BROKEN AUTHENTICATION AND SESSION MANAGEMENT

Made by: Me

INTRODUCTION

- Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities.

PREVALENCE - WIDESPREAD

- Developers frequently build custom authentication and session management schemes, but building these correctly is hard. As a result, these custom schemes frequently have flaws in areas such as:
  - Logout
  - Password
  - Management
  - Timeouts
  - Remember me
  - Secret question
  - Account update and etc.

DETECTABILITY - AVERAGE

- Finding such flaws can sometimes be difficult, as each implementation is unique.

IMPACT - SEVERE

- Such flaws may allow some or even all accounts to be attacked. Once successful, the attacker can do anything the victim could do. Privileged accounts are frequently targeted.

- Brute Force
- Session Spotting
- Replay Attack
- Session Fixation Attack
- Session Hijacking
- Session Expiration

EXAMPLES OF ATTACKS