03. 외부 URL 파일 인클루드 비활성화

외부 URL 파일 인클루드 비활성화

항목설명

웹 서버에 파일을 참조하는 파라미터가 존재할 경우, 외부 URL을 입력한다면 *RFI(Shell 코드 및 악성코드를 실행) 취약점이 발생할 수 있다. 이러한 문제점을 해결하기 위해 PHP 옵션 중 allow_url_fopen 설정이 존재하는데, 해당 설정을 Off로 설정하여 외부 파일을 참조하지 못하도록 설정하는 것을 권고한다.

* RFI(Remote File Inclusion): 공격자가 입력한 URL을 서버가 참조하여 실행하는 취약점

진단 기준	✓ 양호	⊗ 취약
	allow_url_fopen이 Off로 설정된 경우	allow_url_fopen이 On으로 설정된 경우

설명

개발언어는 보통 다른 파일들을 불러와 사용할 수 있다. 파이썬의 **import** 혹은 **php**의 **include** 등등 ...

외부에서 만들어 놓은 **php** 파일을 **URL**에 삽입하였을때 별다른 제한 없이 실행이 될 경우 치명적인 공격이 가능하기 때문에

해당 설정을 **Off** 로 바꿔주어야한다.

딴소리

관련된 취약점으로는 **LFI** 와 **RFI** 가 있다. (현재 취약점의 경우 **RFI** 가 해당)

LFI = Local File Inclusion

RFI = Remote File Inclusion

LFI, RFI 의 차이는 **Local, Remote** 그러니까 로컬에 있는 파일을 불러올지 **,** 외부 파일을 불러올지의 차이라고 볼 수 있겠다 **.**

RFI의 경우 외부 공격자 서버의 **php** 파일 **, ex. 'http://attacker.com/attack.php"** 를 피해자 **URL** 파라미터에 삽입하여 실행을 시키도록 한다는건데

뭔가 시연해보고 싶으니까 별도로 서버를 구현해봐야겠다 **.**

> 기본 값

```
;;;;;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;;;;;

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

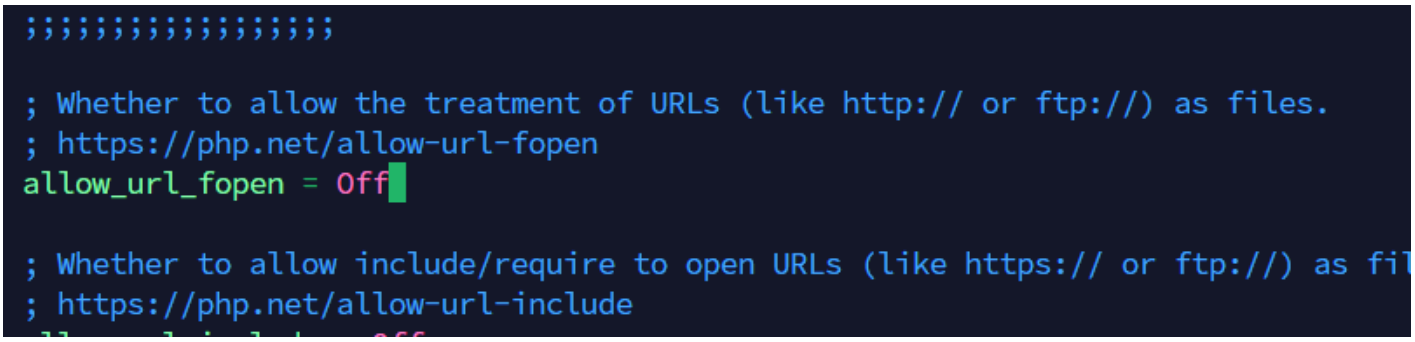
기본 값으로는 활성화가 되어 있음 **->** 취약

> 조치 방법

01. php config 파일로 접근

```
root@bookstack:/etc/php/8.3/cli# pwd
/etc/php/8.3/cli
root@bookstack:/etc/php/8.3/cli# ls -la
total 84
drwxr-xr-x 3 root root  4096 Aug 30 04:31 .
drwxr-xr-x 5 root root  4096 Aug 26 09:47 ..
drwxr-xr-x 2 root root  4096 Aug 26 09:48 conf.d
-rw-r--r-- 1 root root 73715 Aug 29 14:08 php.ini
root@bookstack:/etc/php/8.3/cli#
```

02. allow_url_fopen 을 검색 후 **Off** 로 수정



Revision #5
Created 2025-08-30 12:57:29 UTC by minwoo
Updated 2025-09-02 12:02:39 UTC by minwoo