Initial Post

◄ Initial Post

Initial Post ►

Display replies in nested form

Settings

Initial Post

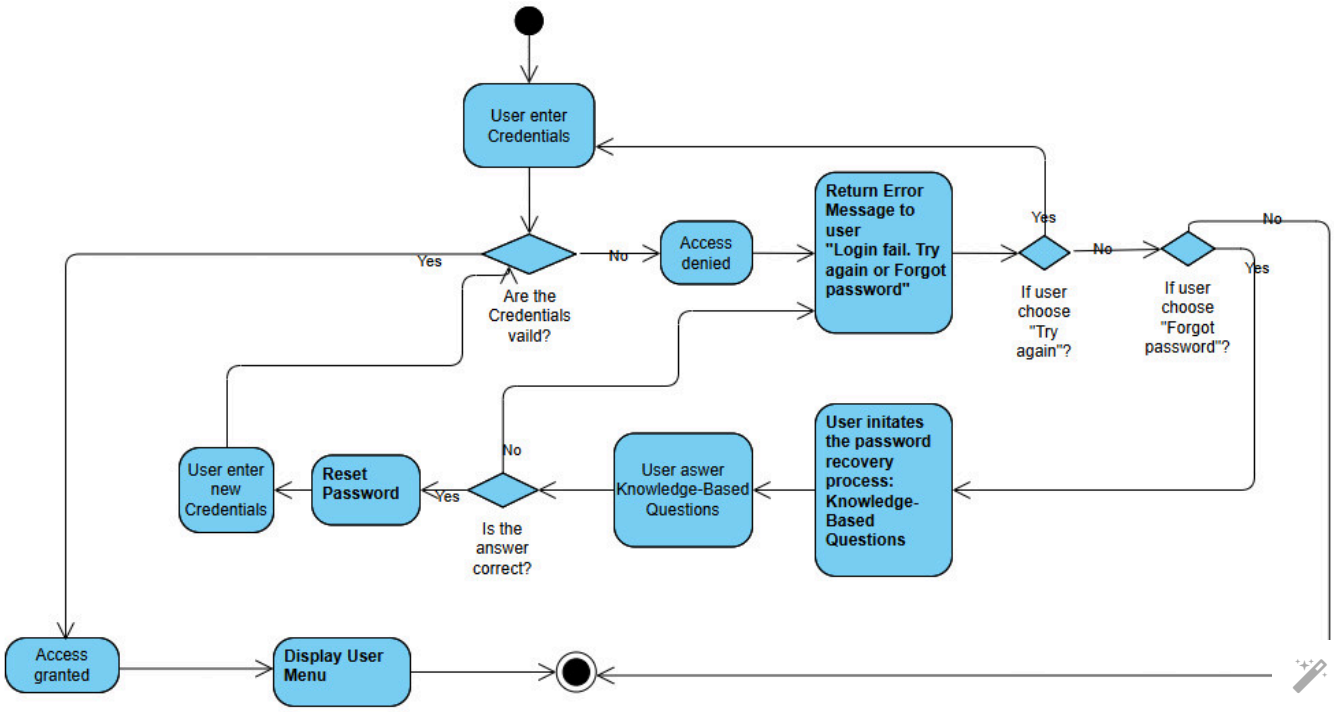
by Oi Lam Siu - Tuesday, 29 October 2024, 6:34 AM

Activity Diagram for Website Login with Identification and Authentication Failures (A07:2021)

I have chosen to use **Visual Paradigm** to create an **Activity Diagram** illustrating the website login process that has incurred several **A07 Identification and Authentication Failures** as described in OWASP Top 10:2021.

Below are the key vulnerabilities in the below Activity Diagram:

1. Permitting Unlimited Failed Login Attempts: The system does not lock out user accounts after multiple failed login attempts, which can lead to brute force or automated attacks such as credential stuffing.
2. Lack of Multi-Factor Authentication (MFA): Not requiring MFA increases the risk of unauthorized access, especially if passwords are compromised.
3. Weak Password Recovery Mechanisms: The use of Knowledge-Based Authentication (KBA) in the password recovery process, which is often easy to guess or find through social engineering, makes the password recovery process insecure.
4. Insufficient Session Expiration: User sessions aren't properly invalidated during logout or a period of inactivity.
5. Account Enumeration Risks: Specific error messages returned can lead attackers to perform account enumeration by analyzing these error messages.



The Activity Diagram is the most appropriate choice compared with other UML diagrams. It visualizing the workflow and process identifying decision points and alternative paths, which is useful to identify and address security constraints on each action. Activity Diagrams are relatively easily understood by non-technical stakeholders compared to other UML diagrams, which enhances effective

communication.

References

Gedam, N. & Meshram, B. (2023). Proposed Secure Activity Diagram for Software Development. *International Journal of Advanced Computer Science and Applications* 14(6): 671-680.

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]

OWASP (N.D.) Authentication Cheat Sheet. Available from: **https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html**

[Accessed 27 October 2024]

OWASP (N.D.) Credential Stuffing Prevention Cheat Sheet. Available from: **https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html** [Accessed 27 October 2024]

OWASP (N.D.) Forgot Password Cheat Sheet. Available from: **https://cheatsheetseries.owasp.org/cheatsheets/Forgot_Password_Cheat_Sheet.html** [Accessed 27 October 2024]

OWASP (N.D.) Session Management Cheat Sheet. Available from: **https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html** [Accessed 27 October 2024]

Visual Paradigm (N.D.) Available from: **https://www.visual-paradigm.com/** [Accessed 26 October 2024]

Maximum rating: - **Permalink** **Reply**

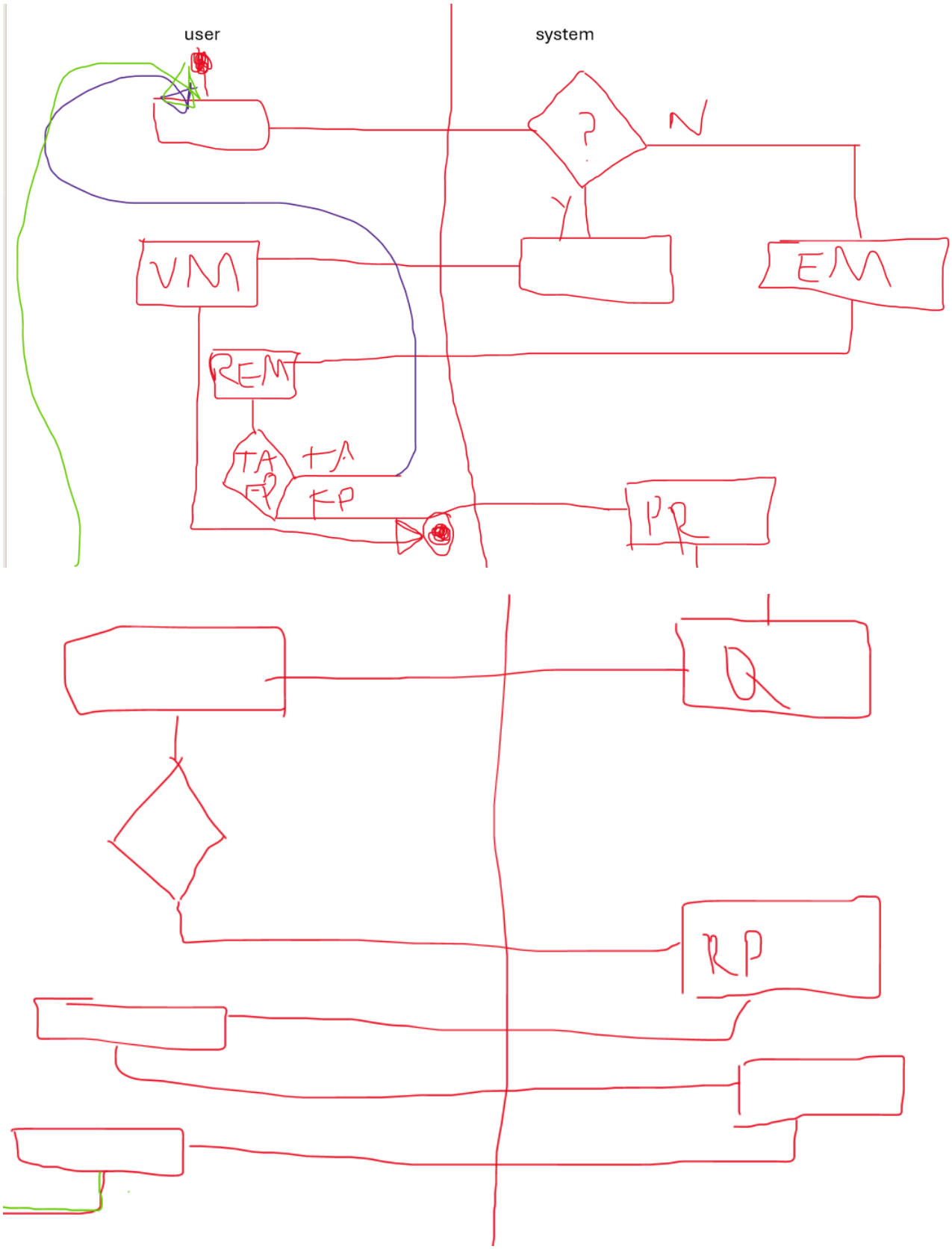
Re: Initial Post

by Cathryn Peoples - Tuesday, 29 October 2024, 2:29 PM

Hi Helen,

Please find my feedback at: https://kaplanopenlearning.zoom.us/rec/share/ZZwhQD8L5jtamsGWceHA1j83EjfIqiVOzitUqJ-oAUBRW9XeX0kcfcQq_I1_IQdm.FeduEITIGijsHIxP

Best wishes,
Cathryn



Permalink Show parent Reply

Peer Response

by Andrius Busilas - Thursday, 31 October 2024, 5:31 PM

Hi Hellen,

Selecting Open Web Application Security Project (OWASP) A07:2021 - Identification and Authentication Failures as your focus is highly relevant, given the increasing prevalence of credential-based attacks (OWASP, 2021). The vulnerabilities you identified, including insufficient account lockout measures, absence of multi-factor authentication (MFA), and inadequate password recovery processes, effectively showcase potential weaknesses in authentication systems. These selections align well with critical risk areas outlined in the OWASP Top 10 (OWASP, N.D.).

Your flowchart, created using Visual Paradigm, is commendable for its clarity and logical structure. It effectively illustrates various decision points, facilitating the visualization of potential attack vectors (Gedam & Meshram, 2023). The choice of an activity diagram format enhances accessibility for diverse audiences, including both technical and non-technical stakeholders.

To further improve the flowchart, consider incorporating a distinct path for account lockout following multiple failed login attempts (OWASP, N.D.). Additionally, implementing visual cues or color-coded elements for security-critical steps, such as MFA or session timeout checks, could enhance clarity. Elaborating on the password recovery process within the diagram would also be beneficial, allowing viewers to identify areas where knowledge-based authentication could be substituted with more robust methods like email or phone verification (OWASP, N.D.).

In conclusion, your diagram and analysis are well-constructed, and these minor enhancements could further elevate the comprehensiveness of your visualization.

References

Gedam, N., & Meshram, B. (2023). Proposed Secure Activity Diagram for Software Development. International Journal of Advanced Computer Science and Applications, 14(6), 671–680.

OWASP (2021). A07:2021 – Identification and Authentication Failures. Retrieved from https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/

OWASP (N.D.). Authentication Cheat Sheet. Retrieved from https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

Permalink **Show parent** **Reply**

Re: Initial Post

by Zukiswa Tuso - Friday, 1 November 2024, 6:58 AM

Hi Helen,

I think your post does a fantastic job of identifying the core vulnerabilities related to A07: Identification and Authentication Failures from the OWASP Top 10 (OWASP, 2021). You've clearly put thought into outlining the specific security weaknesses that can arise in a login process, which is essential for understanding where potential improvements are needed. I also think you've done a great job in listing the primary vulnerabilities, which are critical for identifying areas to improve.
Here are some suggestions:

Perhaps show specific decision points or alternative paths where additional security measures could be implemented would make it clearer how the diagram functions as a visual tool for risk identification. This approach aligns with recommendations by Gedam and Meshram (2023), who advocate for the explicit representation of decision points to enhance security in software workflows.

Your reasoning for using an Activity Diagram is well-stated, in particular the part regarding its ability to engage non-technical stakeholders effectively. Maybe this is also an opportunity to explaining why an activity diagram was the best choice.

Sequence diagrams, for example, which funny enough was my selection - are excellent for showing specific interactions but might be less effective in illustrating the overall workflow (Sommerville, 2016). This would enhance your post by showing that your choice was well-considered among several options.

Overall, you've created a well-thought-out and valuable post that highlights essential aspects of secure authentication.

References:

1. Gedam, N. & Meshram, B. (2023). Proposed Secure Activity Diagram for Software Development. International Journal of Advanced Computer Science and Applications, 14(6), 671-680.

2. OWASP Top 10. (2021). A07:2021 – Identification and Authentication Failures. Available from: https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/ [Accessed 1 November 2024].

3. OWASP. (n.d.). Authentication Cheat Sheet. Available from: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html [Accessed 1 November 2024].

4. Sommerville, I. (2016). Software Engineering (10th ed.). Pearson.

Permalink Show parent Reply

Re: Initial Post

by George Koridze - Sunday, 3 November 2024, 6:28 PM

Thank you for your insightful breakdown of the website login vulnerabilities in your activity diagram. You've highlighted key weaknesses, particularly around unrestricted login attempts, the absence of multi-factor authentication (MFA), and insecure session management—all critical points in OWASP's recommendations (OWASP, 2021). Activity Diagram was a great choice, as it clearly outlines each step in the user journey and highlights specific vulnerabilities in the workflow.

In terms of strengthening these areas, incorporating multi-factor authentication (MFA) action from the list to also in the diagram would be a great addition since it provides additional layer of account security, even when passwords are compromised. Given the rise in automated attacks like credential stuffing, MFA can be considered as a crucial extra layer that verifies user identity (Zviran & Erlich, 2006).

Adding logging and alert systems that notify administrators of suspicious activities, such as repeated login attempts or password reset requests could be another addition to the list of vulnerabilities (OWASP Top 10, 2021).

Your activity diagram is clear and accessible for both technical and non-technical audiences, making it an excellent visualisation for demonstrating security weaknesses and preventions in the login process.

References

OWASP (2021) OWASP Top 10. OWASP. Available from: https://owasp.org/www-project-top-ten/ [Accessed 3 November 2024]

OWASP Top 10. (2021) A07:2021 – Identification and Authentication Failures. Available from: **https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/** [Accessed 3 November 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

Permalink Show parent Reply

◄ Initial Post Initial Post ►