



3,956
RESEARCHERS SINCE LAUNCH

26,318
ACTIONABLE REPORTS PROCESSED

Risk Level	Percentage
CRITICAL / HIGH	5%
MEDIUM	16%
LOW	30%
UNACTIONABLE	49%

ACTIONABLE (includes CRITICAL / HIGH, MEDIUM, and LOW)

Month	Submitted Questionnaires
AUG 2022	576
SEP 2022	527
OCT 2022	645
NOV 2022	282
DEC 2022	470
JAN 2023	486
FEB 2023	429

CWE-200 INFORMATION DISCLOSURE 179

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES ●●●●●●●● 77

CWE-79 CROSS-SITE SCRIPTING (XSS) ●●●●○ 31

CWE-400 DENIAL OF SERVICE ●●○ 21

In February 2023, the DoD VDP received a critical submission regarding verbose error messaging, allowing a researcher to extract PII from a government system. The researcher was able to exploit a password recovery feature found on the website to successfully enumerate valid Social Security Numbers (SSNs) of government personnel. By entering crafted data into the password recovery form the website would return a message indicating that a SSN existed or did not exist in the current database allowing the researcher to compile a list of active SSNs from the site. It is important that system owners ensure authentication messages do not reveal any information that is not required to unauthorized personnel. See the following for more information:

<https://cwe.mitre.org/data/definitions/204.html>

https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

<https://portswigger.net/web-security/authentication/securing>

The DoD VDP Researcher of the Month for February 2023 is [@7v43t!](#). They submitted a critical report of an improper error message producing sensitive information on a DoD asset; if not remediated, it would have led to credential harvesting. Thank you very much! VDP Hackers for the win!