The Hack the Pentagon Bug Bounty Checklist

October 2022

This checklist is designed to encompass all the steps required of the Defense Digital Service (DDS), the crowdsourced security firm, and all other DoD organizations involved in the kick-off period within the phases outlined below.

Live-Hacking Launch: _____

Phase 0: Pre Works and Documentation

- [ ] Receive “commander’s intent,” or leadership endorsement of a bounty
- [ ] Identify the organization who is funding the task order
- [ ] Identify the contracting organization to issue the task order award
- [ ] Define technical scope for the assessment
- [ ] Develop the RFI package for the contracting office
- [ ] Select vendor most suitable for assessment

Phase 1: Pre-Bug Bounty Prep

Joint Asset Owner/DDS/Vendor Tasks

- [ ] Develop stakeholder contact list
- [ ] Review bounty payout tier
- [ ] Establish a cadence for update calls among all stakeholders before the live challenge begins
- [ ] Finalize Rules of Engagement (ROE) for the hackers to abide by during the assessment
- [ ] Send update to JFHQ, DODIN, and all other relevant stakeholders on assessment date and general scope (For cloud based assets, include CSSP organization)
- [ ] Create rootCA and user certificates for distribution to researchers for CAC-enabled sites
- [ ] Determine level of post-challenge phase press with your PAO Public Affairs Officer (if desired)

Asset Owner Tasks

- [ ] Identify the entities required for remediation activity
- [ ] Receive or create an incident response protocol
- [ ] Identify the specific personnel for remediation activity
- [ ] Coordinate a call with remediation internal personnel for a program overview
- [ ] Generate accounts for researchers to track their activity

Vendor Tasks

- [ ] Researcher recruitment and vetting based on skill-set and security criteria
- [ ] Training on platform and issue invitations to all parties
- [ ] Coordinate with system owner to create a VPN connection
- [ ] Phase 2- Bug Bounty Launch/StartPhase
- [ ] Troubleshoot any portal access issues with stakeholders
- [ ] Ensure timely responses from the remediation teams and respond to queries from researchers
- [ ] Assist in determining payout amounts to the researchers when necessary

- [ ] Coordinate post-challenge phase press with your PAO Public Affairs Officer

Phase 2: Launch and Run The Bounty

- [ ] Launch

Phase 3: Post Mortem

- [ ] Close out any remaining reports for triage and remediation
- [ ] Coordinate with the vendor to develop final report to include challenge metrics, vulnerability statistics, lessons learned, etc
- [ ] Coordinate a final leadership outbrief/presentation with internal and external stakeholders
- [ ] Export vulnerability reports and/or VPN activity logs for your record
- [ ] Coordinate with the vendor to shut down challenge portal and delete all vulnerability data as necessary by the system owner

Forms that will need to be completed and submitted as part of the formal process:

1. Technical scoping document
2. IGCE
3. form Section 508
4. form QASP
5. Inherently Government Functions Certificate
6. Non-Personal Services Certificate

**All available to download in the Bounty Playbook at: www.hackthepentagon.mil