

'Hack the Pentagon' program reveals 138 security flaws: US

June 18 2016



Credit: George Hodan/Public Domain

Hackers invited by the US government as part of a pilot program to find flaws with five Pentagon websites discovered 138 security vulnerabilities, Defense Secretary Ash Carter said Friday.

The "Hack the Pentagon" event, the first "bug bounty" in the history of the federal government, attracted 1,410 computer-savvy Americans,

according to the Defense Department. The program cost \$150,000, with about half of that going to hackers.

"It's not a small sum, but if we had gone through the normal process of hiring an outside firm to do a security audit and vulnerability assessment, which is what we usually do, it would have cost us more than \$1 million," Carter said during a short ceremony at the Pentagon.

"Beyond the security fixes we've made, we've built stronger bridges to innovative citizens who want to make a difference to our defense mission."

The hackers were invited to find flaws with five public websites, including defense.gov, between April 18 and May 12.

During that period, the hackers reported 1,189 vulnerabilities, with 138 of them determined to be "legitimate, unique and eligible for a bounty."

David Dworken, an 18-year-old recent high school graduate from the Washington area, appeared at the Pentagon ceremony alongside Carter and said he worked on finding bugs in his spare time.

Dworken said he has been participating in bug bounty programs since he was in the 10th grade, and plans to study computer science in college.

Although Dworken didn't reap any financial awards—the flaws he found had already been reported by others—he said participating was "incredibly rewarding" in terms of networking.

"I'm just in high school. And I have recruiters contact me about internships over the summer," he said.

Citation: 'Hack the Pentagon' program reveals 138 security flaws: US (2016, June 18) retrieved 26 April 2024 from <https://phys.org/news/2016-06-hack-pentagon-reveals-flaws.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.