U.S. ARMY
CYBER COMMAND

www.arcyber.army.mil | Follow @arcyber

Hack The Army

WHAT IS HACK THE ARMY? HACK THE ARMY 3.0

Hack The Army is a "bug bounty" program that builds on the efforts of Army and Department of Defense security professionals in safeguarding DoD and Army networks, systems and data.

The Army's program began in late 2016, following the successful launch of DoD's flagship Hack the Pentagon bug bounty initiative facilitated by the Defense Digital Service (DDS) earlier that year. DDS created Hack The Pentagon to help DoD and the military services run assessments on sensitive digital assets. With oversight from DDS's Hack the Pentagon team, DoD has now executed 14 public bounties on external-facing websites and applications, and 10 private bounties on a range of sensitive, internal DoD systems. Examples of past private bounties include logistics systems, physical hardware, and personnel systems.

The bug bounties aim to evolve the security of DoD and Army networks, systems and data by allowing skilled civilian and military security researchers -- commonly known as hackers -- to perform specific techniques against select public-facing websites, to find vulnerabilities in those sites. Civilian hackers who discover and successfully report vulnerabilities can potentially earn cash rewards.

The first iteration of Hack The Army attracted 371 "white hat" hackers – including 25 government employees, of which 17 were uniformed military personnel -- to a two-month challenge. The event produced 416 reports that yielded 118 valid vulnerabilities, and civilian hackers were awarded about $100,000 for their discoveries. That success was followed by Hack The Army 2.0 in late 2019, during which 52 hackers from six countries found 146 valid vulnerabilities on publicly accessible Army websites in just over a month and civilian hackers earned a total of $275,000.

Hack The Army 3.0, a collaboration between U.S. Army Cyber Command (ARCYBER), DDS, the Army Network Enterprise Technology Command and HackerOne was launched at the end of 2020 and wrapped up in early 2021. During that time, HackerOne reported, 11 assets were in scope and 40 unique, top-tier researchers focused their efforts on identifying vulnerabilities within DDS and Army's range of scope in two applications. The final tally showed that participants had identified 238 vulnerabilities, including 102 rated high or critical and designated for immediate remediation. More than $150,000 was awarded to eligible civilian hackers in bounties. Hack the Army 3.0 saw military researchers invited to participate in the bug hunt for the first time alongside their civilian counterparts.

HOW DO DOD BUG BOUNTIES AND HACK THE ARMY WORK?

DDS works with the agencies whose digital assets are being examined and a trusted private sector partner to recruit highly skilled researchers to conduct crowdsourced penetration tests. These registered participants are given legal consent to hack a variety of DoD assets to uncover and help fix vulnerabilities. All DoD bounties require these researchers to undergo background checks. Private bounties, or those testing internal systems, require background checks and citizenship verification before researchers gain privileged access to DoD systems and information. Most private bounties mandate the use of a virtual private network (VPN) to monitor and log researcher activity for system owner transparency and deconfliction.

During Hack The Army 2.0 hackers were asked to look at more than 60 items, such as the Arlington National Cemetery website and the army.mil domain. Hack The Army 3.0 will offer a dozen explicit domain targets of specific Army interest, as well as sign-on/authentication services and Army-owned VPNs. During the third iteration the entire *.army.mil domain can be targeted by participants as well, but rewards will be paid only for discovering certain categories of vulnerabilities.

The bounties offer both military and civilian participants a unique way to serve their country, while providing an innovative and effective means of “crowdsourcing” security solutions more quickly and economically than by developing similar solutions through more traditional methods.