OWASP #7 – Identification and Authentication Failures

Gavin Lillard (IST-103)

Used to be known as Broken Authentication, this vulnerability deals with potential attackers being able to access accounts/data that is not theirs by means of a multitude of attacks. These attacks consist of credential stuffing, brute force attacks, and other automated attacks. Weak/vulnerable web applications permit these attacks alongside weak credential recovery, missing/ineffective multi-factor authentication, exposed session identifier in the URL, using the same session identifier after a successful login, and not correctly invalidating session IDs (Gorbe, 2024).

Stated by Gorbe (2024), there are a few examples of these attack scenarios. Credential stuffing which is the use of lists of known passwords. This means that the application can be used as an “oracle” to figure out if specific credentials are correct or not. Another example would be authentication attacks pertaining to passwords. Before recent times, “password rotation” and “complexity requirements” would push users to stay with weak passwords. As of late, people are encouraged to use multi-factor authentication, as annoying as it is.

According to Gorbe (2024), the ways to combat this vulnerability consist of the implementation of multi-factor authentication, do not create default credentials especially for administrative users, automate password checks forcing users to change passwords, secure credential recovery ensuring a safe way back into accounts, and limit failed login attempts which will keep automated/brute force attacks at ease. Following these would help ensure the safety of you and your users accounts/sensitive data.

Works Cited

Gorbe, Daniel. “A07:2021 – Identification and Authentication Failures.” *G⌬RBE*, 7 Oct. 2024, gorbe.io/posts/owasp/top-10/identification-and-authentication-failures/. Accessed 23 Apr. 2025.