SecuringPHP

⚠️ THIS IS A SCRATCHPAD DOCUMENT, PLEASE CONSIDER THIS WHEN READING ON 💡

Securing a Multi-site PHP setup

This is a working title.

Due to many requests of this kind #apache, I decided that repeating myself is getting boring, so I will start writing down my approach to this, and I invite anybody who has experience in this field to extend this wiki page.

open_basedir

Prerequisites

To seperate the single PHP sites I host, I use PHP's open_basedir directive.

Due to the fact, that this directive is NOT respected by all functions, be it a design flaw, an exploit or third party libraries that simply ignore this setting, I recommend installing the Suhosin Extension, which in the past has proven to be capable of holding against such flaws.

As always it pays to consider well the directory structure of your sites. The structure I have chose looks as follows:

```
/srv/web/domain.tld/
/srv/web/domain.tld/htdocs/
/srv/web/domain.tld/tmp/
/srv/web/domain.tld/sessions/
/srv/web/sub.domain.tld/
/srv/web/sub.domain.tld/htdocs/
/srv/web/sub.domain.tld/tmp/
/srv/web/sub.domain.tld/sessions/
/srv/web/otherdomain.tld/
/srv/web/otherdomain.tld/htdocs/
/srv/web/otherdomain.tld/tmp/
/srv/web/otherdomain.tld/sessions/
```

/srv/web being the base of my installation, I chose to put every domain and every subdomain of those domains in it's own directory. Please note that this is a simple setup, serving as an idea an example – not a reference installation.

/srv/web/domain.tld/htdocs will be our DocumentRoot, *tmp* and *sessions* will be configured per vhost as directories for temporary uploads and sessions.

Now let's have look at our config!

Example Configuration

```
<VirtualHost *:80>
        ServerAdmin admin@domain.tld

        DocumentRoot /srv/web/domain.tld/htdocs
        ServerName domain.tld

        php_admin_value open_basedir /srv/web/domain.tld/:/usr/share/pear/
        php_admin_value upload_tmp_dir /srv/web/domain.tld/
        php_admin_value session.safe_path /srv/web/domain.tld/sessions/

        <Directory /srv/web/domain.tld/htdocs>
                php_admin_flag engine on
                AllowOverride AuthConfig FileInfo
                Order allow,deny
                allow from all
        </Directory>
</VirtualHost>
```

Explanation

What is happening in this configuration?

First of all we set our *htdocs* as the *DocumentRoot*, set the ServerName and then we allow PHP to access this domain's basedirectory.

The reason for this is that we need need to access *tmp* and *sessions*. I have experienced that copy/move and other functions related to upload from *tmp* to *htdocs* will FAIL if you just specify a path in the style of */foo/bar:/baz*. But the workaround shown here has two advantages: First of all: It works. And secondly, even more importantly it gives an additional security-margin of a separation-of-concerns on a vhost-base!

Also note that *open_basedir* has a special feature, that searches for files or directories starting with *bar* if you specify a path of */foo/bar* – with no trailing slash.

This piece of information is important if you host a wiki for instance, which uses diff or diff3, you will have to supply it in the open_basedir string.

Eventually, in the Directory block, we allow PHP to be executed, via *php_admin_flag engine on*, because by default I have PHP disabled via *egnine off* in */etc/php.ini*.

I also allow the overriding of AuthConfig and that of FileInfo. Note that allowing to override FileInfo is dangerous, as it allows a number of settings to be overridden, some of which could affect your PHP installation as well, but it also allows the use of mod_rewrite.

Limitation

xxx