



KISA 2024 2024 2024 2024

- [01. 2024 2024 2024 \[2024\]](#)
- [02. 2024 2024 2024 2024](#)
- [03. 2024 URL 2024 2024 2024](#)
- [04. 2024 2024 2024 2024](#)
- [05. PHP 2024 2024 2024](#)
- [06. 2024 2024 2024 2024 \[2024\]](#)

01.

항목설명

소스 코드, 예외 처리, 시스템 콜, API 함수 호출 등 오류가 발생한 경우 실행 환경, 개발 정보, 사용자 관련 데이터에 대한 민감한 정보를 포함하는 오류 메시지가 노출될 수 있다. PHP는 `display_errors` 설정이 Off로 설정된 경우 오류 메시지가 웹 페이지에 노출되지 않는다.

진단
기준

양호

display_errors 항목이 Off로 설정된 경우



취약

display_errors 항목이 On으로 설정된 경우

























display_errors = Off -> ☐

Notice: Undefined index: fr_date in /var/www/html/adm/excel_download.php on line 10

Notice: Undefined index: to_date in /var/www/html/adm/excel_download.php on line 16

Notice: Undefined index: sch_field in /var/www/html/adm/excel_download.php on line 30

Notice: Undefined index: sch_name in /var/www/html/adm/excel_download.php on line 35

Notice: Undefined index: cnt in /var/www/html/adm/excel_download.php on line 55

01. PHP conf file -> php.ini

02. display_errors = Off

01. PHP conf file -> php.ini

```
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 29 14:08 .
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. display_errors = Off

```
; Possible Values:
```

```
; Off = Do not display any errors  
; stderr = Display errors to STDERR (affects only CGI/CLI binaries!)  
; On or stdout = Display errors to STDOUT  
; Default Value: On  
; Development Value: On  
; Production Value: Off  
; https://php.net/display-errors
```

```
display_errors = Off
```

```
; The display of errors which occur during PHP's startup sequence are handled  
; separately from display_errors. We strongly recommend you set this to 'off'  
; for production servers to avoid leaking configuration details.  
; Default Value: On  
; Development Value: On
```

02. □□□□ □□ □□ □□

불필요한 헤더 정보 노출

항목설명

HTTP 프로토콜을 이용할 경우 간혹 HTTP 헤더에 PHP 정보가 노출되어 공격자에게 정보를 제공한다. 공격자는 노출된 헤더 정보(운영체제, 웹 서버, PHP 버전 등)를 이용하여 추가 공격을 진행할 수 있으므로, PHP 옵션 중 `expose_php`를 Off로 설정하여 HTTP 헤더에 정보가 노출되지 않도록 설정해야 한다.



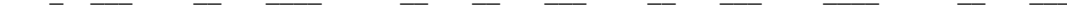
양호

expose_php가 Off로 설정된 경우



취약

expose_php가 On으로 설정된 경우



php 8.3, nginx 1.27 **EOS**

EOS

```
; Miscellaneous ;  
;;;;;;;;;;;;;  
  
; Decides whether PHP may expose the fact that it is installed on the server  
; (e.g. by adding its signature to the Web server header). It is no security  
; threat in any way, but it makes it possible to determine whether you use PHP  
; on your server or not.  
; https://php.net/expose-php  
expose_php = On
```

☐ ☐ ☐ ☐ **expose_php = On ->** ☐

*

ExploitDB [] [][][] [][][] [][][][] [][] [][][][] [][][] [].

□□ □□ □□□□ □□□ □□ **exploit**□ □□□ □□□ □□□ □□□ □□□ □□□ □□

EXPLOIT DATABASE							
☐ Verified ☐ Has App		Filters Reset All					
Show	15	Search: nginx					
Date	D	A	V	Title	Type	Platform	Author
2025-06-20				Ingress-NGINX 4.11.0 - Remote Code Execution (RCE)	Remote	Multiple	Likhith Appalaneni
2022-07-11				Nginx 1.20.0 - Denial of Service (DOS)	Remote	Multiple	Mohammed Alshehri
2019-10-28				PHP-FPM + Nginx - Remote Code Execution	WebApps	PHP	Emil Lerner
2016-11-16				Nginx (Debian Based Distros + Gentoo) - 'logrotate' Local Privilege Escalation	Local	Linux	Dawid Golunski
2013-11-19				Nginx 1.1.17 - URI Processing SecURity Bypass	Remote	Multiple	Ivan Fratric
2010-01-11				Nginx 0.7.64 - Terminal Escape Sequence in Logs Command Injection	Remote	Multiple	evilaliv3
2014-03-15				Nginx 1.4.0 (Generic Linux x64) - Remote Overflow	Remote	Linux_x86-64	sorbo
2013-07-11				Nginx 1.3.9/1.4.0 (x86) - Brute Force	Remote	Linux_x86	kingcope
2013-05-28				Nginx 1.3.9 < 1.4.0 - Chunked Encoding Stack Buffer Overflow (Metasploit)	Remote	Linux	Metasploit
2013-05-17				Nginx 1.3.9 < 1.4.0 - Denial of Service (PoC)	DoS	Linux	Mert SARICA
2013-04-19				Nginx 0.6.x - Arbitrary Code Execution NullByte Injection	WebApps	Multiple	Neal Poole




01. php ☐ ☐ ☐

```
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 29 15:05 .
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. expose_php ☐ Off ☐ ☐

```
; Decides whether PHP may expose the fact that it is installed on the server
; (e.g. by adding its signature to the Web server header). It is no security
; threat in any way, but it makes it possible to determine whether you use PHP
; on your server or not.
; https://php.net/expose-php
expose_php = Off
```

03. URL

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

allow_url_fopen이 Off로 설정된 경우

취약

allow_url_fopen이 On으로 설정된 경우

... import php include

php URL php

Off

LFI RFI (RFI)

LFI = Local File Inclusion

RFI = Remote File Inclusion


```
;;;;;;;;;
```

```
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
```

```
; https://php.net/allow-url-fopen
```

```
allow_url_fopen = Off
```

```
; Whether to allow include/require to open URLs (like https:// or ftp://) as files.
```

```
; https://php.net/allow-url-include
```

```
allow_url_include = Off
```

04. ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

불필요한 명령어 사용 제한

항목설명

PHP 페이지 중 명령어를 입력할 수 있는 페이지 또는 악성 스크립트 파일이 실행(Web Shell, 악성코드 등)될 경우 시스템 권한을 획득할 수 있다. 이러한 문제점을 해결하기 위해 PHP 옵션 중 `disable_functions` 항목으로 명령어를 제어하여 시스템의 피해를 최소화할 수 있다.

진단
기준

 양호

disable_functions에 설정(불필요한 함수)이 존재할 경우

✕ **취약**

disable_functions에 설정이 존재하지 않을 경우



Command injection




CTF


.

111

Diagram illustrating a neural network structure with 10 layers. The layers are represented by rectangles of varying widths, indicating different numbers of nodes. The layers are connected sequentially, with the final layer labeled "hidden".

```

; This directive allows you to disable certain functions.
; It receives a comma-delimited list of function names.
; https://php.net/disable-functions
disable_functions =

; This directive allows you to disable certain classes.
; It receives a comma-delimited list of class names.
; https://php.net/disable-classes

```

`disable_functions` 选项 在 `php.ini` 文件中 -> 选项

选项 选项

01. php config 选项 选项

```

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

```

选项 选项 选项 选项 选项 `php` 选项 `disable_functions` 选项 选项

* 选项 选项 选项 选项 选项 选项 选项 选项 选项 , 选项 选项 选项 选项 选项 选项 .

```

; This directive allows you to disable certain functions.
; It receives a comma-delimited list of function names.
; https://php.net/disable-functions
disable_functions = exec, system, shell_exec, passthru, phpinfo, show_source, popen, parse_ini_file

; This directive allows you to disable certain classes.
; It receives a comma-delimited list of class names.
; https://php.net/disable-classes

```

※ 시스템에 영향을 주는 함수 예시

- exec - 외부 프로그램을 실행하는 함수로 셸 명령어 사용 가능
- system - 외부 프로그램을 실행하는 함수로 셸 명령어 사용 가능
- shell_exec - PHP 상에서 셸 명령어에 대한 결과값을 웹상에 출력하게 하는 함수
- passthru - 외부 프로그램을 실행하고 실행되는 동안 화면을 실시간으로 출력하는 함수
- phpinfo - PHP 정보(OS 및 PHP 정보 등)를 보여주는 함수
- show_source - 소스 코드를 출력하는 함수
- popen - 파일을 실행하고 그 결과값을 반환하는 함수
- parse_ini_file - php 설정 파일을 배열에 저장하는 함수

05. PHP

PHP 실행 경로 제한

항목설명

파일 업로드, 파일 다운로드 및 파일 경로를 참조 페이지가 존재할 경우, 웹 루트 상위 폴더를 벗어나 시스템 파일을 참조할 수 있는 문제점이 발생(예) /etc/shadow, %WINNT%system32/config/SAM)한다. 웹 서버의 피해를 최소화하기 위해 PHP 옵션 open_basedir 경로를 지정하여 지정된 경로의 상위 폴더 접근을 제한할 수 있다.

진단
기준



양호

open_basedir에 경로를 지정한 경우



취약

open_basedir에 경로가 지정되어 있지 않은 경우

path traversal .

http://localhost/home.html ,

.

apache**home.html** ()

/var/www/html/home.html

.

html**(root)**

../../../../ .

ex. http://localhost../../../../../../../../etc/passwd

* ; ; ; ; ; ;

;

```
; open_basedir, if set, limits all file operations to the defined directory
; and below. This directive makes most sense if used in a per-directory
; or per-virtualhost web server configuration file.
; Note: disables the realpath cache
; https://php.net/open-basedir
open_basedir =

; This directive allows you to disable certain functions.
; It receives a comma-delimited list of function names.
; https://php.net/disable-functions
```

open_basedir ; ; -> ;

;

; ; ; ; ; ;

진단 방법

■ PHP 설정 파일 조회

1) # cat /[PHP 설치 디렉터리]/php.ini | grep open_basedir

```
root@ubuntu:/etc/php/8.1/cli# cat /etc/php/8.1/cli/php.ini | grep open_basedir
; open_basedir, if set, limits all file operations to the defined directory
; open_basedir =
; Note: if open_basedir is set, the cache is disabled
root@ubuntu:/etc/php/8.1/cli#
```

조치 방법

■ PHP 설정 파일에서 수정

1) # vi /[PHP 설치 디렉터리]/php.ini

```
; open_basedir, if set, limits all file operations to the defined directory
; and below. This directive makes most sense if used in a per-directory
; or per-virtualhost web server configuration file.
; Note: disables the realpath cache
; https://php.net/open-basedir
open_basedir = /var/www:/tmp
```

php config ; ;

2024 ; ; ; ; .

01. php Config 01 02

```
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 05:14 .
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. 01 02 03 04 05 06 07 08

```
; and below. This directive makes most sense if used in a per-directory
; or per-virtualhost web server configuration file.
; Note: disables the realpath cache
; https://php.net/open-basedir
open_basedir = /var/www

; This directive allows you to disable certain functions.
; It receives a comma-delimited list of function names.
; https://php.net/disable-functions
```

* 01 02 03 04 05 06 07 08 ,

ex. /var/www:/tmp -> /var/www 01 /tmp 02

PHP

LANG

📅 Last updated on 29 August 2025 🚗

 **PHP:** Hypertext Preprocessor (or simply PHP) is a general-purpose programming language originally designed for web development.

Release	Released	Active Support	Security Support	Latest
8.4	9 months ago (21 Nov 2024)	Ends in 1 year and 4 months (31 Dec 2026)	Ends in 3 years (31 Dec 2028)	8.4.12 (28 Aug 2025)
8.3	1 year and 9 months ago (23 Nov 2023)	Ends in 4 months (31 Dec 2025)	Ends in 2 years and 4 months (31 Dec 2027)	8.3.25 (28 Aug 2025)
8.2	2 years and 8 months ago (08 Dec 2022)	Ended 8 months ago (31 Dec 2024)	Ends in 1 year and 4 months (31 Dec 2026)	8.2.29 (03 Jul 2025)
8.1	3 years and 9 months ago (25 Nov 2021)	Ended 1 year and 9 months ago (25 Nov 2023)	Ends in 4 months (31 Dec 2025)	8.1.33 (03 Jul 2025)
8.0	4 years and 9 months ago (26 Nov 2020)	Ended 2 years and 9 months ago (26 Nov 2022)	Ended 1 year and 9 months ago (26 Nov 2023)	8.0.30 (03 Aug 2023)

Show more unmaintained releases

00 00 00 000 **Security Support** 000 0000 00 .

000 0000 0000 00 0000 00000 ,

000 000 000 000 00 000 00000 00 0000 0000 00 000 000 0
000 00 .

