Summary Post

◄ Initial Post

Display replies in nested form

Settings

Summary Post

by Oi Lam Siu - Friday, 8 November 2024, 6:12 AM

After reviewing the tutor and peer feedback for suggested security measures and referring to the OWASP Top 10 Proactive Controls (OWASP, 2024), I have created a new Activity Diagram (Figure 1) that implements several security measures to enhance the security of the website login process.

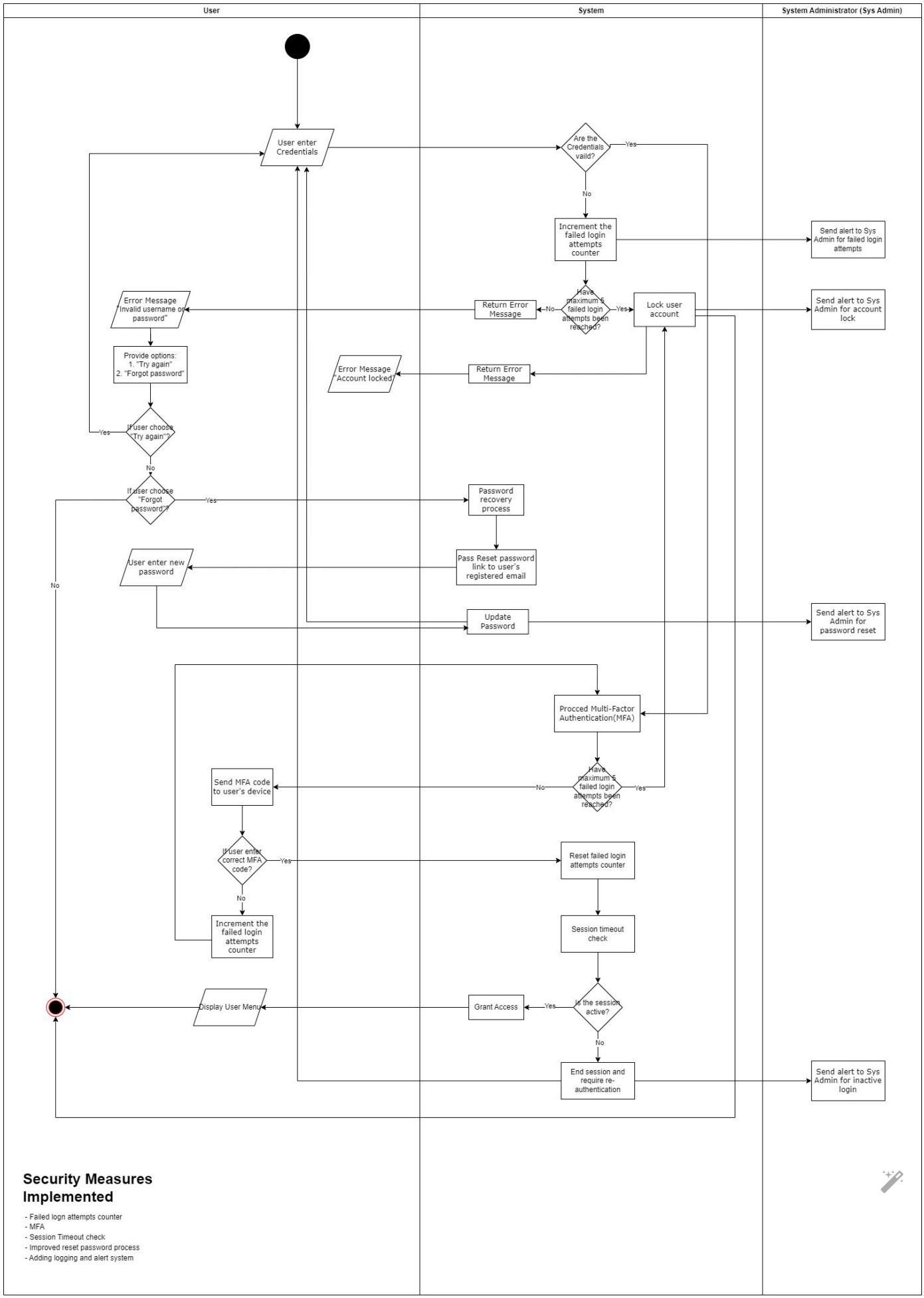
User
System
System Administrator (Sys Admin)
User enter Credentials
Are the Credentials vaild?
Yes
No
Increment the failed login attempts counter
Send alert to Sys Admin for failed login attempts
Have maximum 5 failed login attempts been reached?
No
Yes
Lock user account
Send alert to Sys Admin for account lock
Return Error Message
Error Message "Invalid username or password"
Provide options:
1. "Try again"
2. "Forgot password"
Return Error Message
Error Message "Account locked"
If user choose "Try again"?
Yes
No
If user choose "Forgot password"?
Yes
Password recovery process
Pass Reset password link to user's registered email
User enter new password
No
Update Password
Send alert to Sys Admin for password reset
Procced Multi-Factor Authentication(MFA)
Have maximum 5 failed login attempts been reached?
No
Yes
Send MFA code to user's device
If user enter correct MFA code?
Yes
No
Reset failed login attempts counter
Increment the failed login attempts counter
Session timeout check
Is the session active?
Yes
No
Grant Access
Display User Menu
End session and require re-authentication
Send alert to Sys Admin for inactive login
Security Measures Implemented
- Failed logn attempts counter
- MFA
- Session Timeout check
- Improved reset password process
- Adding logging and alert system

Figure 1: Activity Diagram for Website Login

Below are the details of the security measures implemented:

Failed Login Attempts Counter

The system increments a counter each time a user fails to log in successfully. After a maximum of 5 failed attempts, the account is locked.

Aligned with OWASP Proactive Control C7: Secure Digital Identities (OWASP, 2024), which emphasises protecting user identities by implementing strong authentication mechanisms, including account lockout policies to prevent unauthorised access through brute force attacks.

Multi-Factor Authentication (MFA)

Users must enter a correct MFA code sent to their registered device after providing valid credentials.

Aligned with OWASP Proactive Control C7: Secure Digital Identities (OWASP, 2024), adding an additional layer of security beyond passwords, reducing the risk of unauthorised access even if credentials are compromised.

Session Timeout Check

The system checks if the session is active and ends the session, requiring re-authentication after inactivity or a predefined time.

Aligned with OWASP Proactive Control C1: Implement Access Control (OWASP, 2024), ensuring that user access is appropriately managed and that sessions are securely maintained and terminated to prevent unauthorised use.

Improved Reset Password Process

Password reset links are sent to the user's registered email without revealing whether the account exists, accompanied by alerts to the system administrator.

Aligned with OWASP Proactive Control C7: Secure Digital Identities (OWASP, 2024), securing the process of handling digital identities, including password resets, and preventing account enumeration by not disclosing account validity.

Adding Logging and Alert Systems

Alerts are sent to system administrators for failed login attempts, account locks, password resets, and inactive logins.

Aligned with OWASP Proactive Control C9: Implement Security Logging and Monitoring (OWASP, 2024), enabling detection and response to suspicious activities, facilitating timely intervention and incident response.

By aligning the security measures in the activity diagram with the OWASP Top 10 Proactive Controls 2024, particularly focusing on C1: Implement Access Control, C7: Secure Digital Identities, and C9: Implement Security Logging and Monitoring, the risks associated with A07: Identification and Authentication Failures (OWASP, 2021) can be effectively mitigated.

References

OWASP. (2021) OWASP Top 10 – A07:2021 – Identification and Authentication Failures. Available from: OWASP [Accessed 26 October 2024]

OWASP. (2024) OWASP Top 10 Proactive Controls – Top 10 2024. Available from: OWASP Proactive Controls [Accessed 7 November 2024]

Bibliography

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

Soni, R. (2020) Login Security: 7 Best Practice to Keep Your Online Accounts Secure. Available from: **https://www.loginradius.com/blog/identity/login-security/** [Accessed 8 November 2024]

Tan, T.G. et al. (2020) Securing Password Authentication for Web-based Applications. DOI: 10.48550/arXiv.2011.06257

Maximum rating: -