hackerone

Announcing the Results of Hack U.S.

Introduction

On July 4th, 2022, Chief Digital and Artificial Intelligence Office (CDAO) Directorate for Digital Services), DoD Cyber Crime Center (DC3), and HackerOne publicly launched the "Hack U.S." bug bounty, allowing ethical hackers from around the globe to earn monetary rewards for reporting of critical and high vulnerabilities from within the DoD vulnerability disclosure program (VDP) published scope. Through the piloting of Hack U.S., DoD gains critical insights into how the hacker community competes for prizes with an end goal of strengthening the security of the hundreds of thousands of assets in the DoD scope.

Infographic Summary

HackerOne met with Katie Savage, Deputy Chief Digital & Artificial Intelligence Officer at DDS and Melissa Vice, Director, DoD VDP at DC3 from the organizing teams of Hack U.S. to discuss the impact of the challenge, why they consider hackers a must-have for an effective defense-in-depth strategy, and how the findings from Hack U.S. will help secure public-facing U.S. government information systems long-term.

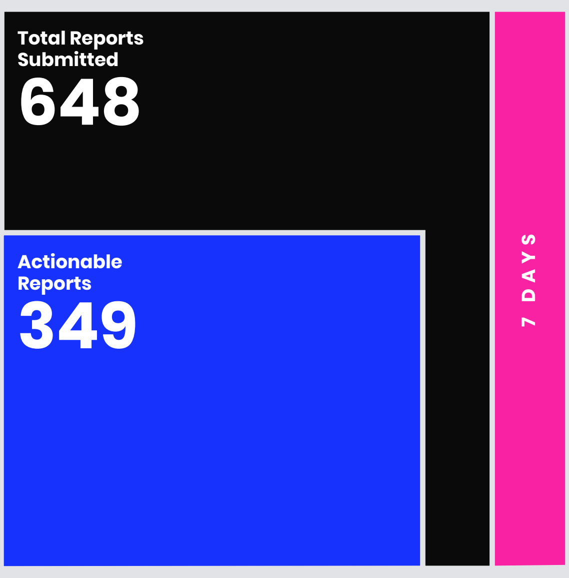
648
Total Reports Submitted

$75k
Total Bounty Paid

267
Different Researchers

VULNERABILITY STATS

Vulnerability Breakdown



> "In just seven days, Hack U.S. ethical hackers submitted 648 reports, including numerous reports which could have been critical had they not been identified and remediated during this bug bounty challenge. We knew from years of a successful VDP that professional hackers are a critical extension of our team. This bounty challenge shows the extra value we can earn by leveraging their subject matter expertise in an incentivized manner."
>
> **Melissa Vice**
> VDP DIRECTOR,
> DOD CYBER CRIME CENTER (DC3)

> "We have to make sure we stay two steps ahead of any malicious actor. By paying out monetary rewards to ethical hackers, we harden our defenses in a very impactful way. This crowd-sourced security approach is a key step to identifying and closing potential gaps in our attack surface."
>
> **Katie Savage**
> DEPUTY CHIEF DIGITAL &
> ARTIFICIAL INTELLIGENCE OFFICER,
> DDS

BOUNTIES PAID

Total Paid Bounty

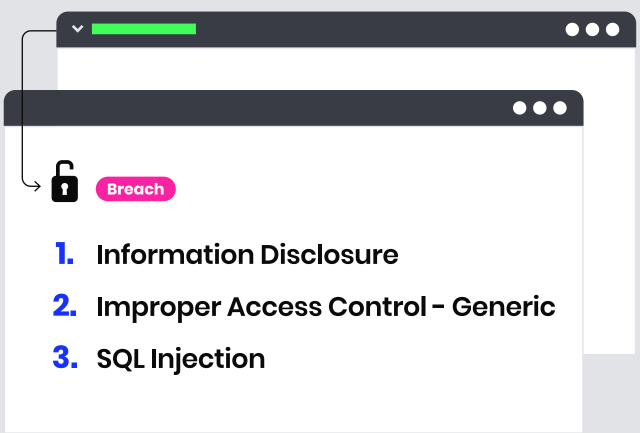
$75,000

Total Paid Bonus & Awards

$35,000

MOST COMMON VULNERABILITIES

Top Three Vulnerability Types



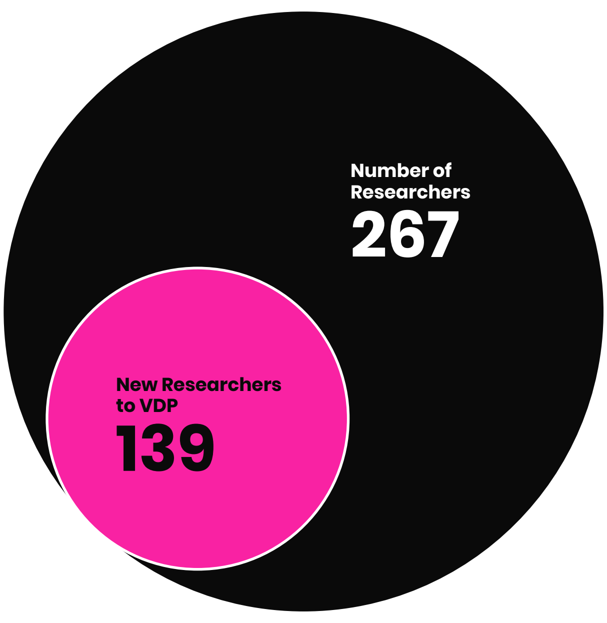
1. Information Disclosure
2. Improper Access Control - Generic
3. SQL Injection

> "Through initial evaluation of Hack U.S. reporting, the most commonly identified vulnerability is categorized as "Information Disclosure." With the identification of vulnerability trends, we can seek out patterns of detection and ultimately create new processes and system checks to ensure we address the root cause and develop further mitigations against malicious actors who might try to exploit our systems."
>
> **Melissa Vice**
> VDP DIRECTOR,
> DOD CYBER CRIME CENTER (DC3)

> "This challenge saw 267 ethical hackers participating as global team members who assisted by offensively testing DoD systems for the collaborative goal of defending the U.S. Over the years, the partnership between ethical hackers and the U.S. Government has yielded thousands of security insights and created lasting partnerships with security experts around the world. Every hacker report is another step toward lowering the collective cyber risk and safeguarding our nation, so we're grateful to every hacker who participated in Hack U.S.".
>
> **Katie Savage**
> DEPUTY CHIEF DIGITAL &
> ARTIFICIAL INTELLIGENCE OFFICER,
> DDS

HACKER INFO

The Researchers


Number of Researchers
New Researchers to VDP