Broken Authentication

Broken authentication attacks are attempts to use flaws in the application’s authentication to use other user’s accounts. These attacks can be from a user in an application or an anonymous attacker. The attacker may be able to access admin accounts using this method which is risky for the applications users because a typical admin account has access to all modules of an application. Broken authentication and session management often come in a package because session management can also be used to access other user’s account. This attacks can be caused by all sorts of flaws like error or bugs in the implementing the authentication and session management of an application. All web and application servers are vulnerable to this kind of attack.

Risks

* Identity theft
* Leakage of personal and website data
* Administrative control to unauthorized users

Methods of attacks

• Brute Force – uses a trial and error method to obtain a user’s login credentials.

• Replay/ Playback Attack – a network attack wherein data transmission in a network is delayed or repeated thus its term replay of playback.

• Session Fixation Attack – an attack where a hacker will assume another user’s identity by using another user’s session ID which can be found in a URL or in the POST data.

• Session Hijacking – this method uses a valid computer session to gain access to information and or services in a system.

Prevention:

* Use a strong password – stronger and more complex passwords will make attackers have a hard time obtaining the user’s credentials especially through the brute force method.
* Login restriction – the number of failed attempts a user is allowed to have should be restricted. The user should be informed of the failed login attempts. Lastly, the failed passwords should not be logged.
* Change password restriction – certain credentials must be provided in order allow users to change their passwords and codes should be sent to the user’s email in order to authenticate whether the user who wants to change the account’s passwords is the account’s owner.
* Password encryption – password should be hashed and encrypted in order for the hackers to have a harder time stealing and accessing any users’ accounts.
* Credential protection in transit – when user credentials and transactions are being passed to and from the server they should be encrypted by using SSL.
* Account list protection – other people should not gain access to the account list. This can be done by using pseudonym (screen name) to actual accounts.
* Caution in browser caching – authentication and session data should not be part of the browser’s cache to prevent other users to use the back button in order to gain access to an account.
* Never trust – each component of the system should have its own authentication in order to avoid a full system being compromised.