Hack the Pentagon & Bug Bounty 101

October 2022

Hack the Pentagon is a program run by the Directorate for Digital Services (DDS) that facilitates Bug Bounties — crowdsourced penetration tests — to assess the cybersecurity of DoD assets. Since bringing the first bug bounty to the US Government in 2016, Hack the Pentagon has facilitated over 40 bug bounties across every service and many agencies within the DoD, including many 'repeat customers' such as the Army and Air Force.

What is a Bug Bounty?

A Bug Bounty within the DOD is an organized event where you partner with approved vendors to execute a specific program with researchers also known as ethical hackers. These researchers look for vulnerabilities also known as bugs and provide detailed instruction on how to fix them. After the vulnerabilities are verified researchers are paid a preset monetary amount and community points to increase their ranking and reputation.

Bug Bounties have been around for several years and are used by some of the biggest companies in the world, such as Apple, Cisco, Facebook, Google and Twitter.

How are Bug Bounties valuable?

We continue to find that Bug Bounties are a reliable method to find critical vulnerabilities that can be missed by traditional pen tests. Hack the Pentagon bug bounties have found zero-days and CAC bypasses among other vulnerabilities.

- ➔ Researchers in Bug Bounties typically have a more diverse, often non-standard background and expertise than traditional (DoD) red teams
- ➔ Bug Bounty researchers leverage a wider variety of tactics, techniques, and procedures, including open source, commercial, or custom tools
- ➔ Bug Bounty researchers are more incentivized to find more critical vulnerabilities due to the per-vulnerability financial incentives
- ➔ In Bug Bounties, asset owners can more directly control researcher incentives, such as controlling which assets or vulnerabilities researchers should pursue.

How much does it cost?

System owners can expect to pay $250—800K per bounty. Factors to consider include; public vs. private, complexity, and scope.

How long does a Bug Bounty last?

Our typical bounties follow a 4x4x4 model; four weeks pre-planning, four weeks active bounty, and four weeks wrap up.

What assets can I test with a Bug Bounty?

Bug bounties can be used for most assets, including:

1. Websites
2. Public-facing assets such as routers or VPNs
3. Internal networks (e.g. NIPR enclaves)
4. NIPR systems or networks behind a CAC authentication wall
5. (Software) Applications
6. Internet of Things (IoT) devices
7. ICS/SCADA (preferably in a testing / non-production environment)
8. Hardware (may require in-person bug bounty, or sending samples to researchers)
9. Control systems (e.g. building automation, fire, water, alarm, and warehouse management systems)

While Bug Bounties are typically run remotely, if certain assets require in-person testing, Bug Bounty vendors can bring researchers onsite to perform an in-person bug bounty if necessary. EX: F15.

Who is a good candidate?

Successful bounties have these attributes: senior level support, funding, ability to scope the testing, and the technical expertise to allow connections into the network from the research platform and to help triage and mitigate vulnerabilities.

Find out more and submit a request at: www.hackthepentagon.mil