**취약한 인증 공격**

- 공격자는 사용자 계정 정보를 확인 또는 인증에 사용되는 토큰 정보 입수하여 인증 과정 우회

- 취약한 인증 위험은 인증 과정이 제대로 보호되지 않아 공격자가 인증 과정 우회할 때 발생

- 예시

1) 사용자가 로그인 여러 번 실패해도 다음 로그인 시도에 제한이 없는 경우, 브루트포스 공격

2) 그래픽카드를 이용한 크래킹 프로그램 등 수억 개의 사용자명/패스워드 조합하여 공격

3) 프로그램 설치 시, 기본 관리자 계정이 “admin/admin”과 같이 쉽게 추측할 수 있는 값으로 설정

4) 패스워드 또는 패스워드를 알아내기 위한 힌트를 다른 사용자가 초기화 및 복구할 수 있는 경우-

5) 세션 관리 문제로 인해 사용자의 세션 ID가 노출되어 공격자가 세션 하이재킹 공격이 가능한 경우

6) 세션 ID를 쉽게 추측할 수 있는 경우

7) 세션에 대한 타임아웃이 없어, 오래된 세션 ID를 사용해서 인증이 가능한 경우

**1. 브루트 포스 공격**

- 특정 정보를 알아내기 위한 공격

- 패스워드 크래킹을 위해 사용 및 웹 애플리케이션을 대상으로 로그인에 필요한 사용자 패스워드를 알아내고자 할 때도 사용

- 웹 애플리케이션 중 로그인을 여러 번 실패해도 다음 로그인에 제한이 없는 경우, 무작위 값으로 무한히 로그인을 시도하여 특정 사용자의 패스워드를 알아냄.