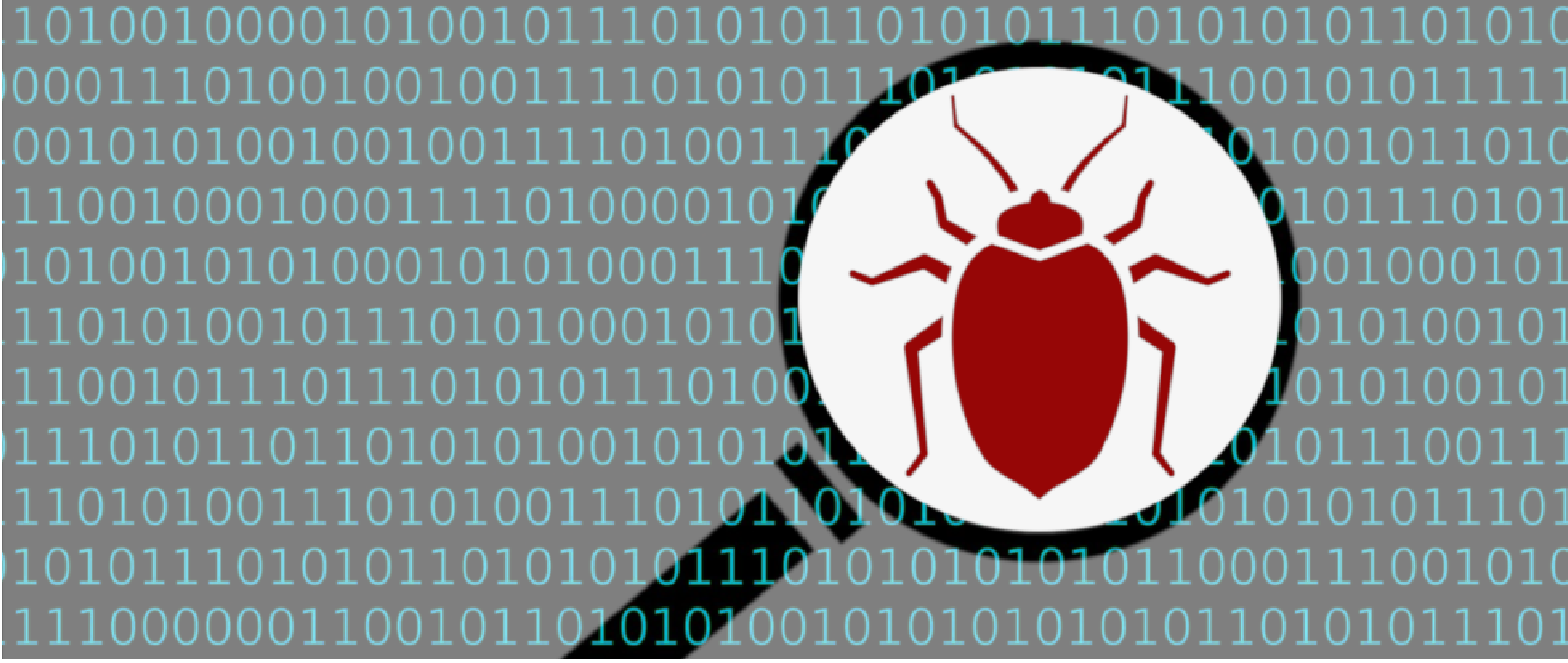

Bug Bounty Programs 101

Demystifying BBPs and Their Benefits

What is a BBP?

As federal agencies seek to improve their cybersecurity postures, there is growing interest in utilizing **Bug Bounty Programs** (BBPs) to address critical gaps. In recent years, BBPs have become an increasingly popular method used by organizations across the public and private sectors to identify and fix system vulnerabilities, particularly those relating to security vulnerabilities and exploits.

A BBP is an arrangement in which ethical hackers are given legal permission to test an organization's system(s) for vulnerabilities and report the bugs they find to the organization for a reward, usually a financial payout. Testers submit their vulnerability reports, typically through a third-party vendor, for the organization to review. If the bug is legitimate, the organization will patch the bug and compensate the finder. The significance of the discovered vulnerability determines the amount paid for it.

Bug Bounty Success Stories

Many types of critical bugs can be found during BBPs. For example, during a Shopify BBP, a participant reported that they could gain administrative access to the site by setting up two partner accounts with a shared email. Meanwhile, the first BBP run by the public cryptocurrency exchange Kuna uncovered numerous critical vulnerabilities which would have allowed malicious hackers to steal a user's accounts or alter their account balances.

Why Run a BBP?

The Pool of Talent: Through BBPs, organizations can leverage the collective power of many experts to test their systems in a short amount of time. A 2020 report found that it takes an organization on average 280 days to detect a security incident. With BBPs, the detection timeframe can be significantly shortened.

Cost-Effectiveness: BBPs are a comparatively inexpensive approach to enhancing an organization's cybersecurity posture. The average cost of a data breach in 2021 was $4.24 million; BBPs are a fraction of that price. As ethical hackers only receive payouts when they find in-scope bugs, BBPs can also be cheaper than hiring in-house staff or contractors to find the same system vulnerabilities.

Realistic Threat Simulation: BBPs are one of the best ways to simulate real threats against systems. Unlike malicious hackers who look for vulnerabilities for their own benefits, ethical hackers participating in BBPs identify bugs to help secure an organization's systems.

BBPs Launched in Governments

There have already been several BBPs executed by governments worldwide with rewarding outcomes. In 2016, the Department of Defense launched its highly successful Hack the Pentagon program, under which over 1,400 participants submitted 138 legitimate reports on unique vulnerabilities found in Department of Defense systems in less than a month.

Meanwhile, in 2018, the government of Singapore launched its first of many BBPs. In 2019, the European Union's European Commission announced a BBP for popular open-source projects, which led to the identification of 195 unique and credible vulnerabilities. Most recently in 2021, the Department of Homeland Security and the United Kingdom's Ministry of Defense piloted both their own similarly rewarding BBPs.

How Do I Know if Our Agency's Systems are Ready for a BBP?

You can gauge whether your agency's system(s) are ready to execute a BBP by taking **CISA's Bug Bounty Program Readiness Survey** to get your **BBP Readiness Score**. System preparedness is scored on predetermined factors that have been customized to be specifically applicable to federal agencies' systems. Take the **Survey** here [link to final survey].

To learn more about the survey and what your Readiness Score means for your agency, review **CISA's Bug Bounty Program Readiness Guide** and supporting documentation here. For more information on how to execute BBPs on your agency's system(s), contact CISA.