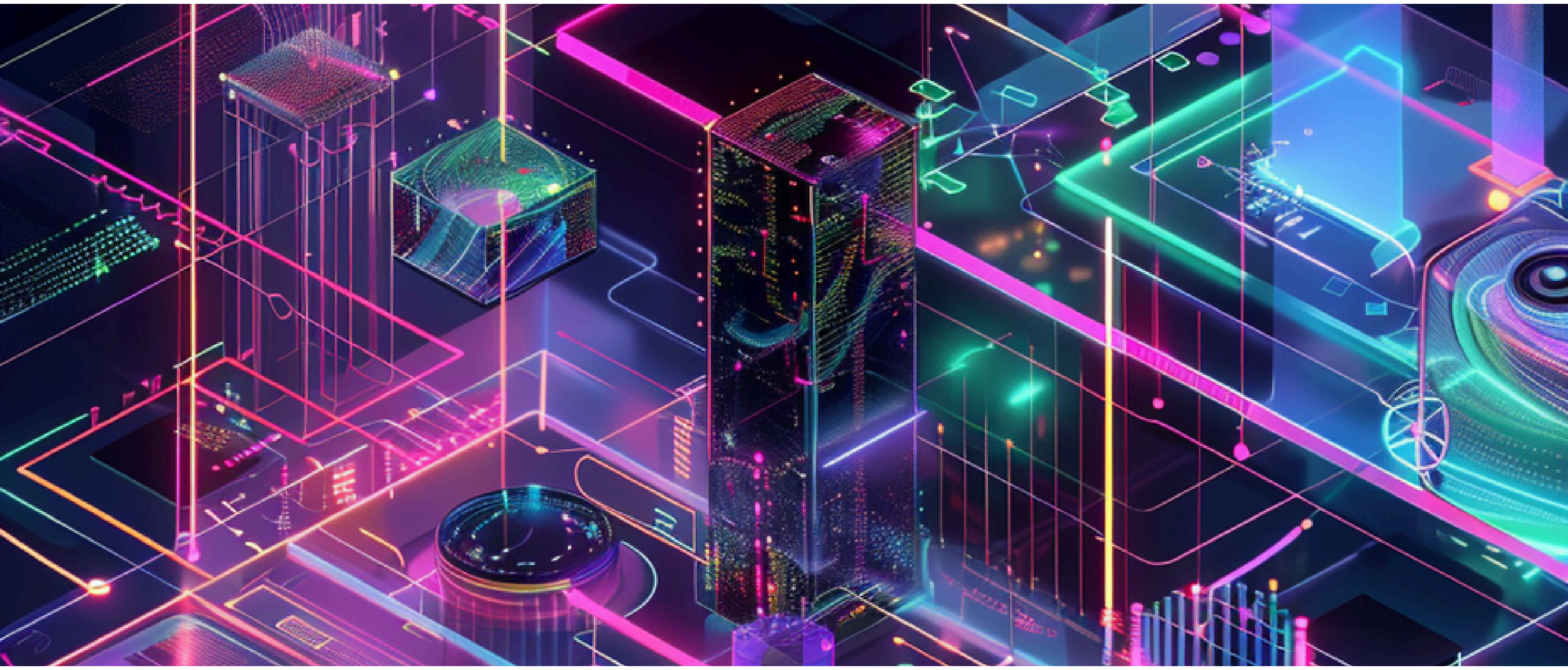
CASE STUDY



Adobe and HackerOne's Decade-Long Partnership with the Ethical Hacking Community

Founded 40 years ago on the simple idea of creating innovative products that change the world, Adobe offers groundbreaking technologies that empower everyone, everywhere, to imagine, create, and bring digital experiences to life.

Adobe has been an active participant in the security community, engaging with partners, standards organizations, and security researchers to collectively enhance the security posture of its products and services. Adobe recognizes ethical hackers as a force multiplier in their quest to provide a safer experience for their customers. Over the past ten years, Adobe has partnered with HackerOne and ethical hackers to enhance Adobe's security resilience.

Key Takeaways

Challenges

- Replace legacy vulnerability submission workflows to improve efficiency
- Reduce false positives
- Increase testing scope and strengthen collaboration with testers and hackers

Security Goals

- Increase product security resilience and confidence
- Scale identification and mitigation of vulnerabilities
- Extend testing coverage for Adobe assets
- Optimize spend on high-impact, actionable results

Key Hacker Skill Sets

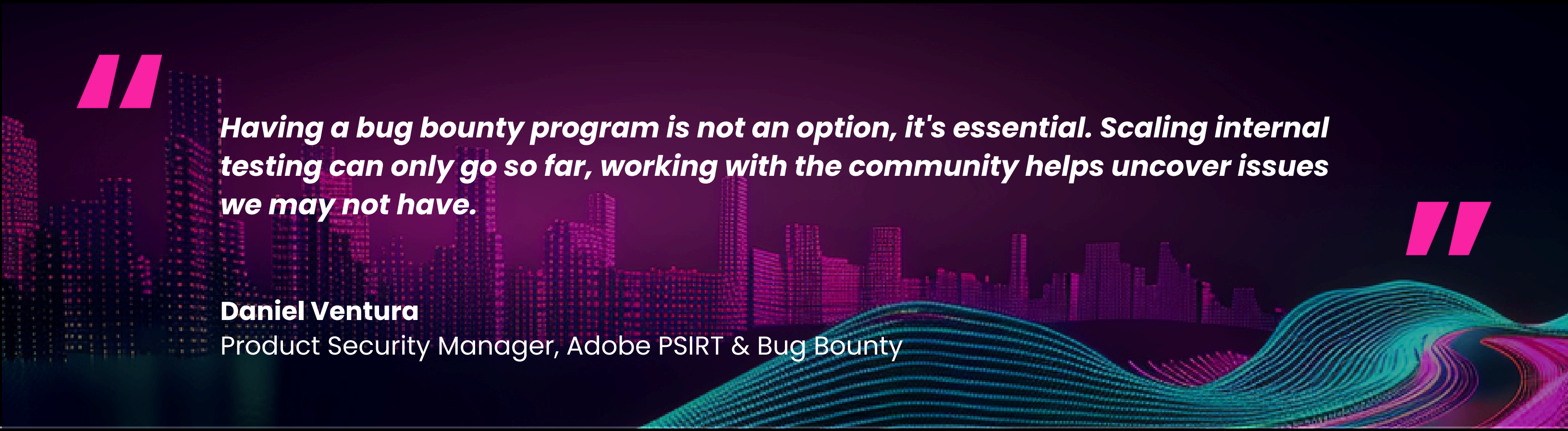
- Android and iOS applications
- APIs and API backend
- AWS, Azure, GCP
- Distributed cloud architectures
- Mobile security expertise
- Linux, Unix shell
- GenAI and Large Language Models (LLM)

Platform Solutions

- HackerOne Bounty
- HackerOne Pentest
- HackerOne Challenge
- HackerOne Triage
- Live Hacking Events

Why HackerOne

- Review of products and services by a global community of security experts
- Scale the Adobe Product Security Incident Response Team (PSIRT) reach and integrate the platform into existing workflows
- Triage services to manage a higher volume of submissions by filtering out noise and prioritizing addressing security risks



> ***"Having a bug bounty program is not an option, it's essential. Scaling internal testing can only go so far, working with the community helps uncover issues we may not have."***
>
> **Daniel Ventura**
> Product Security Manager, Adobe PSIRT & Bug Bounty

Building Community and Engagement with Hackers

Adobe sees tremendous value in the ethical hacking community and is actively pursuing an offensive security strategy through various private security testing programs and public initiatives like the Researcher Hall of Fame and the Ambassador World Cup (AWC).

As of May 2024, Adobe has efficiently resolved over 7,403 reports and acknowledged the efforts of 1,473 ethical hackers participating in its program since 2015. This demonstrates Adobe's commitment to security, underscored by the rapid response times—an average of just eight hours to initial contact. Adobe's proactive approach and response efficiency demonstrate its dedication to attracting top-tier security talent and enhancing security for Adobe products.

Celebrating Researcher Contributions

The hacking community recognizes Adobe as a leading collaborator. Alongside its bounty program, Adobe recently launched a Researcher Hall of Fame Initiative to highlight and further engage security researchers as they collaborate to enhance digital security. This initiative celebrates exceptional researchers contributing to Adobe's product security and participating in Adobe's dedicated bug bounty program. These efforts reflect Adobe's dedication to and appreciation of the ethical hacker community, which is crucial to strengthening its digital security.

Higher Impact Reports with AWC

The Ambassador World Cup is a multi-round live hacking event that builds community engagement and ambassador brand awareness in the ethical hacker community. The AWC is led by HackerOne Brand Ambassadors, allowing hackers worldwide to team up to identify impactful vulnerabilities in participating customer programs. A.S. Watson, Epic Games, Mercado Libre, MetaMask, OpenSea, Shopify, Stripe, TikTok, Tinder, and Yahoo joined Adobe in the 2023 AWC.

> ***Participating in the AWC was an incredible opportunity for Adobe to build deep relationships with the hacker community. I received great feedback about our bug bounty program and the AWC experience. Many hackers were new to our program, which was a great way to expand Adobe's outreach to the hacking community.***
>
> **Daniel Ventura**
> Product Security Manager, Adobe PSIRT & Bug Bounty

By participating in the AWC, Adobe guided hackers toward focusing on select web properties: Photoshop Web, Lightroom Web, Adobe Sign, Adobe Commerce (formerly Magento), Adobe Firefly, and Adobe Identity Management System (IMS). On average, the AWC generates 32% high or critical reports, compared to around 20% in a typical bug bounty program. This increase in reports is due to the AWC's commitment to bringing in motivated hackers whose collaboration and creativity help them find more novel bugs. Adobe participated in the final AWC round, hosted live in Buenos Aires, Argentina, which allowed them to develop direct, personal relationships with hackers, thereby adding a new and valuable element to their security strategy.

Driving Safer, More Secure AI Innovation With the Community

With a strong foundation in cybersecurity, Adobe has focused on mitigating risks associated with generative AI by fostering transparency about the capabilities and limitations of large language models (LLMs). By engaging with ethical hackers, Adobe enhances its security measures and addresses potential AI vulnerabilities early in the development process.

To that end, Adobe's bug bounty program includes rewards for discovering vulnerabilities in Content Credentials and Adobe Firefly. Content Credentials, built on the C2PA open standard, provide tamper-evident metadata for digital content, ensuring transparency in creation and editing processes. These credentials are integrated into Adobe applications like Firefly, Photoshop, and Lightroom.

Adobe Firefly, a family of generative AI models, is available as a standalone web application and within flagship Adobe apps. Adobe gathers insights on AI vulnerabilities provided by the hacking community, focusing on issues such as prompt injection and training data poisoning, as highlighted in the OWASP Top 10 for Large Language Models. Adobe's proactive approach aims to enhance AI security, foster innovation, and promote responsible AI development.

> ***"We require a proof of concept with the HackerOne report to help us focus our efforts on vulnerabilities, and that's where the bug bounty programs program shines."***
>
> **Daniel Ventura**
> Product Security Manager, Adobe PSIRT & Bug Bounty

Increasing Security Through Collaboration

Adobe's various programs and initiatives underscore its commitment to embracing human-powered security as a key element in testing its software and services through a hacker's mindset. Adobe's security team understands that if ethical hackers can uncover vulnerabilities, so can malicious actors, and a strategy that leads to closer collaboration between teams to understand and counter adversary tactics is a worthwhile investment.

Scaling PSIRT With Triage Services

Adobe scaled its PSIRT by implementing HackerOne's triage services to manage the volume of bug submissions. The triage integration into Adobe's workflows, facilitated by the HackerOne API, improves response times and efficiency. By adopting Triage, Adobe's security team enhances its vulnerability disclosure program (VDP), directly aligning it with the security demands of its public-facing digital assets and customer base. Through Adobe's bug bounty program, development teams can access detailed reports and proof of concepts demonstrating exploitable bugs from submitted tickets, giving teams more actionable insights than traditional security software scanning results. This in-depth information improves collaboration between security teams and engineers by clearly demonstrating the potential impact of bugs.

Enhancing Internal Processes

Adobe also leverages its bounty program to enhance its internal processes. Typically, bug bounty findings highlight initial access points but don't delve deeper. The Adobe Red Team, in some cases, leverages these initial footholds and explores the extent to which an adversary might exploit them. This approach helps the security team discover the full impact of a potential exploit by measuring how long such intrusions can remain undetected and how much data access an attacker could achieve. The Red Team continuously assesses the effectiveness of Adobe's internal detection and response capabilities by employing real-world attack methods.

Enhancing the Hacker Experience

The bug bounty program provides the Adobe security team with collaboration, expertise, and unique perspectives. HackerOne Triage plays a pivotal role in the bug bounty program by acting as a proxy between the hackers and Adobe's security team. Triage helps Adobe be the best collaborator possible with the hacker community and continues to bring new hackers into their program. The positive engagement with a global community of security experts delivers detailed insights, enhancing the overall security of Adobe's products and services.

Keeping Up With Hackers

Adobe is also a member of HackerOne's Technical Advisory Board (TAB), a select group of HackerOne customers that convenes in an annual, two-day joint session with the Hacker Advisory Board (HAB). The HAB consists of some of the top hackers in the community. Through the TAB, Adobe stays in tune with the evolution of how ethical hackers approach hacking and builds deeper relationships through in-person discussions around strategy, industry trends, and attack surface security.

> "***The community is a force for good. Partnering with ethical hackers helps us build increased resilience and confidence in our product security posture because more eyes on our products translates to better coverage.***"
>
> **Daniel Ventura**
> Product Security Manager, Adobe PSIRT & Bug Bounty

Rethinking Traditional Pentests

Adobe has expanded its comprehensive security strategy by working with HackerOne Pentest as a Service (PTaaS) as an additional layer for its pentesting efforts.

> ***HackerOne includes our product teams in the process so they can interact directly with the pentester to understand the analysis. It offers seamless integration with existing systems by creating tickets automatically.***
>
> **Daniel Ventura**
> Product Security Manager, Adobe PSIRT & Bug Bounty

HackerOne's PTaaS offering brings the following enhancements to Adobe's pentesting process:

Elevated Vulnerability Discovery:

Community-driven pentesting increases the discovery of unique vulnerabilities, helping strengthen Adobe's security defenses.

Platform Integration:

Adobe's product team can directly engage with pentesters on the HackerOne platform, fostering more immediate and meaningful interactions.

Automated Ticket Creation:

Issues identified during pentests will automatically generate tickets, streamlining the issue-tracking process for the security team.

Streamlined Launch:

The accelerated setup and scheduling process helps with rapid deployment of HackerOne's pentesting services.

> ***Collaboration with HackerOne, in addition to Adobe's pentests, uncovers unique vulnerabilities while helping Adobe meet customer security expectations. We're leveraging the HackerOne platform for reporting, ticketing automation, and taking action on further details on vulnerabilities reported.***
>
> **Dana Pirvu**
> Manager, Product and Software Security, Adobe

hackerone | Adobe

HackerOne has vetted hackers for organizations including:

gm

Lufthansa

ZEBRA

zoom

Spotify

citrix

PayPal

Uber

HYATT

U.S. Department of Defense

Google

reddit

Nintendo

Adobe

A.S. Watson Group

sumo logic

yahoo!

priceline

shopify

slack

yelp

salesforce

TOYOTA

Contact us

About Adobe
Adobe is changing the world through digital experiences. For more information, visit www.adobe.com.

About HackerOne
HackerOne pinpoints the most critical security flaws across an organization’s attack surface with continual adversarial testing to outmatch cybercriminals. HackerOne’s Attack Resistance Platform blends the security expertise of ethical hackers with asset discovery, continuous assessment, and process enhancement to reduce threat exposure and empower organizations to transform their businesses with confidence. Customers include Citrix, Coinbase, Costa Coffee, General Motors, GitHub, Goldman Sachs, Hyatt, Microsoft, PayPal, Singapore’s Ministry of Defense, Slack, the U.S. Department of Defense, and Yahoo. In 2023, HackerOne was named a Best Workplace for Innovators by Fast Company.