SQL INJECTION

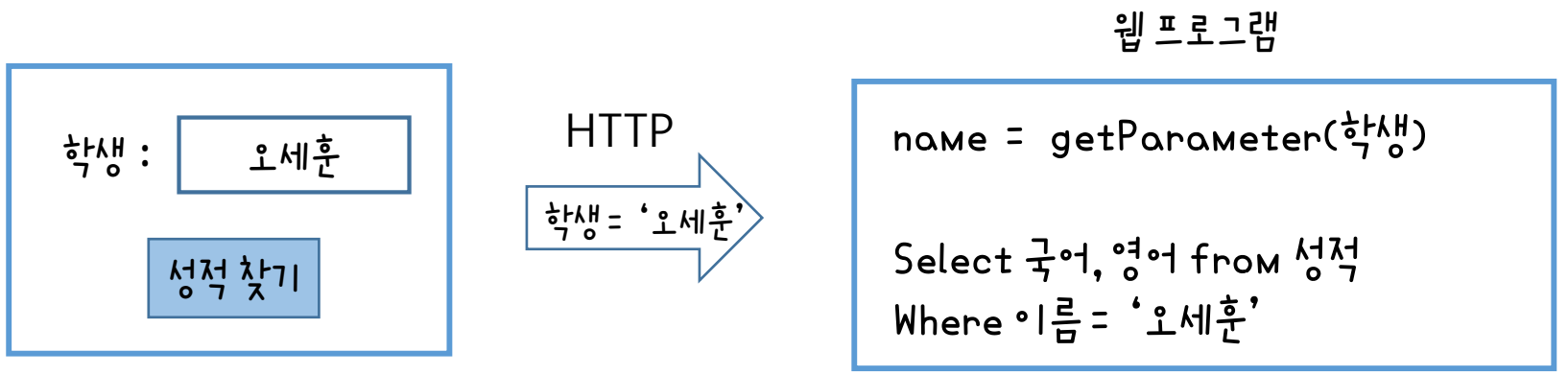
18.07.05

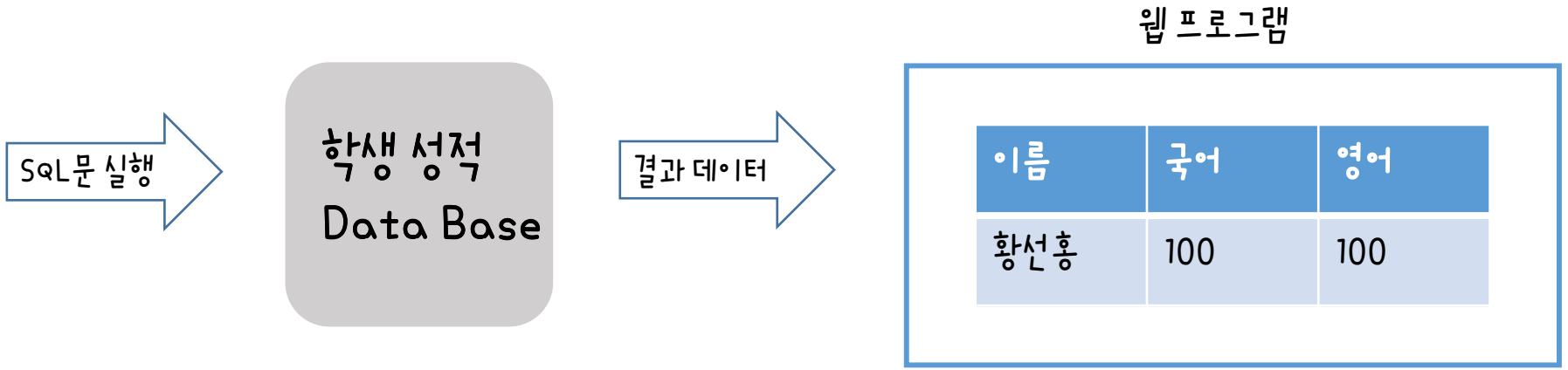
〈 목차 〉

1. SQL injection 이 뭐니..?

? DB의 데이터를 다루는 프로그램 언어

- 웹사이트 보안상의 허점을 이용해 특정 SQL문을 보내서 데이터 베이스의 중요 정보나 공격자가 원하는 정보를 가져오는 해킹 기법

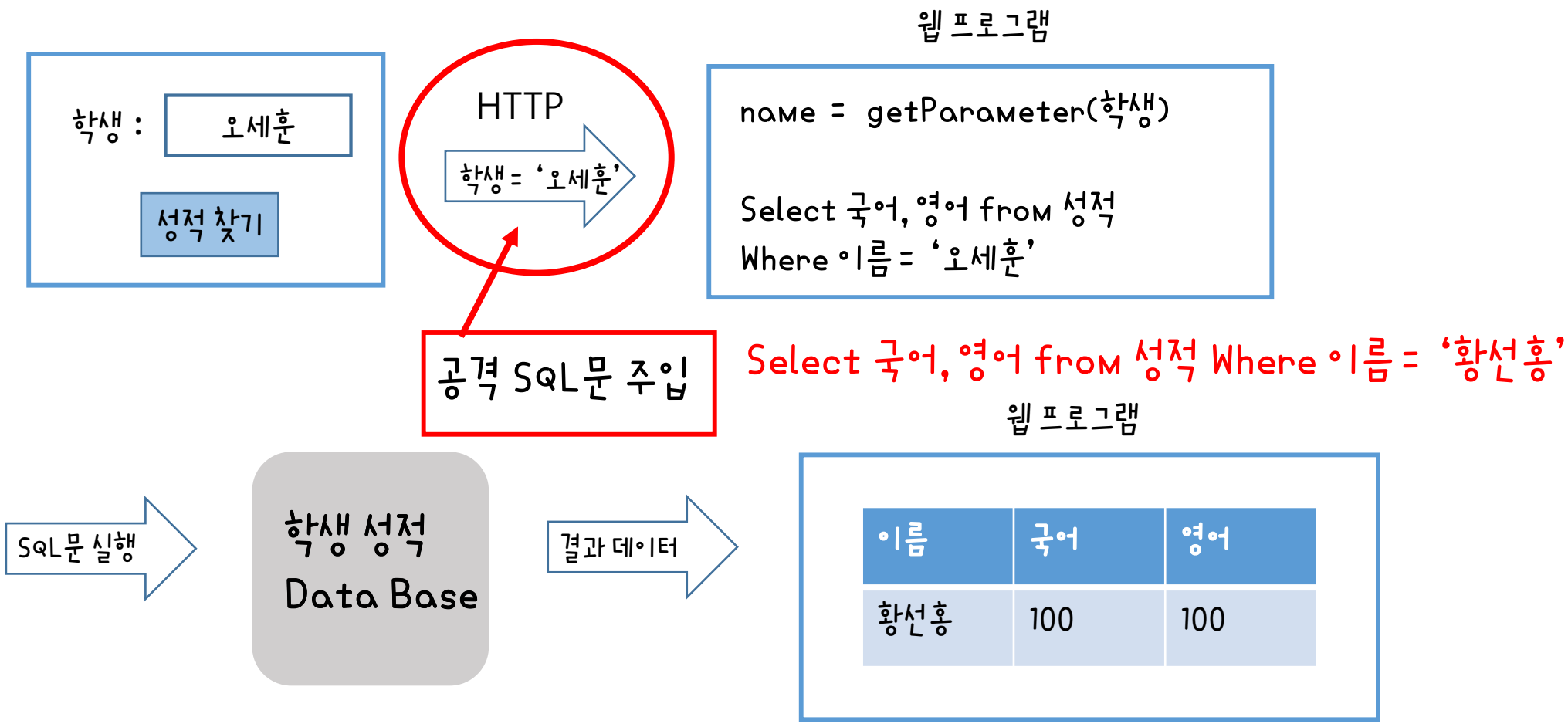




1. SQL injection 이 뭐니..?

? DB의 데이터를 다루는 프로그램 언어

- 웹사이트 보안상의 허점을 이용해 특정 SQL문을 보내서 데이터 베이스의 중요 정보나 공격자가 원하는 정보를 가져오는 해킹 기법



1. SQL injection 이 뭐니..?

SQL injection 공격의 종류

1. 특정 데이터 조회

2. 인증 우회

3. 기밀 데이터 접근

4. 웹 사이트 콘텐츠 변경

5. DB 서버 shutdown

2. Los wargame 1번 문제

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__);
?>
```

2. Los wargame 1번 문제

?id = Yell&pw = 1234

query : **select id from prob_gremlin where id='yell' and pw='1234'**

```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__);
?>
```

2. Los wargame 1번 문제

query : **select id from prob_gremlin**

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__);
?>
```

Q&A