OWASP #5 – Security Misconfiguration

Gavin Lillard (IST-103)

As implied in the name, security misconfiguration refers to flawed systems that are not correctly configured. Since it revolves around misconfiguration, it can occur at any layer of the application stack. Ways to tell if an application is vulnerable due to misconfiguration include “missing appropriate security hardening across any part of the application stack, unnecessary features being enabled/installed, default accounts/passwords are still enabled and unchanged, overly informative error alerts to users, latest security features not being enabled, security settings not being set to secure values, and out-of-date software” (Learnitweb, 2024).

Applications that offer sample applications that have admin console privileges and default passwords are an example of misconfiguration. The attacker signs in with the default password and has control of the admin console. Another example would consist of detailed error messages sent to users. This would display valuable and sensitive information the attacker can use to formulate an attack into your application/server.

According to Learnitweb (2024), ways to prevent misconfiguration of security details include an automated configuration for application environments with different credentials in each environment, minimalistic platform excluding unnecessary components, tasks to review/update the configurations implementing them as part of the patch process, and segmented architectures.

Works Cited

Team, Editorial. “A05:2021 – Security Misconfiguration - Learnitweb.” *Learnitweb*, 31 Dec. 2024, learnitweb.com/java-security/a052021-security-misconfiguration/. Accessed 23 Apr. 2025.