**SQL 인젝션 공격**

**1. SQL 인젝션 공격 개요**

- SQL 인젝션 취약점은 웹 서버 영역의 데이터베이스로 전송되는 SQL 쿼리문을 사용자가 임의로 조작할 수 있는 경우에 발생

- 공격자는 취약점을 이용하여 데이터베이스에 저장되어 있는 다른 사용자의 개인정보 등 허가되지 않은 정보에 접근하거나 데이터를 변조

- 두 가지 사례 (회원 ID를 입력하여 회원정보를 조회하는 웹 페이지)

- SQL 쿼리문을 구성하는 웹 애플리케이션의 소스코드를 다음과 같다고 가정

$id = $\_REQUEST[ ‘id’ ];

$query = “SELECT name, email FROM users WHERE id = ‘$id’;”;

- 위 경우에서 SQL 인젝션 취약점 발생

**1) WHERE 구문 우회**

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

- 사용자는 ID가 1인 사용자 정보 요청

- 요청을 받은 웹 애플리케이션은 내부의 데이터베이스로 다음과 같은 SQL 쿼리문 전송

SELECT name, email FROM users WHERE ID=’1’

- 쿼리문에는 WHERE 조건문에서 사용자가 입력한 ID 값 1이 조건으로 입력

- 이 쿼리문은 users 테이블에서 ID가 1인 사용자의 이름과 이메일을 가져오는 쿼리문

- 쿼리문을 받은 데이터베이스는 쿼리문을 실행하여 ID가 1인 사용자 정보 반환

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

- 공격자는 원래의 ID 값 1 대신 SQL 쿼리문 조작을 위해 다음과 같이 입력

1’ or ‘1’=’1

- 이 값을 SQL 쿼리문에 그대로 삽입하면 다음과 같이 구성

SELECT name, email FROM users WHERE id =’1’ or ‘1’=’1’;

- WHERE 이하를 보면 “or” 키워드와 함께 삽입되어 항상 참이 되는 조건으로 변경

- ID 값이 1인 사용자의 데이터뿐만 아니라 모든 사용자의 이름과 이메일 전달

- 공격자가 입력할 수 있는 입력 값에 제한이 없고, 그 입력값이 SQL 쿼리문에서 그대로 실행된다면 SQL 인젝션 성공

**2) UNION 공격**

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

- 공격자는 “or” 키워드를 이용한 구문 대신에 UNION 키워드를 삽입 후 사용자 이름과 패스워드를 요청하는 SELECT 구문을 삽입

- 다음과 같은 SQL 쿼리문이 실행

SELECT name, email FROM users WHERE ID=’1’ UNION SELECT name, pw FROM users#’

- UNION을 사이에 두고 SELECT 구문 두 개가 위치

- UNION으로 합집합으로 두 개의 SELECT 구문의 결과를 모두 포함

- ID가 1인 사용자 정보 외, users 테이블의 모든 사용자의 이름과 비밀번호 같이 반환

- 쿼리문 끝에 “#”은 MySQL DB에서 “#” 뒤에 오는 내용 주석 처리 위함

- “#”이 없다면 짝이 없는 가장 끝의 문자 “ ‘ “로 인해 에러 발생 가능성

**2. SQL 인젝션 공격 실습**

**1) WHERE 구문 우회 실습**

텍스트, 전자제품, 스크린샷, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

<DVWA level-low / SQL Injection>

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

- “User ID”에 1을 입력하면 ID가 1인 유저 admin이 출력

- SQL 인젝션 공격에 취약한지 테스트 할 수 있는 기본적인 방법은 “ ‘ “ 입력

텍스트, 스크린샷, 멀티미디어 소프트웨어, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

- 취약한 경우 위와 같은 에러 발생

- “ ‘ “을 입력하면 따옴표 쌍이 맞지 않아 형식 에러가 발생한 것 -> SQL 쿼리문에 영향을 줄 수 있음

- 처음과 마지막에 작은 따옴표를 입력하지 않는 이유는 입력 값을 문자열로 처리하는 SQL 쿼리문의 소스코드에 이미 작은 따옴표가 존재하기 때문

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

텍스트, 스크린샷, 디스플레이, 번호이(가) 표시된 사진

자동 생성된 설명

- 위와 같이 입력하면 admin 사용자 외에도 다른 사용자의 정보가 같이 출력

**2) ORDER BY 및 UNION 공격 실습**

- UNION은 합집합이기 때문에 원래의 조회하는 SELECT문의 컬럼 개수와 UNION 뒤의 SELECT 문에서 요청하는 컬럼의 개수가 같아야 함.

- 공격 성공을 위해 원래의 SQL 쿼리문이 몇 개의 컬럼을 반환하는지 알아야 함.

- 컬럼의 개수는 ORDER BY 구문으로 알아낼 수 있음

- 컬럼 이름을 ORDER BY 구문으로 지정하거나 위치 인덱스를 이용하여 정렬 가능

Ex) ORDER BY 1은 첫 번째 컬럼을 기준으로 정렬. ORDER BY 2는 두 번째 컬럼을 기준으로 정렬

- 만약, 전체 컬럼 수보다 큰 수를 입력하면 에러 발생

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

- 첫 번째 컬럼을 기준으로 정렬 시도하였을 때 정상적인 표시

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

텍스트, 스크린샷, 멀티미디어 소프트웨어, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

- 세 번째 컬럼을 기준으로 정렬하면 에러 발생 -> 컬럼의 총 개수 = 2

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

- “1' UNION SELECT 1,2#”을 입력하면 사용자 ID가 1인 사용자 정보와 함께 UNION으로 추가한 결과 표시

- SELECT 문 뒤에 상수를 입력하는 것이 가능 -> 해당 숫자가 나타나는 위치로 어떤 컬럼의 정보에 웹 페이지의 어느 위치에 나타나는지 쉽게 파악 가능 (모두 웹 페이지에 표시되는 것은 아님)

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

- Mysql DB에는 information\_schema라는 DB에서 DB 이름, 테이블, 컬럼 정보 관리

- information\_schema의 schemata 테이블로부터 schema\_name을 가져오는 SQL 쿼리문을 이용하여 DB 이름을 알아낼 수 있음

- 데이터베이스의 이름이 모두 First name 뒤에 출력

- DVWA에서 사용하는 데이터베이스는 dvwa라는 것을 추측 가능

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

- table\_schema가 dvwa인 조건을 주어 dvwa 테이블만 출력

- guestbook과 users라는 테이블 출력

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

- users 테이블의 컬럼 목록을 알아냄

- users와 password 컬럼 주목

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

- users 테이블에서 user와 password 컬럼을 가져온다.

- 사용자의 아이디와 비밀번호가 그대로 노출된다.

- 현재 비밀번호는 해시 값으로 암호화되어 있는 상태이므로 복호화를 진행해줘야 함

텍스트, 스크린샷, 폰트, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

- 웹 브라우저의 검색창에 해시 값을 입력하자 복호화된 값을 알려주는 사이트 등장

- admin 유저의 비밀번호는 password라는 것을 알아냄

**3. 블라인드 SQL 인젝션 공격**

- 블라인드 SQL 인젝션 공격은 일반적인 SQL 인젝션 공격과 달리 출력되는 결과 값이 입력 값의 존재 여부만 알려줌

- 에러가 발생하지 않도록 처리되어 있음

- SQL 쿼리문의 처리가 어떤 방식으로 되는지 모름

- SQL 쿼리문이 실행된다는 것을 알고, 입력 값에 따라 존재 유무에 대한 결과가 달라지면 블라인드 SQL 인젝션 공격을 시도해볼 수 있음

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

<1’ AND 1=1# 입력 화면>

- 위와 같은 입력을 했을 때, 정상적인 처리가 된다는 것을 확인 -> AND 조건이 같이 처리되었다는 의미, 처리되지 않으면 비정상적인 값으로 판단하여 사용자가 없다는 메시지가 나와야 함.

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

<1’ AND 1=2# 입력 화면>

- 사용자가 없다는 출력 메시지가 뜸 -> AND 뒤의 1=2가 거짓이 되기 때문

- 입력하는 값이 SQL 쿼리문을 통해 처리되는 것을 확인

텍스트, 스크린샷, 폰트, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

- 실제 소스코드를 보면 SQL 쿼리문이 사용되는 것을 확인할 수 있음.

- 위와 같은 과정을 통해 “어떤 사용자가 웹사이트에 존재하는가?”와 같은 명제의 참·거짓을 가려낼 수 있음

- 참과 거짓일 때의 결과 차이를 분석하여 어떤 정보를 알아내는 기법 -> 블라인드 SQL 인젝션 공격

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

스크린샷, 텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

텍스트, 소프트웨어, 멀티미디어 소프트웨어, 스크린샷이(가) 표시된 사진

자동 생성된 설명

- 웹사이트에 출력되는 메시지가 참과 거짓일 때, 모두 같으면 응답 시간으로 구별 시도

- SLEEP() 함수를 통해 참일 경우, 함수가 같이 동작하도록 구성

- 존재하는 사용자 ID 1을 입력했을 때는 출력이 5초간 지연되는 것을 확인

- 존재하지 않는 사용자 ID 6을 입력했을 때는 지연 없이 바로 메시지가 출력되는 것을 확인

- 블라인드 SQL 인젝션 공격의 경우 자동화 프로그램을 통해 수많은 쿼리문을 실행하여 공격

**4. sqlmap 자동화 공격**

- SQL 인젝션 공격 프로그램

- Python으로 개발된 CLI 기반 프로그램

텍스트, 스크린샷, 폰트, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

- 여러 가지 옵션 중 자주 사용되는 옵션

1) -u: 필수 옵션으로 공격을 시도할 URL 지정

2) --cookie: 로그인이 필요한 경우, 로그인하고 난 다음 발급된 세션 쿠키 값 지정

3) --data: POST 요청의 폼을 공격하고자 할 때, 바디로 전달되는 데이터 지정

4) -p: 테스트할 파라미터 지정

5) --dbms: 데이터베이스의 종류를 알고 있는 경우 지정

6) --current-db: 현재 데이터베이스의 이름 알아내기

7) -D: 데이터를 입수할 데이터베이스 지정

8) -T: 데이터를 입수할 테이블 이름 지정

9) -C: 데이터를 입수할 컬럼 지정

10) --tables: 데이터베이스의 테이블 알아내기 (주로 -D 옵션과 같이 사용)

11) --columns: 데이터베이스의 컬럼들 알아내기 (주로 -D, -T 옵션과 같이 사용)

12) --dump: 데이터베이스의 정보 알아내기