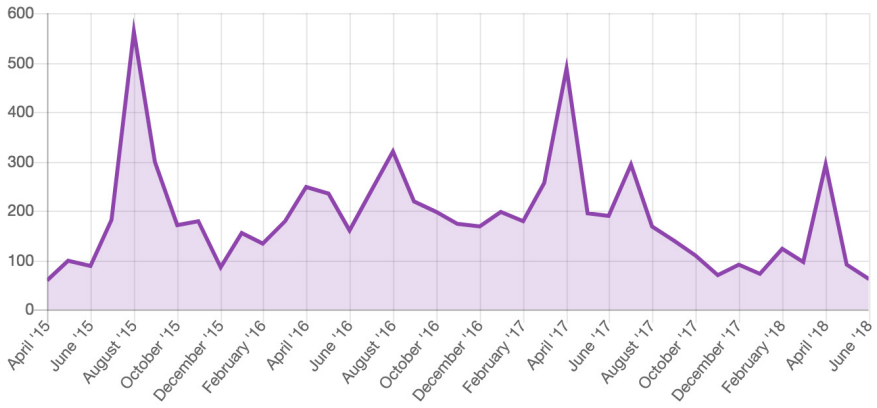
At Salesforce, trust is our #1 value, and we take the protection of our customers' data very seriously. Salesforce's Bug Bounty program is one of the many efforts that contributes to the security of our products, and therefore, our customers. Bug bounty programs work by providing a monetary reward, or "bounty," to security researchers who responsibly disclose security issues on our platform. This also helps us engage with the broader infosec community on an ongoing basis.

We just concluded the third year of Salesforce's Bug Bounty program. In these three years, we have received a lot of interesting bugs and worked with hundreds of researchers around the world. The program has been successful because of the continued contributions from diverse, talented researchers, security engineers who triage and guide teams to remediate, and our engineering team that is always enthusiastic to learn from these bugs.

Below is a snapshot of the number of bugs that were reported in the last few years through the Bug Bounty program. Over three years:

- We have received more than **3,200** valid submissions from **1,200+ researchers**
- Almost **70%** of submissions are valid (includes duplicates)
- Our average bounty: **$850**
- Our highest bounty till date is **$15,000**
- **51%** of 2017 security bugs were reported through Bug Bounty
- **Over 90%** of externally reported security issues were through Bug Bounty in 2017

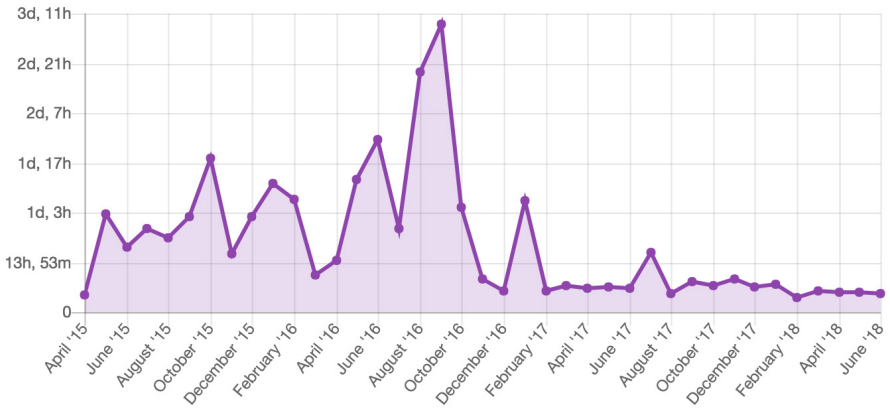
New reports per month:



Graph from HackerOne showing our incoming reports, by month

One of our core objectives is to keep our researchers happy and encourage responsible disclosure. We award bounties based on severity and complexity of the bug, and are always open to a discussion with the researchers about this. We have also improved our response time for a bug from more than 24 hours to less than five hours by having a dedicated triage team.

Response time per month has changed over the last few years significantly:



Graph from HackerOne showing our response time, by month

We help researchers by providing guidance around why a certain report was triaged at a certain severity and help them understand the products in more depth. Occasionally we offer bonus and bounty multipliers for either certain products or classes of bugs which has always spiked the number of reports on the program.

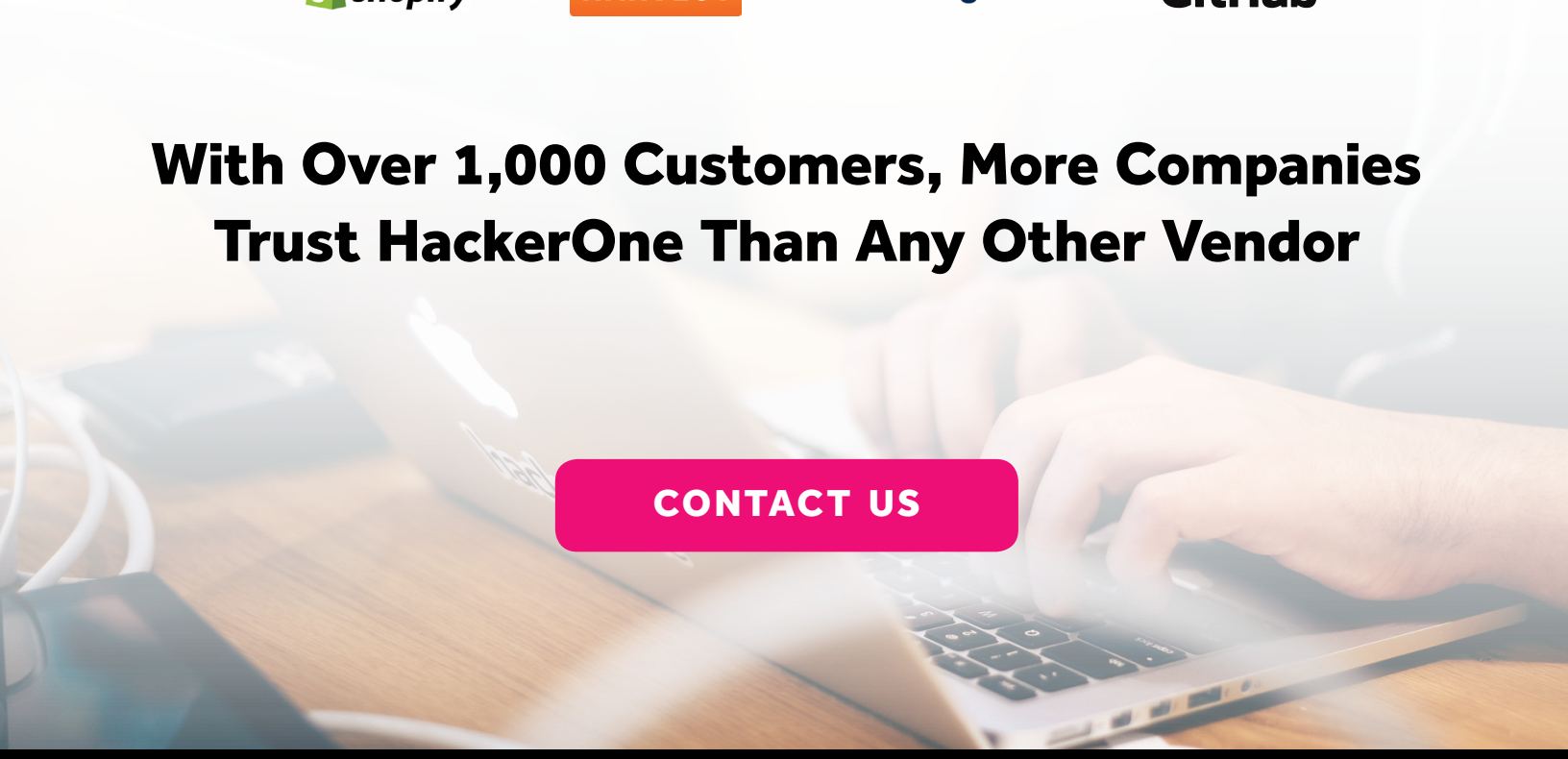
Recently we launched the VIP program, in which top researchers participate to test newer features and products which then mature and get included to our ongoing bug bounty program. This has spiked the number of reports we receive.

We thank our researchers and are excited about the continued success of our Bug Bounty program. If you find a security vulnerability, please send the details of the bug in an email to security at salesforce.com; if you want to join the team at Salesforce, find open security positions here.

Published on Medium.com July 11, 2018

HackerOne Has Vetted Hackers For Hundreds of Organizations Including:

With Over 1,000 Customers, More Companies Trust HackerOne Than Any Other Vendor



CONTACT US