MediaWell

News Item

Bug Bounties For Algorithmic Harms? | Algorithmic Justice League

By Josh Kenway, Camille François, Sasha Costanza-Chock, Inioluwa Deborah Raji, and Joy Buolamwini
January 27, 2022

> Paying hackers to disclose bugs was once considered radical; now, it's common.
>
> 'Bug bounty' programs (BBPs) for cybersecurity vulnerabilities, wherein participants are rewarded for identifying exploitable flaws (or security 'bugs') in software or hardware, are increasingly popular. Google, the Department of Defense, Starbucks, and hundreds of other companies and organizations regularly use BBPs to buy security flaws from hackers. A wide variety of organizations have adopted BBPs, and a growing number of people participate, most often via platforms such as HackerOne or BugCrowd.
>
> Recently, some companies have adopted BBPs to address issues beyond security bugs. For example, Rockstar Games, Twitter, and others have begun to use BBPs to address various kinds of socio-technical problems, including algorithmic harm. Yet the conditions under which BBPs might be useful for finding, exposing, and stopping algorithmic harm remain relatively unexamined. In *Bug Bounties For Algorithmic Harms? Lessons from Cybersecurity Vulnerability Disclosure for Algorithmic Harms Discovery, Disclosure, and Redress*, AJL researchers Josh Kenway, Camille François, Sasha Costanza-Chock, Inioluwa Deborah Raji, and Dr. Joy Buolamwini dive deep into the question "How might we apply BBPs to areas beyond cybersecurity, including algorithmic harm?"

Source: Bug Bounties For Algorithmic Harms? | Algorithmic Justice League