Summary Post on Collaborative Discussion 1

Summary Post

Reflecting on the discussion surrounding my initial post on OWASP Top 10's A07:2021 "Identification and Authentication Failures," I appreciate the valuable insights provided by my peers, which have deepened my understanding of critical authentication measures. My original post and flowcharts outlined vulnerabilities such as permitting unlimited login attempts, lacking multi-factor authentication (MFA), and risks with weak password recovery processes. The feedback emphasized expanding these considerations, specifically around enhancing clarity and the integration of MFA during authentication.

Helen's feedback highlighted the importance of clear representation in my flowcharts. She suggested integrating adaptive authentication in cases where there are potential risk factors, such as new device logins or unusual locations. I found this suggestion insightful, as adaptive authentication adds another layer of security without imposing continuous additional verification on users. Furthermore, Helen's recommendation to showcase MFA more explicitly in the login process aligns with industry standards, where MFA is increasingly recognized as essential for securing authentication.

Additionally, feedback from another peer emphasized the need to refine the password flowchart to illustrate specific criteria for password strength and address reused passwords in separate steps. This approach could help streamline the registration process by making it clear when users are required to enhance their

password strength versus when they are advised against reusing credentials. I also found the suggestion to incorporate session management in the login flowchart crucial. This addition, referencing CWE-613 on insufficient session expiration, serves as a reminder that security in authentication extends beyond password checks and includes securing session duration and device recognition.

In conclusion, the feedback from my peers has enhanced my original post by emphasizing clarity in process depiction, reinforcing MFA's role, and expanding security measures in session and device management. Implementing these recommendations would strengthen the authentication process, helping mitigate risks associated with compromised credentials and unauthorized access, according to best practices in secure software development.

References

OWASP Top 10. (2021) A07:2021 – Identification and Authentication Failures. Available from: https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/ [Accessed 26 October 2024]

Das, S., Wang, B., Kim, A., & Camp, L. J. (2020) *MFA is A Necessary Chore!: Exploring User Mental Models of Multi-Factor Authentication Technologies*. In HICSS.