

## < 목차 >

1. LFI & RFI

2. 실습

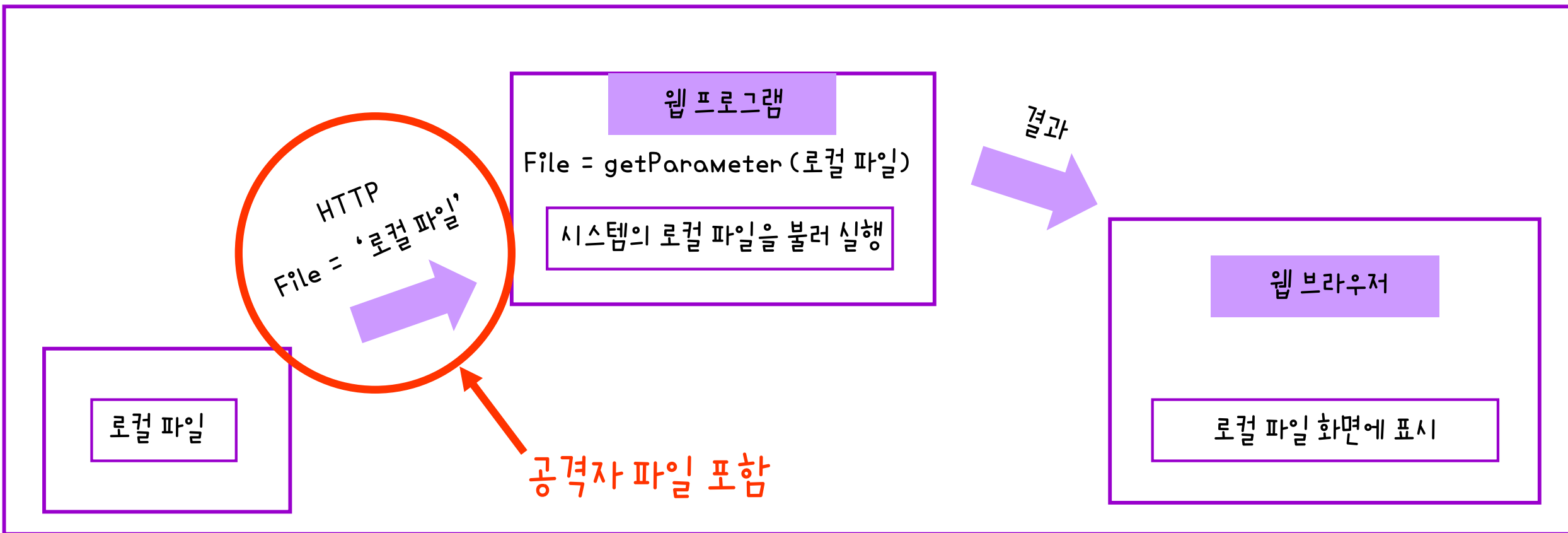
3. Q&A

# 1. LFI & RFI

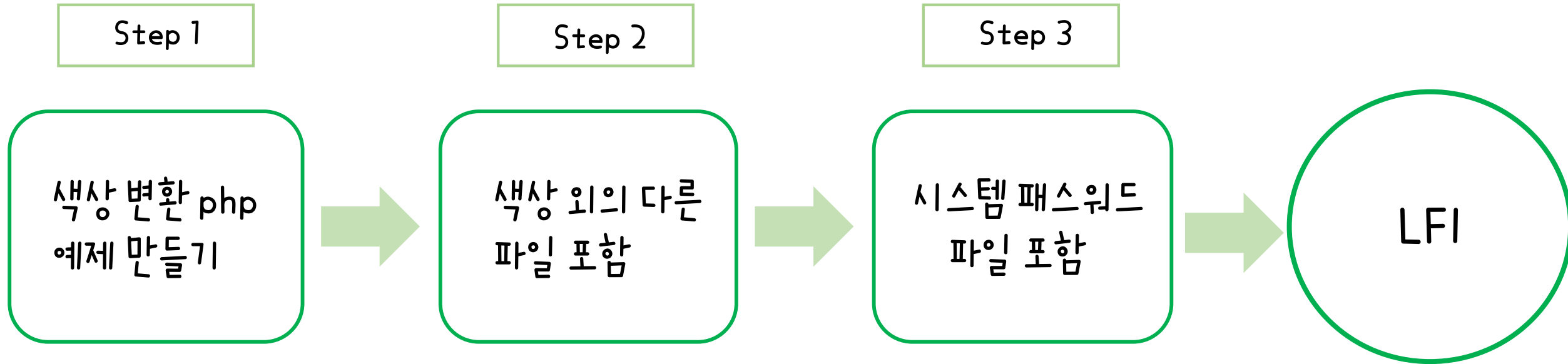
\* Inclusion ??

- LFI - Local에 대한 File Inclusion
- RFI - Remote에 대한 File Inclusion

내 외부에서 특정 파일을  
포함시키는 해킹 기법



## 2. 실습



## 2. 실습

### Step 1

#### Color.html

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

#### Blue.php

```
<center>
<font color = 'BLUE'><h1>BLUE</h1></font>
</center>
```

#### Red.php

```
<center>
<font color = 'red'><h1>RED</h1></font>
</center>
```

#### Vulneable.php

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

## 2. 실습



red ▼ 제출



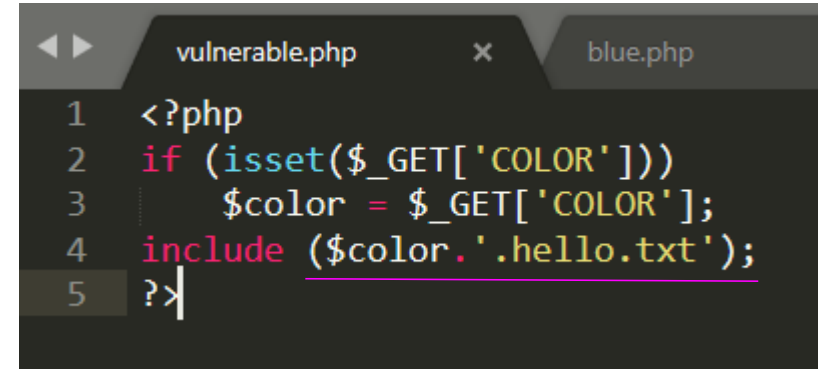
RED

## 2. 실습

### Step 2

Hello.txt

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



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

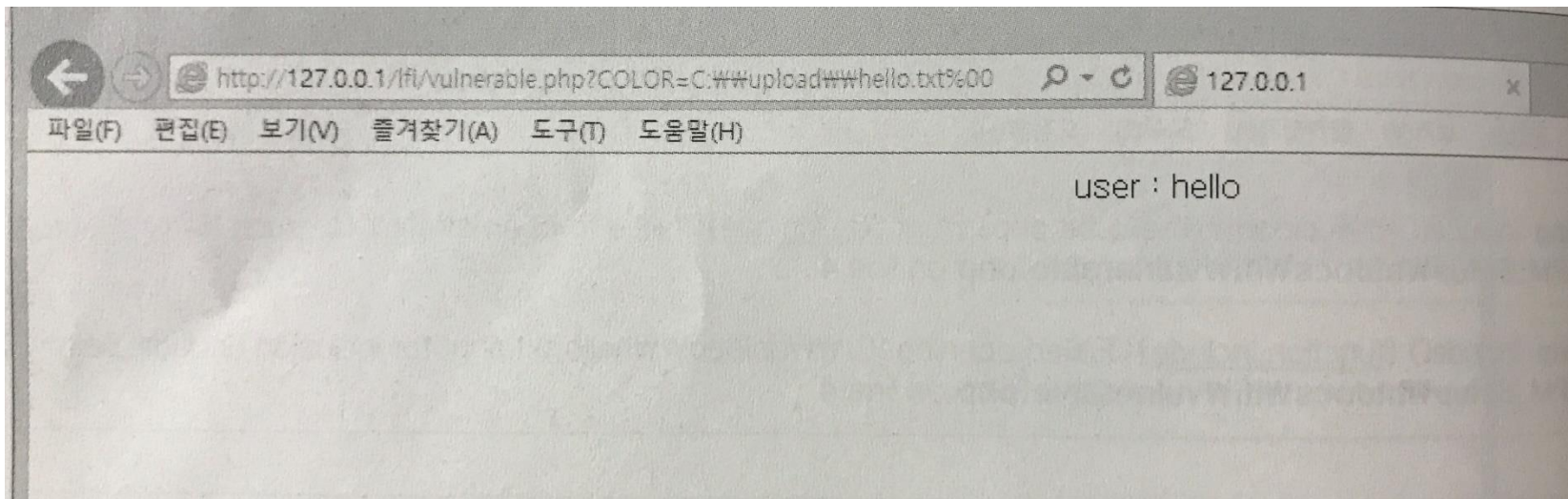
← → ↻ ⓘ 127.0.0.1/ifi/2/vulnerable.php?COLOR=C:₩upload₩₩hello.txt

**Warning:** include(C:₩upload₩₩hello.txt.php): failed to open stream: No such file or directory in C:₩AutoSet9₩public\_html₩ifi₩2₩vulnerable.php on line 4

**Warning:** include(): Failed opening 'C:₩upload₩₩hello.txt.php' for inclusion (include\_path='.') in C:₩AutoSet9₩public\_html₩ifi₩2₩vulnerable.php on line 4

## 2. 실습

`http://127.0.0.1/lfi/2/vulnerable.php?COLOR=C:₩₩upload₩₩hello.txt%00`



← → ↻ ⓘ 127.0.0.1/lfi/2/vulnerable.php?COLOR=C:₩₩upload₩₩hello.txt%00

**Warning:** include(): Failed opening 'C:₩₩upload₩₩hello.txt' for inclusion (include\_path='.') in **C:₩₩AutoSet9₩₩public\_html₩₩lfi₩₩2₩₩vulnerable.php** on line 4



## 2. 실습

### Step 3

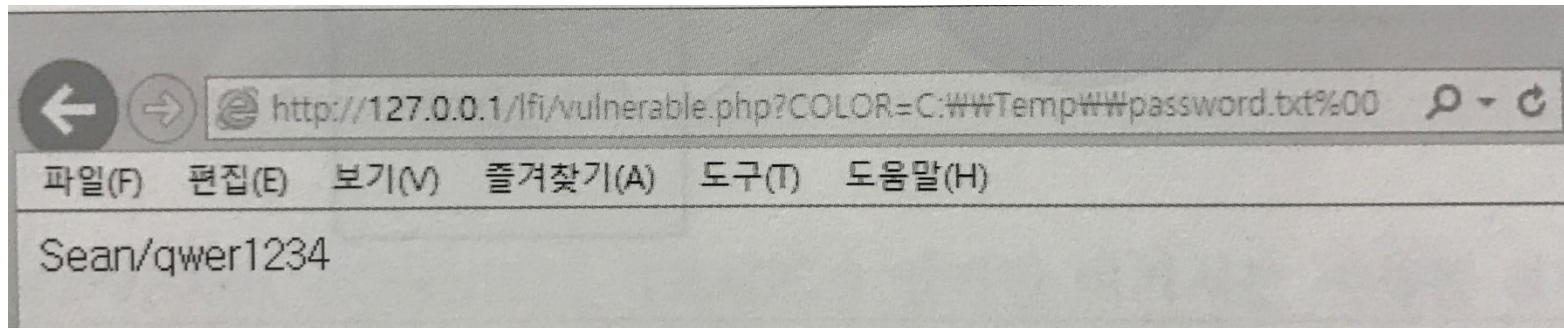
C:\Temp\password.txt

password.txt - 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

Sean/qwer1234

http://127.0.0.1/lfi/2/vulnerable.php?COLOR=C:\Temp\password.txt%00



← → ↻ ⓘ 127.0.0.1/lfi/2/vulnerable.php?COLOR=C:\Temp\password.txt%00

**Warning:** include(): Failed opening 'C:\Temp\password.txt' for inclusion (include\_path='.') in C:\AutoSet9wpublic\_html\lfi\2\vulnerable.php on line 4

## 2. 실습

원래 책에나오는 소스코드는 .php 가 있지만 저는 %00 이라는 시스템이 인식하는 null 이 되지 않아 생략했습니다.

이 공격은 성공하지 못했다. 이 방법은 윈도우에서 통하지 않는다!



Q & A