PHP open_basedir Tweak

For cPanel & WHM version 64

(*Home >> Security Center >> PHP open_basedir Tweak*)

Overview

The `open_basedir` tweak limits the user's ability to browse the file system with PHP. It prevents PHP's access to the user's home directory, the `/tmp` directory, and some necessary PHP system directories. This helps to protect your system from unauthorized access through PHP.

Note:

This security tweak modifies the Apache configuration file, regardless of the PHP handler that you select.

- Apache only uses configuration file PHP directives if you select the DSO handler.
- If you configure PHP to run as a CGI, suPHP, or FastCGI process, you **must** manually specify the `open_basedir` directive in the appropriate `php.ini` file. Each user **requires** their own `php.ini` files when you select a PHP handler that is not DSO.

Enable the open_basedir tweak

To enable the `open_basedir` tweak, perform the following steps:

1. Select the *Enable php open_basedir Protection* checkbox.
2. Select the checkboxes that correspond to the domains that you wish to exclude.
3. Click *Save*.

open_basedir directives

When you enable the `open_basedir` tweak, the system adds PHP directives to each Virtual Host in the `httpd.conf` file.

These directives limit users' PHP access to the following directories:

```
/usr/lib/php
/usr/local/lib/php
/tmp
```

Additional documentation

- PHP open_basedir Tweak
- Apache mod_userdir Tweak
- PHP FAQ
- SSL Storage Manager
- ModSecurity Vendors