hackerone

ZOMATO'S HACKER-FOCUSED APPROACH TURNS THE TABLES ON SECURITY VULNERABILITIES

Connecting eaters with restaurants is Zomato's main business, so they took a hospitable approach to hackers, driving engagement and quality submissions vital to the security of Zomato's customers and core business applications.

CUSTOMER STORY

zomato

Customer Data

PRODUCT TYPE

HackerOne Bounty

LAUNCH DATE

July 2017

TOTAL BOUNTIES PAID

>$100,000

AVERAGE RESPONSE TIME

4 Hours

COMPANY SIZE

2,000+ Employees

INDUSTRY

Hospitality

HACKERS THANKED

355

TOP BOUNTY AWARDED TO DATE

$1,000

zomato

Zomato works with hackers to make sure the **data of 55 million eaters** is secure.

Headquartered in India, restaurant discovery, online ordering, and table reservations platform Zomato currently operates in 24 countries, from the United States to South Africa, and New Zealand to Slovakia. Its security team, lead by Prateek Tiwari, is tasked with protecting sensitive information for over 55 million unique monthly visitors.

Since launching their bug bounty program with HackerOne in July 2017, the company has paid out more than $100,000 to over 350 hackers, all while maintaining an average response time of 4 hours. Now that's a speedy delivery!

Delivering a Tasteful Customer Experience

Zomato is in the business of connecting hungry customers with great food. They conduct millions of transactions per day, with most containing sensitive personal, financial, and other data. Keeping that data secure lets their customers enjoy their meals and gives their dining partners confidence in the Zomato platform.

Part of their security approach is hacker-powered, and they've had a great experience with HackerOne ever since their program began.

"Thanks to HackerOne and the committed community, the results have been outstanding and have far exceeded our expectations," said Prateek Tiwari, security lead at Zomato. "We had one goal at the beginning of the program: make Zomato more secure. Thanks to the community, with every single report resolved, we're getting closer to this goal."

> Thanks to HackerOne and the committed community, the results have been outstanding and have far exceeded our expectations.
>
> **PRATEEK TIWARI, SECURITY LEAD, ZOMATO**

Better Response Times are Better than Bounties

Zomato's focus on the hacker community has also impacted the success of their program. Part of that is their focus on timely response, which they view as critical to keeping hackers coming back to the Zomato bounty program.

"It's crucial to maintain a great relationship with the hacker community," said Tiwari. "Our team prioritized response time for that reason. Bounties are important, but timely responses to hackers and keeping them informed at every step is critical to keep hackers engaged and loyal to the program. HackerOne also played a crucial role in cutting down the noise so we could focus only on the valid issues."

> HackerOne also played a crucial role in cutting down the noise so we could focus only on the valid issues.
>
> **PRATEEK TIWARI, SECURITY LEAD, ZOMATO**

Tiwari's point, that response times to hackers are equally as important as the bounty values, is a critical distinction. With large enterprises awarding as much as $250,000 for critical bugs, mid-sized and smaller companies are angling to compete for the same talented hackers. But hackers are people, and people like to be valued and respected. Zomato's effort to respond in just a few hours pays off by giving hackers added visibility into the results of their efforts.

Building Relationships with Hackers

Beyond respecting hackers' time with fast responses, Zomato's security team strives to maintain personal relationships with their top performing hackers. In fact, when we questioned Tiwari about their program, he started naming names and recalling individual vulnerability reports.

"@Gerben_Javado stands out for his impressive vulnerability reports," said Tiwari. "One of his most interesting reports was one where he escalated a very important vulnerability in our Android app—it wasn't easy to find. His work truly demonstrates creative thinking and persistence, and we are blessed to have such brilliant ethical hackers on the HackerOne platform."

> It's crucial to maintain a great relationship with the hacker community.
>
> **PRATEEK TIWARI, SECURITY LEAD, ZOMATO**

It's that personal connection that keeps their best hackers coming back. And if you click over to @Gerben_Javad's hacktivity page, you'll see that he's personally reported more than 100 potential vulnerabilities for Zomato!

Doubling-Down on Bounty Values

Much of Zomato's customer traffic comes from their Android app, so it's an obvious focus on their security team and bounty program. Lucky for them—and especially for their hackers—HackerOne works with Google to offer an add-on rewards program. It enables hacker to earn bounty awards in addition to what Zomato offers.

"Our apps were recently added to Google Play Security Reward Program, so hackers can earn additional bounties if they find vulnerabilities in our apps," added Tiwari.

And, continuing their hacker-first approach, Zomato plans to pay bounties to hackers earlier in the process, putting their hard-earned money into their bank accounts faster. There are also plans to increase bounties and offer more swag, two things hackers absolutely hunger for.

Advice from a Fast-Growing Bounty Program

Every HackerOne customer is different, and each has specific security needs, concerns, and capabilities. Zomato is no different, and their policy page reflects their program's structure and scope, as well as eligibility requirements. After a couple of years of experience, here's what Zomato's security team recommends to those considering hacker-powered security.

BE PREPARED

Bet ready for the rush of incoming reports as hackers discover your program and quickly find the first level of potential vulnerabilities. "At the launch of the program, there will be a swarm of reports," recalled Tiwari. "Consider an internal audit first to clear up as much low-hanging fruit as possible."

Many companies work with HackerOne's expert triage and managed services team, which includes full triage and bug bounty program management to serve as the most convenient option for resource constrained organizations. Find out more.

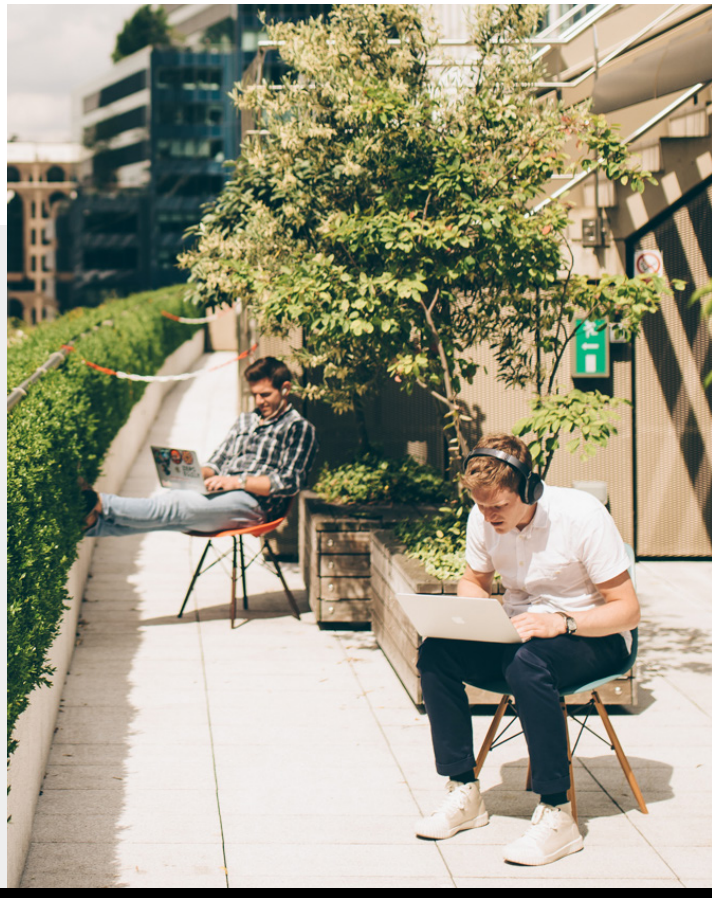
BE SPECIFIC

Keep hackers focused and noise low with a clear and concise scope as well as detailed reporting expectations. It can help hackers better understand what's going to be denied before they set out looking for things. "Defining the scope of the program pre-launch is also critical," added Tiwari. "It gives a clear picture to hackers of what vulnerability reports are accepted versus what aren't.

BE RESPECTFUL

As mentioned above, Zomato went out of their way to make their program appealing to hackers, and it wasn't in the bug bounty award values. Their team bet that shorter response times would result in motivated hackers who submit better reports, and they were right. "Creating a good relationship and clear process with the engineering team is also important for resolving reports in timely manner," said Tiwari. "Keep your response times consistently low. As a program owner, you must ensure that hackers are appreciated for their work."

Because, when hackers get respect from bug bounty programs, they come back for seconds...and more!
#TogetherWeHitHarder



About HackerOne

HackerOne is the #1 hacker-powered security platform, helping organizations find and fix critical vulnerabilities before they can be exploited. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security alternative. The U.S. Department of Defense, General Motors, Google, Twitter, GitHub, Nintendo, Lufthansa, Panasonic Avionics, Qualcomm, Starbucks, Dropbox, Intel, the CERT Coordination Center and over 1,000 other organizations have partnered with HackerOne to resolve over 76,000 vulnerabilities and award over $32M in bug bounties. HackerOne is headquartered in San Francisco with offices in London, New York, and the Netherlands.

For a comprehensive look at the industry based on the largest repository of hacker reported vulnerability data, download the The Hacker-Powered Security Report 2018.