

## BUG BYTES AUGUST 2024



52,751

VULNERABILITIES SINCE LAUNCH

6,689

RESEARCHERS SINCE LAUNCH

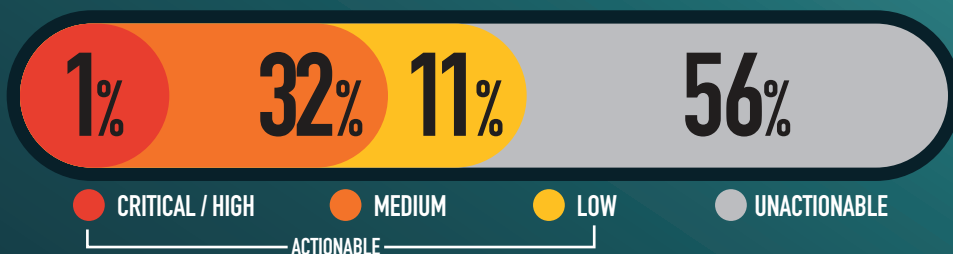
29,162

ACTIONABLE REPORTS PROCESSED

141

ACTIONABLE VDPs FOR THE MONTH

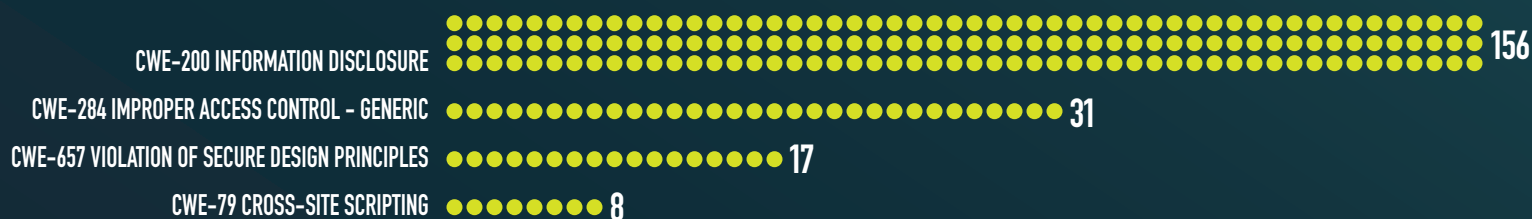
## SEVERITY FOR THE MONTH



## SUBMITTED VULNERABILITIES



## LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH



## KNOWLEDGE BYTE

In August 2024, the DoD VDP received a high-severity submission demonstrating a cross-site request forgery (CSRF) attack in a vulnerable web application. CSRF is a vulnerability where an authenticated user is manipulated into performing an unwanted action on a trusted website via a browser session. It was demonstrated that some user account setting could potentially be altered during an authenticated session. System owners are encouraged to review and implement appropriate CSRF prevention strategies. Further information is available in the following resources: <https://portswigger.net/web-security/csrf> & [https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site\\_Request\\_Forgery\\_Prevention\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html) & [https://trouge.net/papers/csrf\\_webframeworks\\_raided2021.pdf](https://trouge.net/papers/csrf_webframeworks_raided2021.pdf)

## RESEARCHER OF THE MONTH

**Critical Discovery! @Shaybt12** has found exposed credentials in a GitHub repo used by a DoD asset. This vulnerability opens the door to potential unauthorized access. **Urgent action required:** Lock down the repo and update all credentials. #CyberSecurity #DOD #InfoSec