hackerone | grammarly

CASE STUDY

Grammarly Exceeds Customer Expectations with Hacker-Powered Security

As the world's leading writing assistant serving 30 million people and 30,000 teams daily, Grammarly's top priority is to ensure the data their customers trust them with remains secure. To strengthen that trust, Grammarly turned to HackerOne.

Key Takeaways

Before Challenges

- Ensure brand and user trust during accelerated growth
- Continuous testing of potential security gaps
- Needed hacker expertise for complex systems

Key Requirements

- Access to a diverse range of skilled security researchers
- A first response team to reduce operational workload
- 24/7 support to improve processes, meet SLA's, and enable transparent communication
- Integrations with Slack and Jira

Security Goals

- Protect their users' data
- Provide the most secure products possible
- Supplement traditional ad-hoc penetration testing with a continuous program
- Maintain trust and show transparency with users
- Maintain agility and speed to market

Why HackerOne

- Most trusted and effective global community
- Access to a large number of security researchers with a diverse range of skills
- Renowned reputation and robust platform security

Solutions

- HackerOne Bounty
- HackerOne Pentest
- HackerOne Triage

Hacker Skill Sets

- Domain expertise to cover broad technical requirements: Browser extensions, Website and web apps, APIs, Mobile keyboards, Office add-ins, Desktop editors

"Our product was at the early stages of accelerated growth and scale. We wanted to go above and beyond standard security practices and do what it takes to provide the most secure product possible. We wanted an extra layer of assurance that our product is secure, and we wanted to be transparent with our customers to maintain their trust."

Joe Xavier

VICE PRESIDENT OF ENGINEERING, GRAMMARLY

About Grammarly

Grammarly, widely recognized as one of the world's most innovative AI companies, is a cloud-based digital writing assistant that scales across multiple platforms and devices. Millions of people worldwide use their AI-powered product to improve their personal and business writing and communication.

Grammarly was founded in 2009 with the goal of helping people communicate more effectively. Innovation has been a guiding principle since, and Grammarly is committed to using new approaches like advanced machine learning and deep learning to improve their offerings.

Grammarly has always considered cybersecurity as fundamental to their success. As the organization scales and expands their advanced writing assistance capabilities, this rings true more than ever. Security is Grammarly's most important feature, and keeping users' data safe and secure is their top priority.

Hackers Ensure Accelerated Growth

In mid-2017, Grammarly was in the early stages of accelerated growth. To ensure robust security as they scaled, they wanted to understand where there might be existing and potential gaps in their security. They were also eager to give their users additional assurance that their product was secure.

"We wanted to know what we didn't know. We didn't want to just rely on the results of the custom-ordered penetration tests. The complexity of our systems didn't allow researchers to find in-depth scenarios during fixed, time-bound engagements," says Joe Xavier, Grammarly's VP of Engineering.

Grammarly's security team was convinced that involving a global security research community would provide the subject matter expertise they needed for their complex SaaS platform and ultimately yield significantly better results. Additionally, the organization believed treating security as a continuous process rather than a point-in-time assessment would radically improve their security strategy. They were right.

Bug Bounty as a Security Default

The idea to implement a bug bounty program was introduced by Grammarly's engineering team and supported by executive leaders as a top priority. Grammarly launched a private bug bounty program with HackerOne Bounty in September 2017. They knew ongoing collaboration with a talented group of security researchers would lead to a better, more secure product. The Grammarly team worked with HackerOne to define program policies, scope, and best practices for reporting metrics, bounty rewards, and response SLAs. HackerOne also assisted Grammarly in planning the long-term hacker-powered security program, which would ultimately include a public HackerOne Bounty program and HackerOne Pentests. The result was a successful bug bounty program supported by healthy performance and engagement metrics.

The private bug bounty program showed a quick return on investment, and early findings resulted in systematic changes across all production environments to ensure end-to-end protection.

One prominent example from the private bug bounty program was the company-wide introduction of the CSRF protection method based on a Double Submit Cookie technique instead of a prior protection mechanism. Initially, a seemingly reliable solution looked close to optimal. Once Grammarly's security team received the first few reports from the hacker community, they found it necessary to iterate on the solution design to re-implement the protection across all their applications. This finding resulted in a significant decrease in the attack surface.

> **"We wanted to know what we didn't know. We didn't want to just rely on the results of the custom-ordered penetration tests. The complexity of our systems didn't allow researchers to find in-depth scenarios during fixed, time-bound engagements."**
>
> 
>
> **Joe Xavier**
> VICE PRESIDENT OF ENGINEERING, GRAMMARLY

Leveraging the data from hacker findings has helped Grammarly make improvements throughout the SDLC. According to Joe, "for example, based on HackerOne reports, we created custom rules for static code analysis tools integrated into our CI/CD process. This allows us to find similar cases in the code for all our repositories. Every valid vulnerability we receive signals to our team that we have to implement a new defense layer to ensure we won't introduce similar issues in the future. If our team ever receives a high severity vulnerability report, we will conduct a detailed security review to revisit our approach to securing that specific part of our product feature."

Securing the Future with a Multi-Pronged Approach

Working with hackers in a private bug bounty program reinforced Grammarly's belief that security must be a continuous process. They spent the first several months gathering learnings and fine-tuning their internal processes and SLAs to accept and remediate vulnerabilities. Once the team refined their internal processes, it was time to launch a public bug bounty program. Now almost three years old, the public bug bounty program has helped their team immediately identify potential vulnerabilities as the product evolves and they develop new features.

"The bug bounty program is now an integral part of our security controls framework," says Joe, "Security researchers have helped us improve our strategy in the fields of client-side security, like CSRF, CSP and web security headers, cookie isolation, native apps security, and security of our backend services, including API structuring, network, and OS isolation."

Since its inception, Grammarly's bug bounty program has been open-ended and continually running, so validation and testing happen around the clock. Grammarly adds new product offerings to the program scope as soon as product development begins, through beta releases, and then keeps them available for additional testing once they are fully operational. This is especially important to their overall security posture as Grammarly frequently iterates on existing offerings, adding new features to improve functionality and user experience. With hacker-powered security, Grammarly ensures that every new product version is exposed to security researchers.

Grammarly also supplements its bug bounty program with customer-tailored HackerOne Pentests. These types of pentests help Grammarly achieve specific objectives like meeting the regulatory requirements of their customers, conducting additional tests by select subject-matter experts from the researcher community, and beta testing select versions of their product.

Additionally, Grammarly leverages HackerOne Triage to help their security team stay focused on what requires their attention.

"Since the HackerOne Triage team is well-calibrated on our scope, they offload some of the work from our security team, such as report triage, identifying duplicated reports, and scope mismatch. In other words, the HackerOne Triage team acts as an extension to our security team," says Joe.

"Since the HackerOne Triage team is well-calibrated on our scope, they offload some of the work from our security team, such as report triage, identifying duplicated reports, and scope mismatch. In other words, the HackerOne Triage team acts as an extension to our security team."

Joe Xavier
VICE PRESIDENT OF ENGINEERING, GRAMMARLY

More Transparent Than Ever Before

Security and transparency are at the heart of Grammarly's culture. Their Security Champions program ensures security and privacy concerns are kept top of mind across the company, and they're committed to sharing the results of their cybersecurity program on public and private platforms. The security team provides internal updates to their executive team and communicates program results to the broader organization through all-hands events and Slack updates. This communication helps drive awareness of and engagement in their hacker-powered security program among the engineering teams and beyond.

Today, Grammarly says their product security is more transparent than ever before. They are proud to demonstrate the program's effectiveness on their public program page and consider it another way to build trust in the market. Externally, Grammarly proactively shares the results and health metrics of the bug bounty program with prospective and existing customers to increase their level of confidence in their product.

"A combination of a healthy public program metric and a custom pentest exercise by a curated team of security engineers is perceived well by our customers and prospects," says Joe.

HackerOne has also helped Grammarly attract great talent. One of the top researchers who worked on their private program eventually joined their full-time staff as a Security Engineer.

With hacker-powered security, Grammarly takes important steps to keep security at the heart of their business and build trust with their customers, prospects, and the broader market with the most secure product possible. As the organization looks to the future, they continue to consider ways to position their program to attract the best researchers, including encouraging sophisticated analysis with complex use cases and high-value bounties.

> **"A combination of a healthy public program metric and a custom pentest exercise by a curated team of security engineers is perceived well by our customers and prospects."**

Joe Xavier
VICE PRESIDENT OF ENGINEERING, GRAMMARLY

hackerone

HackerOne has vetted hackers for hundreds of organizations including:




With over 2,000 customer programs, more companies trust HackerOne than any other vendor

Contact Us