hackerone

PAYPAL ON CREATING STRONG RELATIONSHIPS WITH SECURITY RESEARCHERS

—

This blog post was written and contributed by Information Security Engineer, Ray Duran, on behalf of the PayPal Bug Bounty team.

Customer Story

PayPal

PayPal has been a leader in leveraging the unique and valuable perspectives of the security research community to strengthen security since 2012.

Over the past 8 years, we have awarded more than $6 million to roughly 3,000 ethical hackers who have contributed to our bug bounty program. The success of our program would not have been possible without a collaborative partnership between our security team and the participating researchers.

At PayPal, we consider security researchers as a complement to our security team and aim to maintain an open dialogue with the HackerOne community. Building relationships with researchers has always been a priority as these relationships have not only improved engagement but also humanized the bug bounty program. We're inspired by many of the personal stories from researchers about how the PayPal and other bug bounty programs have changed their lives in a positive way. Getting to this point wasn't always easy. It took time, patience, and numerous iterations. We wanted to share what we've learned along the way.

BE OPEN TO FEEDBACK

Two-way communication goes a long way in building strong relationships with security researchers and achieving better results. By being receptive to program feedback, scope questions, disclosure requests, etc., we open a dialogue with the HackerOne community so that they can be more productive in our program. We strive to be transparent and give context around our decisions and we hope for the same in return. At the end of the day, we all have the same goal — to make the internet and PayPal more secure.

In addition to feedback from program participants and the security researcher community, we stay actively involved in discussions and share knowledge with other bounty programs. There is always more to be learned and being open to alternative perspectives helps make the program stronger and more successful. We believe we have a responsibility to share our methodology and learnings with the larger industry. The more we share knowledge, the stronger cybersecurity becomes.

THE CASE FOR OBJECTIVITY

Security teams can build credibility and trust with security researchers by letting them in on why scope is structured a certain way, or why vulnerabilities are rewarded the way that they are. At PayPal, the use of CVSS parameters allows us to be objective about risk and eliminate subjectivity in awarding payments.

After looking through data, we initially developed a system to associate ranges of CVSS scores to Low, Medium, High, and Critical severities. However, we realized it would still be open to judgment in determining where in the range a report would fit and therefore what the precise payout would be. We wrote an additional script to tie exact bounty amounts to exact CVSS scores, which makes for a repeatable, specific, and objective measure. Lastly, CVSS parameters act as an objective foundation for discussions with researchers on severity. Most notably, @alexbirsan incorporates CVSS in submissions regularly, which has led to productive and insightful conversations about report severity. Keep it up, Alex!

REPORTS HAVE POWER

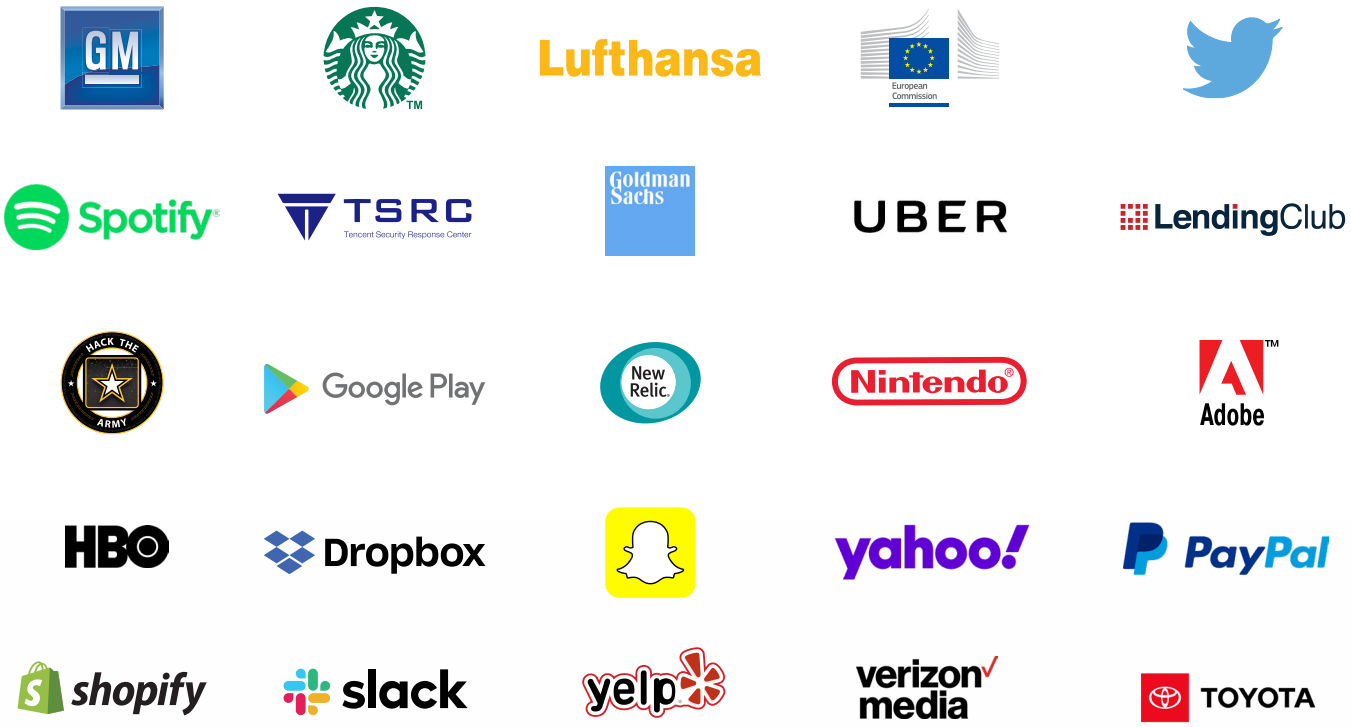
Researchers play an important role in building relationships with the security teams they work with. Researchers who submit well-written reports with detailed proof of claims and clear reproduction steps stand out in the pack. @defparam and @ngalog have stood out to the PayPal security team for their detailed reports and collaborative spirit. The best submissions are simple; support claims with evidence, and demonstrate impact. Well-written reports help reduce back-and-forth conversations, allowing us to quickly move on to remediation steps and faster bounty payouts. We also greatly appreciate researchers who are willing to assist in re-testing or who quickly respond to requests for more information as our investigation unfolds.

Thank you to everyone in the HackerOne community who participates in the PayPal bug bounty program. We're more secure thanks to your research and partnership.

To learn more about the PayPal program and get hacking, visit https://hackerone.com/paypal.

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