Peer Responses to My Initial Post

Peer response from Helen Oi Lam Siu

by Oi Lam Siu - Monday, 4 November 2024, 5:40 AM

Hi George,

Thank you for your insightful post on identification and authentication securities. You did an excellent job highlighting the critical vulnerabilities outlined in the OWASP Top Ten 2021, particularly focusing on weak username and password policies and insufficient protection against automated attacks, which were also one of my focus points in my initial post.

I appreciate how you incorporated the findings from Zviran and Erlich (2006) to underscore the significance of multi-factor authentication (MFA) and strong password enforcement. Your discussion on the risks associated with weak or compromised authentication methods effectively highlights the potential consequences, such as unauthorized access and data breaches.

Regarding your flowcharts, I was impressed by how clearly they illustrate the processes for registration and login authentication between the user and the system, which aligns with the suggestions from our tutor in my initial post. The first flowchart effectively demonstrates enforcing strong password policies during registration, ensuring that users cannot use default, weak, or previously used passwords. This proactive approach is crucial in mitigating the risk of unauthorized access from the beginning.

The second flowchart excellently outlines the login process with protections against automated attacks. By including steps like secure credential recovery mechanisms and defenses against credential stuffing and brute-force attacks, you provide a

comprehensive view of how to enhance security during authentication.

One suggestion for improvement might be to expand the flowcharts to include additional security measures, such as implementing adaptive authentication, where the system assesses risk factors (e.g., login from a new device or location) and requires additional verification when necessary. Additionally, explicitly showcasing the integration of MFA in your login process could strengthen your flowchart by highlighting the extra layer of security it provides.

Overall, your post and flowcharts offer valuable insights into addressing authentication weaknesses. Your detailed analysis encourages further reflection on how we can effectively implement these strategies to enhance security systems.

Looking forward to discussing these ideas further.

Best regards,

Helen

Reference:

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]

Zviran, M., & Erlich, Z. (2006) Identification and Authentication: Technology and Implementation Issues. Communications of the Association for Information Systems 17. DOI: https://doi.org/10.17705/1CAIS.01704