Review an Application using OWASP

Professor: Paul Dunn
Name: Muhammad Zainul Zahid
Date: November 18, 2023

The American Express Mobile Banking app is an essential tool that helps users transact, handle their accounts, and keep an eye on their finances while they're on the go. This feature-rich application provides a complete banking experience on a portable device by enabling a variety of functions, such as checking balances and making payments.

Examining its security environment, a step-by-step analysis is conducted. First, the analysis moves through the elements and user interfaces of the application. With its login screens, account summaries, and payment interfaces, the user interface becomes apparent as a central feature. Upon closer examination, it becomes clear that the app relies on APIs to communicate with American Express servers; it stores vital data such as transaction histories, user account information, and personal data; additionally, it may incorporate third-party services into its architecture. Wi-Fi and cellular networks are two examples of network communication channels that are essential for data transmission.

As the investigation goes on, the emphasis switches to evaluating the attack surface and identifying any weak points that might allow for security breaches. Authentication mechanisms are vulnerable to credential stuffing and brute-force attacks, especially when it comes to the login screens. Furthermore, there are inherent risks in segments that involve the transmission of sensitive data, like payment processing and account details storage. The APIs draw attention to vulnerabilities as well because they act as gateways for managing user data or interacting with servers.

The analysis delves into suggested actions to manage and mitigate these risks in an efficient manner. One way to strengthen security layers is by integrating multi-factor authentication (MFA) into authentication mechanisms. One important defense is encryption, which protects private information while it's being transmitted and discourages would-be eavesdroppers. The idea of routinely updating and patching APIs is essential for fixing known vulnerabilities and guaranteeing the app's defense against new attacks.

Strengthening authentication and encryption mechanisms is crucial in preventing unwanted access and data breaches, as this theoretical study emphasizes. Furthermore, it underscores the importance of adopting a proactive stance, promoting ongoing surveillance and prompt updates to accommodate and mitigate changing risks and weaknesses.

However, cooperation with security experts, access to complex app architecture, and specific vulnerability data are necessary for a thorough and exhaustive assessment. It becomes essential for everyone to work together to carry out a thorough assessment, pinpoint particular vulnerabilities, and successfully apply customized security measures. In the end, this theoretical analysis acts as a fundamental roadmap, providing information about possible weak points and

recommending proactive security steps to strengthen the American Express Mobile Banking app's protection against online attacks.