**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 개요**

- 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.

- 두 가지 방법

**1) 일련의 문자들을 하나씩 입력**

장점: 시간이 많이 걸리지만 언젠가는 패스워드를 찾아냄. 컴퓨터의 성능이 좋아질수록 시간이 줄어듦.

단점: 패스워드의 길이가 길어질수록 공격이 어려움.

Ex) 0000부터 9999까지 입력

**2) 사람들이 자주 쓰는 패스워드 이용하여 로그인 시도 (딕셔너리 공격)**

장점: 패스워드 생성시, 기억하기 쉬운 패스워드를 사용하기 때문에 무작위보다 적은 시도로 패스워드를 알아낼 확률이 높다.

단점: 아무 의미가 없는 무작위 패스워드의 경우, 알아낼 수 없다. -> 목록이 더 많은 패스워드 파일을 사용하거나, 변형, 조합 등의 방법으로 더 많은 패스워드 검사

Ex) “password”, “iloveyou”와 같은 단어 이용

**2. 브루트 포스 공격 실습**

텍스트, 전자제품, 스크린샷, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

<보안 레벨 – Low / Brute Force>

- 직접 로그인 폼에 패스워드를 입력할 수 있지만 너무 오래 걸림

- Burp Suite의 인트루더 기능 활용

텍스트, 전자제품, 스크린샷, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

- 초기 설정: “admin”이라는 계정 이름을 알고 있음

1) Burp Suite의 인트루더 off

2) 아무 패스워드로 1회 로그인 시도

3) 히스토리에서 메시지 확인 후, “Send to Intruber”

텍스트, 스크린샷, 소프트웨어, 웹 페이지이(가) 표시된 사진

자동 생성된 설명

4) “Clear” 버튼을 눌러 선택된 것 모두 삭제

5) 패스워드 부분을 선택(블록)한 후, “Add” 버튼 클릭

6) Payload 탭으로 이동

텍스트, 스크린샷, 소프트웨어, 디스플레이이(가) 표시된 사진

자동 생성된 설명

7) “Payload type”이 “Simple list”로 되어 있다면, 페이로드 옵션 리스트에 등록된 문자열을 하나씩 사용한다는 의미

8) 페이로드 옵션에서 “Load” 버튼 클릭

9) /usr/share/john/password.lst 경로의 리스트 로드

텍스트, 스크린샷, 소프트웨어, 컴퓨터 아이콘이(가) 표시된 사진

자동 생성된 설명

10) 주석 “remove” 버튼을 이용하여 모두 제거

11) 우측 상단 “Start attack” 버튼 클릭

텍스트, 스크린샷, 소프트웨어, 번호이(가) 표시된 사진

자동 생성된 설명

12) 응답 길이 (Length)가 다른 하나 발견 (로그인 성공 응답, 나머지는 실패 응답)

13) “password”라는 패스워드 찾음

**3. 브루트 포스 공격 대응**

**1) 락킹(Locking)**

- 짧은 시간 내에 일정 횟수 이상 로그인 시도에 실패하면, 정해진 시간 동안 로그인 하지 못하게 하는 방법

- 로그인 시도 간격이 길어져서 패스워드를 찾는 데 걸리는 시간이 무한하게 늘어나 브루트 포스 공격 차단

- 공격자가 락킹을 노리고 사용자가 로그인을 못하게 만들 수도 있음

**2) 캡챠(CAPTCHA)**

- 흘려 쓴 글자나 그림 문자를 로그인 시도 시 입력하도록 하는 방법

- 사람만 식별할 수 있는 문자나 그림 이용

**4. 세션 ID 노출 사례 및 보호 대책**

- 세션 ID가 노출되면 공격자는 그 세션 ID를 이용하여 인증 과정을 우회해 웹 사이트 접속

- 세션 ID는 일반적으로 쿠키를 통해 전달

- 설정 오류나 구현상의 이유 등으로 URL을 통해 전달되는 경우도 있음 -> 세션 ID 노출 위험

- 대다수의 웹 서버들은 웹 요청을 전달받으면 요청 URI를 로그 파일에 기록

- 인터넷을 통한 웹 사이트 원격 접속은 어떤 경로로 전달되는지 알 수 없는데, 이 과정에서 중계 장치들도 요청 URI를 로그로 남김

- 공격자가 이러한 파일에 접근하게 되면 노출된 세션 ID 입수 가능

텍스트, 전자제품, 스크린샷, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

<bWAPP의 보안 레벨 – Low / Session ID in URL>

1) bWAPP에서 A2 항목 아래에 있는 “Session Management – Session ID in URL” 메뉴 선택

2) 자동으로 요청 하나 전송

3) Burp Suite의 Proxy 히스토리 기능에서 확인

텍스트, 전자제품, 스크린샷, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

4) 요청 URI의 쿼리 스트링 부분에 “PHPSESSID”가 노출되어 전송되는 것 확인

- 세션 ID는 쿠키나 폼의 히든 필드를 통해 전달되도록 구현하는 것이 좋음

- 하지만, 노출 위험이 완전히 사라지는 것이 아니기에 다음과 같은 방법 고려

1) 세션 ID가 URI를 통해 노출되지 않아야 한다.

2) 세션 ID는 HTTPS 암호화 채널을 통해 전달되어야 한다.

3) 세션 ID를 쿠키로 전달할 경우 Secure, HttpOnly와 같은 쿠키 속성 추가해야 한다.

4) 세션 ID에 유효 시간을 적용하여 일정 시간이 지나면 세션 ID를 파기한다.

5) 로그아웃이 된 세션 ID는 즉시 파기되어야 한다.

6) 웹 브라우저를 종료하면 자동으로 로그아웃 되도록 한다.

7) 세션 ID는 랜덤으로 생성되어야 하며, 절대 추측할 수 없는 값이어야 한다.