A history of bug bounty programs & incentivised vulnerability disclosure

BY ANNA HAMMOND · JUNE 23, 2021 · LAST UPDATED ON MARCH 6, 2025

Hacker-powered security and bug bounty programs are growing concepts within the cybersecurity sector today. What you may not know is that ethical hacking, often dubbed as white-hat hacking, predates black-hat hacking activities. Throughout the sixties, hacking simply meant optimising systems and machines to make them run more efficiently.

Today, we're going to circle back to the beginning of bug bounty programs to discover how incentivised vulnerability disclosure came to be. In this blog, we're exploring the history of bug bounty programs.

The history of bug bounty programs and incentivised vulnerability disclosure

1995: The world's first bug bounty

In 1995, Netscape took the initiative to offer a cash reward for non-employees to report bugs. They launched a brand new cybersecurity concept, now known as a bug bounty, for their Netscape Navigator 2.0 Beta.

Netscape's Vice President of marketing, Matt Horner, gave some context on the decision at the time: "By rewarding users for quickly identifying and reporting bugs back to us, this program will encourage an extensive, open review of Netscape Navigator 2.0 and will help us to continue to create products of the highest quality."

The impressive and forward-thinking program ran until the final release of Netscape Navigator 2.0.

2002: IDefence becomes the middleman

Seven years later, bug bounty programs finally began to catch on with other software vendors. IDefence, the security firm, was the first to follow in Netscape's footsteps. They launched their Vulnerability Contributor Program whereby bug bounty hunters could report vulnerabilities discovered on *any* software. The idea was that they would take on the role of a middleman for the software vendor and researcher.

It takes three more years before IDefence's competitor, TippingPoint, launches a similar business model.

2004: Mozilla launches vulnerability disclosure for Firefox

In 2004, Mozilla launches a bug bounty program whereby researchers were offered a bounty of up to $500 for reporting critical vulnerabilities within Firefox. The program is still live and popular amongst the ethical hacker community today.

2010: Google rolls out bug bounty across its web apps

The concept of hacker-powered security begins to take off with the backing of Google. The tech giant kickstarts a bug bounty program across its web applications after successfully launching something on a smaller scale for the open-source Chromium project. Shortly after this, Mozilla expands its program to include most of its products. Other big names, such as Barracuda Networks, Deutsche Post, the German federal postal service also launch a program.

2011: Facebook launches its Whitehat program

Facebook also joins the club by launching its Whitehat program. In fact, the social media network makes quite a statement by putting no upper limit on reward pay-outs. It also offers researchers a minimum earning potential of $500. In March 2011, Facebook paid a 22-year old security researcher $15,000 for a single bug, and by 2015, the social media network had paid out more than $4.3 million to researchers globally.

2013 – 2015: Bug bounty flourishes in Silicon Valley

By 2013, investment in crowd security in Silicon Valley, California, was picking up speed. Microsoft, GitHub, and Etsy, amongst others, had all also launched bug bounty programs by 2015.

2016 – 2021: Intigriti brings the benefits of bug bounty to Europe

Cybersecurity enthusiast and entrepreneur, Stijn Jans, makes the major decision to step away from his successful penetration company and commit to the world of bug bounty. He launches Intigriti and immediately hires multi-award-winning ethical hacker, Inti De Ceukelaire. With their combined knowledge and passion for sustainable security, the two began driving hacker-powered security throughout Europe.

In 2020, Intigriti raises €4.1 million to grow its ethical hacking community and protect sustainable tech companies. It also wins several awards, including Deloitte's Technology Fast 50 2020. This is an award that recognises the top 50 best-performing and fast-growing technology start-ups in Belgium, and beyond.

The future of bug bounty and incentivised vulnerability disclosure

Modern, digital businesses with a strong focus on agility will need to mirror this with agile, scalable security testing. Bug bounty programs can meet this need thanks to their stability, scalability and potential to stay one step ahead of ever-evolving cyber threats.

The world's most famous tech and innovation brands have had a lot of attention in bug bounty history for their programs. As a result, there is a common misconception about bug bounty programs that they're only for bigger companies with large budgets. There's also a belief that most programs are public. Even though many companies strive towards a public program, the reality is that most bug bounty programs begin with a private program.

A private bug bounty program is a great first step into crowd security because it enables businesses of all sizes to work with hand-selected security experts. They can also choose to exclude certain areas from

external testing as well as direct researchers to look for specific breaches, such as vulnerabilities with potential financial impact.

Hacker-powered security will continue to build momentum as perceptions of ethical hackers change and companies embrace their contribution to cybersecurity.

Interested in inviting ethical hackers to contribute towards your security testing? Speak to a member of the Intigriti team today to request a demo.

REQUEST A DEMO	VISIT THE WEBSITE	GET IN TOUCH
intigriti.com/demo	intigriti.com	hello@intigriti.com