



49,995

VULNERABILITIES SINCE LAUNCH

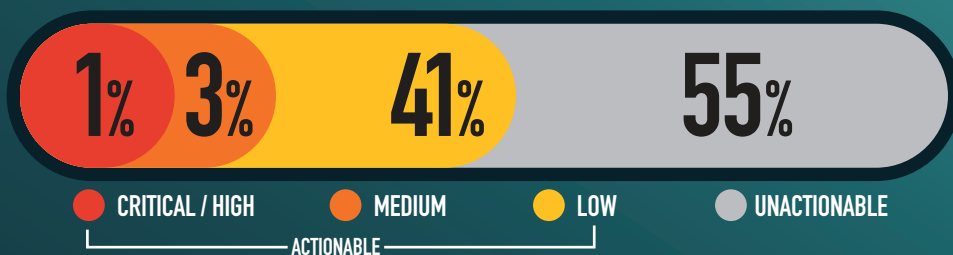
5,808

RESEARCHERS SINCE LAUNCH

28,215

ACTIONABLE REPORTS PROCESSED

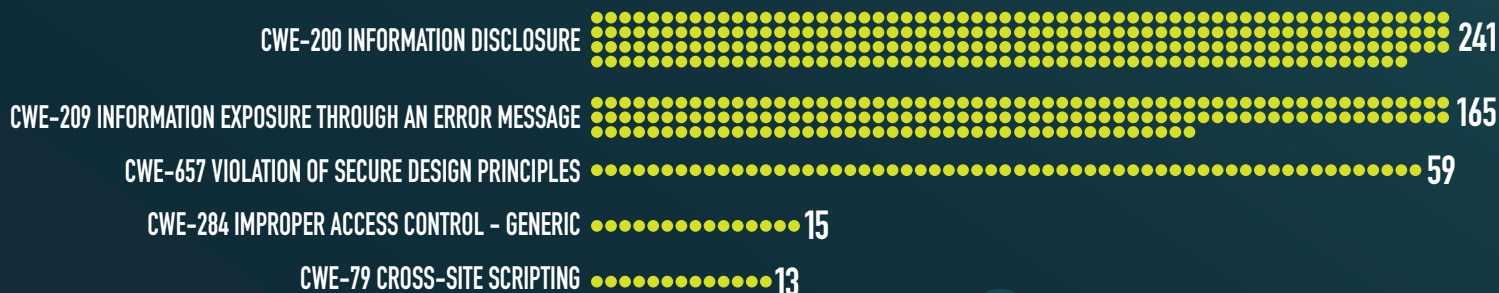
SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES



LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH



KNOWLEDGE BYTE

In February 2024, a high severity submission was received by the DoD VDP demonstrating a blind SQL injection (SQLi) vulnerability within a webservice. Blind SQL injections utilize a vulnerable query parameter to extract information from databases. The injections are "blind" because the queries don't return explicit database information. However, analyzing different responses of specially crafted queries can be used to derive valid information. Researchers identified a vulnerable parameter within the webservice that could potentially be used to determine database names and users. It is important all queries utilize appropriate input validation and safe coding practices. Further information can be found in the following resources: <https://portswigger.net/web-security/sql-injection> & https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html & <https://sites.cc.gatech.edu/fac/Alex.Orso/papers/halfond.viegas.orso.ISSSE06.pdf>

RESEARCHER OF THE MONTH

🎉 Huge congratulations to [@Krevetk0Valeriy](#), our February 2024 Researcher of the Month! 🏆 Their dedication to cyber excellence shines through, especially with their critical findings this month, including uncovering multiple PII leaks over the past 4 months. We're grateful for their invaluable contributions to our cybersecurity efforts! 🔒 Keep up the fantastic work, Valeriy! #ResearcherOfTheMonth #DODVDP 🌟