PROGRAM INSIGHTS FROM THE PAYPAL SECURITY TEAM

PayPal | hackerone

PayPal's digital payments platform gives 267 million active account holders in more than 200 markets around the world the confidence to connect and transact in new ways, whether they are online, on a mobile device in an app, or in person.

Through a combination of technological innovation and strategic partnerships, they enable consumers and merchants to receive money in more than 100 currencies, withdraw funds in 56 currencies and hold balances in their PayPal accounts in 25 currencies. Its security team is tasked with helping to protect the financial information for these merchants and consumers every day.

We sat down with PayPal Information Security Engineers Ray Duran, Sonal Shrivastava, and Pax Whitmore, and Project Manager Rebecca Francom to learn more about how PayPal works with the researcher community, the journey of a reported bug, and what findings are most impactful. Check it out!

Ray Duran
Information Security Engineer at PayPal, CISSP

Sonal Shrivastava
Information Security Engineer at PayPal

Pax Whitmore
Information Security Engineer at PayPal

Rebecca Francom
Project Manager at PayPal

Q: Why did PayPal start a bug bounty program in the first place?

Ray: The safety of our customers and brand is extremely important and launching a bug bounty program offered a worldwide partnership to keep our customers' security our top priority. The program is an opportunity for us to collect and remediate vulnerabilities found externally. Our team's mission is to protect PayPal's customers, merchants, and data by being a world leader in the security community. Internally, our goal is to be as agile as our development teams and support them as a security service. Externally, our goal is to be coveted by the security researcher community and provide vulnerability information back out into the industry for the betterment of online applications.

Q: How has the program evolved over time?

Rebecca: Through our program, we've learned a lot and continued to make adjustments as we learn — evolving our scope, revamping terms and conditions to ensure our program remains competitive with the industry standards, and more. We have tripled our

bounty payouts, introduced several new acquisitions, and our program has won international accolades.

Q: PayPal has run a bug bounty program independently for years. Why switch to a platform?

Ray: Over the course of our program we have evolved from accepting submissions via email, building our own platform, to officially partnering with HackerOne. This transition has allowed us to grow the program from starting with around 2,000 security researchers to now over 300,000. Our goal is to offer the opportunity to all researchers globally to participate in our continually growing program. Partnering with HackerOne offered us that opportunity. Joining HackerOne also allows us to align ourselves with industry standards as well as give back to the community from our own lessons learned.

Q: How has the bug bounty program impacted PayPal's overall security posture and strategy?

Pax: PayPal has many fantastic, dedicated security teams, including strategy, automation, pen testing, and incident response. The bug bounty program is a part of that, and vulnerabilities surfaced through our program get fed back to our other teams (we even like to refer to the program as the "backstop"). We've had situations where, because of an issue identified through a bug bounty submission, we've been able to revise a proactive or framework-level control. This doesn't happen just because something was missed, but because external researchers give us a unique perspective. I can safely say I learn something new every day working with bug bounty researchers, and being able to share that with colleagues who are equally passionate and driven is a genuine pleasure.

Q: What have been some of the most memorable interactions with hackers to-date? Any notable bugs?

Pax: There have been too many awesome submissions to include them all, but one that stands out for me is a Struts zero-day that was reported in early 2017. The researcher had helped discover the bug, which could lead to Remote Code Execution (RCE) via some poor error handling in the HTTP headers. After disclosing to Apache, the researcher sent it out to multiple bug bounty programs. Thanks to their hard work, we were able to coordinate an immediate response and deploy WAF rules to help stop any malicious traffic, even before the exploit was public or any patch was released. We were also able to identify additional attack vectors and contribute our own findings back out to the world. It was a great testament to the value of bug bounty researchers, and some truly outstanding work from the security community.

In the past six months, we've been thrilled to receive some helpful submissions on Android applications. Mobile applications are a huge priority for us, and it's great to see some of the bleeding-edge research being done. We hope to build some strong and long-lasting relationships with mobile security experts, particularly bagipro!

Q: Tell us more about the journey of a bug. Once it gets reported, then what?

Sonal: Once a security vulnerability is reported by the researcher to HackerOne,

1. The report gets triaged by the HackerOne team

2. All the validated findings are forwarded to PayPal's Bug Bounty team for further review.

3. PayPal's Bug Bounty team replicates the issue and assess the risk ratings.

4. If the report is valid then –

- A reward is set based on CVSSv3 risk rating, followed by payment to the researcher.
- Then, the issue is escalated, an internal ticket is created, and the Development teams are notified. These teams are responsible for fixing the vulnerability.
- Once fixed, the Bug Bounty team then validates the fix and closes the internal ticket as well as HackerOne ticket. Often the researcher and HackerOne team is involved to help verify the fix.
- If the finding is not valid (duplicate, etc.) the Bug Bounty team sends the report back to HackerOne with an explanation for why it is invalid.

5. We regularly review any public disclosure requests that we have received after the vulnerability is fixed and closed.

Due to the large ecosystem at PayPal and our holdings, sometimes we come across issues which require additional due diligence to confirm if the issue holds a risk. This further validation could lead to delay in triaging. Thus, even though the process remains the same for all the reports, there are some reports which take time to get validated delaying the researcher's payment.

Q: What bugs get your team most excited? In other words, what findings are most interesting to your team?

Sonal: When an RCE is reported by a researcher, it gets its due attention with high visibility and fast resolution times. Additionally, vulnerabilities related to server side attacks or database attacks are also critical to us. However, some of the most interesting submissions, are low risk vulnerabilities which can be chained together for greater impact. We are equally delighted on receiving a well written report and often end up paying bonuses for them. It should be noted that creative doesn't mean impactful, and a submission with a clearly explained impact statement tends to gain more traction than a POC that appears tricky.

Q: Why should hackers participate in your program? What advice would you give them?

Pax: 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. The best submissions always speak softly and carry a big stick: keep it simple, support claims with evidence, and show a clear impact. When it comes to vulnerabilities, it's never what you know, it's always what you can prove.

HackerOne Has Vetted Hackers for Hundreds of Organizations Including:

GM · Starbucks · Lufthansa · European Commission · Twitter · Spotify · Hack the U.S. Air Force · LINE · UBER · LendingClub · Hack the Army · Google Play · New Relic · Nintendo · Adobe · HBO · Dropbox · Snapchat · YAHOO! · PayPal · shopify · slack · yelp · verizon media · TOYOTA

With Over 1,400 Organizations, More Companies Trust HackerOne Than Any Other Vendor

CONTACT US