A2-Broken Authentication

Almost all people nowadays has an access in the internet. All users are prone to different threats. Many users do not have any knowledge about these threats.

Broken Authentication means that anonymous attackers may attempt to steal accounts from users who has accounts on the internet that contains their personal information. It happens when attackers can get into web applications without proper credentials. Attackers may use leaks from the user to impersonate them by knowing their accounts, passwords and ID’s. This is very common because a lot of users do not have any knowledge about this threat. Without knowing about this threat, users will input the requirements of the different sites or web applications that they are visiting. Some users visits sites or links without even knowing what’s in there. Some links can know the session and accounts of the user, since session IDs are not rotated after login. Users will never know about this unless they experience it. Attackers get into web applications for money laundering, identity theft and to know the sensitive information of the users. There are a lot of attackers because they can get a lot of money through online, it will be easy for them because they already have a knowledge about this. Broken authentication happens because the credentials of the users are not protected when stored using hashing. Attackers can guess or overwrite credentials because of weak password. Session ID are exposed in the URL, attackers can easily impersonate a victim and can get into the page without having proper credentials.

Medication of the threat

To prevent this broken authentication, multi factor authentication is one of the solution. This is when the page requires one or more method that the user should use like thumb print, eye scan or other authentication. Next is password checking, webpages will check their database to know the commonly used password, then the webpages will inform or give a note to the users that they should change it. Next solution is password complexity, this is when the webpages requires the user to have a password that contains a series of guidelines to have a strong password. It should contain upper and lowercase letters, digits, non-alphanumeric characters or Unicode characters. Another solution is to limit failed login, this means that when the user has 3 or more attempts of not having the correct password, then the account will lock. It will lock for hours or it depends. Developers should not avoid basic security measures because it is one of the reason why many attacks occur. Developers should validate the token given by the users every request by encrypting the back end code and comparing it with the information that the user logged in.

Example

One example is the Starbucks hack, millions of accounts was exposed and the hackers raiding the consumer’s bank accounts, credit cards and Pay Pal. Starbucks denied that the app was hacked. Starbucks blamed the consumers because of having weak passwords.