hackerone

HackerOne Triage

What Is HackerOne Triage?

An Extension of Your Security Team

Triage and validation are at the heart of any bug bounty program (BBP) or vulnerability disclosure program (VDP). Despite their central role, not all triage teams and workflows are created equal. HackerOne Triage stands out for its breadth and depth of analyst expertise, user-friendly platform, and cost-effective model with proven efficiencies.

HackerOne security analysts are on the front lines, facilitating every step necessary for the customer to prioritize vulnerabilities, understand the impact, and remediate as needed. At the same time, our analysts ensure hackers receive detailed feedback, fostering positive collaboration that keeps the process moving forward smoothly and effectively.

HackerOne Triage is an ideal choice for businesses that:

- **Have an established VDP and/or BBP and have already formulated effective internal processes for maintaining and operating the program**
- **Are ready to scale up the bug bounty and disclosure program but require additional capacity and capability to do so**
- **Desire a cost-effective model for triage support while benefiting from the depth and breadth of analyst expertise offered by HackerOne**

What Makes HackerOne Security Analysts Stand Out?

At HackerOne, we realize that delivering the most effective triage experience for customers and hackers is a meticulous job and requires a team of experts who should function as an extension of your security or development team. That's where HackerOne security analysts come in.

HackerOne Triage Services consists of more than 45 highly skilled in-house security analysts who triage over 4,000 reports per week and 16,000 reports per month across five continents. Our global coverage enables the triage team to deliver quicker results and faster resolution at scale.

HackerOne's security analysts have a broad array of technical skills and industry experience to cover a diverse range of assets, including web, mobile, API, binary, firmware, IoT, and hardware. All team members have a finger on the pulse of high-volume reports, zero days, and other vulnerabilities. Our team understands security concepts inside and out. They know how ethical hackers think and behave, based on their own experience.

About the team:

Hundreds of years of combined experience in AppSec, hacking, and triaging

A geographically diverse structure, covering Pacific to Eastern time zones in the Western Hemisphere and British Standard Time to India Standard Time in the Eastern Hemisphere, allowing the team to correspond with hackers in over ten languages

In-depth knowledge with prior industry experience at global organizations such as Adobe, DoD, Dell, RSA, Microsoft, HP, GoDaddy, and more

Average time to first response of 11 hours

Meet Some of HackerOne's Elite Triage Analysts

Nabeel Ahmad

Nabeel is a Senior Security Analyst, working in the Triage team since May 2022. In his current role as EMEA team lead, he excels in spearheading pivotal initiatives and steering an exceptional team toward safeguarding HackerOne customers against diverse vulnerabilities in a timely manner. He takes pride in fostering strong connections with customers and working collaboratively daily via Slack to ensure a seamless customer experience. According to Nabeel, his favorite vulnerabilities to hunt for and exploit in BBP programs include Server-Side Request Forgery (SSRF), Cache Poisoning, HTTP Request Smuggling, Mass Assignment, and Broken Access Control issues. Beyond work, Nabeel enjoys engaging in web app hacking through bug bounty programs, as well as indulging in gaming.

Goonjeta M.

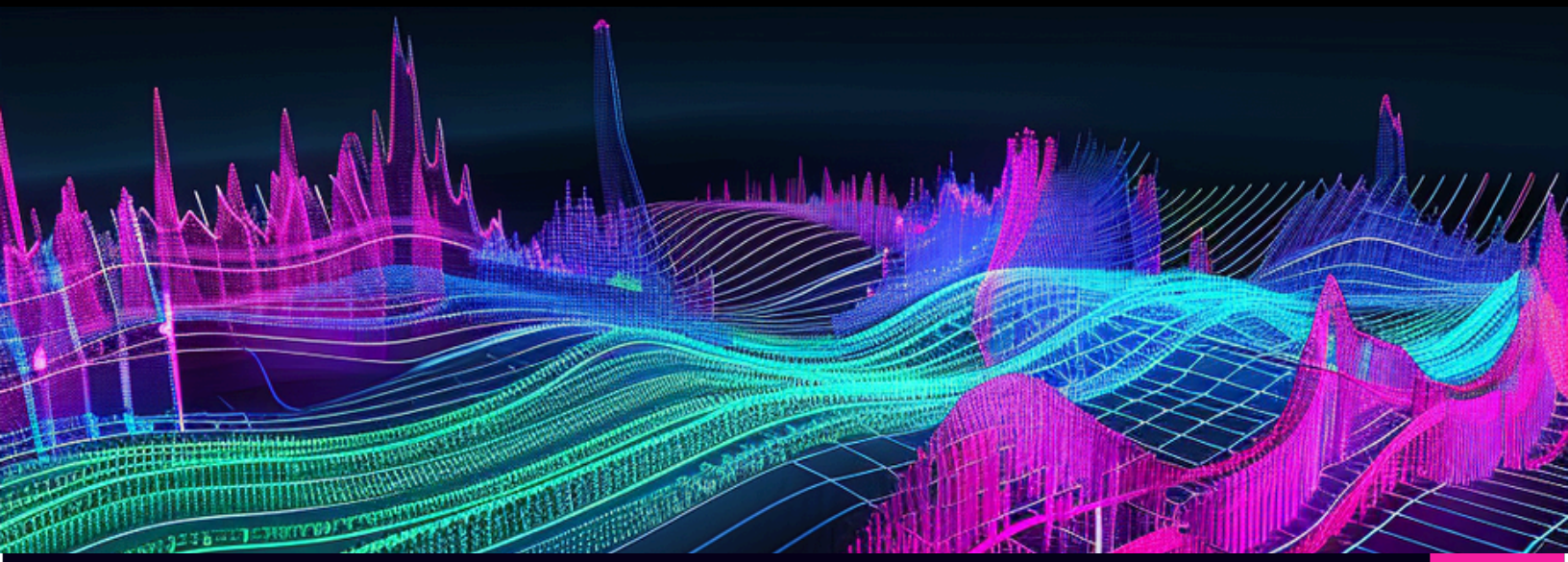
Goonjeta is the Team Lead for Technical Services at HackerOne, where she blends cybersecurity expertise with leadership finesse. She is responsible for leading and managing a highly motivated team, assisting customers with their queries and concerns, analyzing and validating issues, and aligning processes for optimal efficiency. Goonjeta excels with advanced technologies, including Web3, AI/LLM, Web, API, and Internal and External network. As the youngest female ever to achieve OSCP certification—clearing the exam at just 18 years old—Goonjeta brings the same level of perseverance and determination to leading and managing her team. Outside of work, she enjoys pentesting and bug bounty hunting, along with hobbies that include painting and dancing.

Everton Michels

Everton is a Senior Technical Lead for the Triage team, and has been working for HackerOne for seven years. Everton's extensive experience in triaging enables him to assess technical vulnerabilities with a keen eye—evaluating the impact based on nuanced factors that are often not visible to external actors. His years of service have not only sharpened his skills but also enabled him to develop strong relationships with hackers and customers alike. Outside of work, Everton is an aspiring sailor and enjoys driving vintage cars.

Who Uses HackerOne Triage?

Customers across the globe rely on HackerOne Triage:



What HackerOne Customers Say About Triage

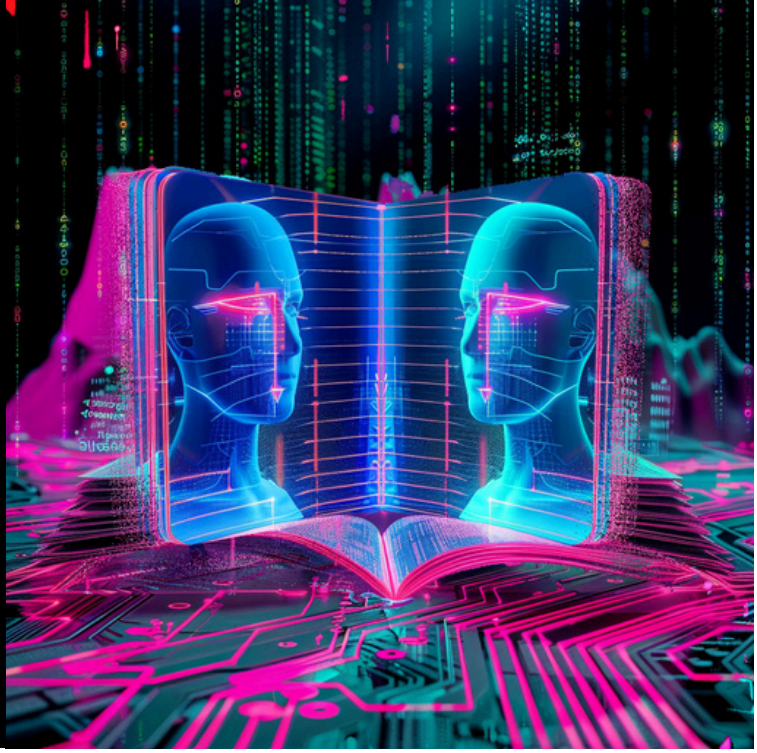
"HackerOne Triage has been really helpful in making sure that top-notch reports get attention right away, with quick responses and efficient resolutions for contributors. This lines up with our commitment to stick to industry response times, making sure our researchers' input is recognized promptly and issues are sorted out fast and effectively."

Nouman J. Hashmi
Senior Security Engineering Manager, Delivery Hero

"Internally, we are faster at fixing a HackerOne finding than a finding from anywhere else, notes Jasyn. We also get nearly zero false positives from HackerOne, thanks to triage. This speaks to the findings' quality and our confidence in HackerOne."

Dr. Jasyn Voshell
Director of Product and Solution Security, Zebra Technologies

How HackerOne Triage Is Using GenAI



HackerOne recently launched the beta version of our GenAI copilot—Hai—into the HackerOne Platform.

Hai is becoming an integral part of HackerOne's triage workflow, making our industry's largest in-house analyst team better able to push boundaries and continue to help our customers operate exceptional bounty and disclosure programs. Security analysts are already consistently using Hai to summarize hacker reports, greatly reducing the time spent on manual tasks and effectively scaling the triage function at HackerOne.

Traditionally, analysts have spent extensive time reviewing and closing invalid and duplicate reports, and then explaining those decisions. As we further integrate Hai's excellent reasoning capabilities into the triage process, many of these decisions can be made and justified by Hai so our analysts can focus on new vulnerability reports.

Hai can screen and enhance reports with higher-fidelity metadata during the submission process, reducing the burden on customers and empowering our analysts to focus on reproducing and remediating the true positives.

Resource: What Makes a Strong Report?

A concise and high-quality report from hackers speeds up the triage process, enables quicker issue validation, and expedites remediation for program resolution and payout.

HackerOne educates hackers on how to improve the quality of submissions, making the process move smoothly for all involved.

We advise hackers to:

- **Select an asset and set the severity of each report.** This will save the hacker some headache from submitting reports that might be out of scope, and the severity setting can give us insight into how impactful this issue might be. (More on the severity in a moment.)
- **Provide a summary up front.** Something succinct that illustrates the relevant vulnerability and what it means sets the stage for what you're reporting.
- **Tell us how to reproduce this.** Attention to detail is key! Provide comprehensive, step-by-step instructions outlining the workflow for both triage and the program to replicate your issue. Additionally, consider using visuals, such as images, to enhance clarity. Some triagers may appreciate a video proof of concept (POC), but only if it is concise and to the point (less than 2 mins).
- **Explain the impact.** Why is this important for the business? What might someone with bad intentions achieve if they take advantage of this weakness in a real situation? Describe in simple terms how this vulnerability could lead to actual problems for the program, and clarify your thoughts by explaining the CVSS score in detail. You can find additional details on this subject in the section labeled "Impact" below.

Many programs have template report requirements that already adhere to these best practices. So adopting this mentality not only makes things smoother for those triaging your reports, but aligns with what programs are looking for in their submissions. You may have even seen it. **A typical structure would look like this:**

##Summary
A quick description of the issue. Example: A stored XSS vulnerability exists on the endpoint `www.asset.com/the/path/to/xss` via the parameter `vulnerable_param`.

Reproduction Steps

1. List a detailed step-by-step breakdown of how to reproduce this vulnerability.
2. You don't need to overstate everything, but make sure all the relevant details are there.
3. Note any special permissions that are required, or if the vulnerable element is buried somewhere, give us a URL path to the location or steps on how to get there.
4. If it's something like Stored XSS, noting the POST endpoint and the vulnerable parameter is helpful!
5. Screenshots that help clarify the impact and prove your finding should be included as well.
6. If you have code snippets or want to share HTTP requests with us, use proper [formatting](https://docs.hackerone.com/organizations/using-markdown.html) to help make things readable and quick to reuse when we test it.

Impact
Describe the impact from a business or user perspective. What are the implications of this issue for the business? For the victim? What does an attacker gain from this? This is your chance to help sell the importance of your finding.

For example, if you find a Reflected XSS vulnerability on an asset, you can help sell your idea on severity if you explain the level of damage an attacker could get away with. Can you access the victim's session cookies and take over their account? Is this a flagship or critical application?

What Makes a Strong Report?

"A good report is all about communicating properly. A report that describes the issue in a clear and concise way, with detailed steps to fully reproduce the issue, including information about the application itself and not only the vulnerabilities per se. And, of course, a working proof of concept that clearly demonstrates impact." – **Everton**

" Providing evidence such as screenshots or a proof of concept code strengthens the report's validity. Additional details include providing a video PoC, mentioning the exact vulnerable assets and endpoints, and providing the vulnerable request." – **Goonjeta**

"Clear reproduction steps that also detail prerequisites. Reports containing information on how to set up the environment needed to reproduce help a lot. Also, images are a must, in my opinion. And finally, the impact of the vulnerability; if this bug was to be exploited, how can this undermine the security of other users or that of the platform? If you can't answer this question, it's likely the bug will be closed as Informative or N/A, as there must be a security impact for it to be eligible for a bounty." – **Nabeel**