SSH

Secure Wordpress Installations Server-wide (cPanel/WHM)

On a Server where You're not using cageFS and proper configurations a user may be able to access the files owned by other users.

It has been known that whenever some hacker/intruder gets access to one account on cPanel Server, he tries to gain access to all sites hosted on the server. Most common method is to scan the CMS configuration files which are present on the server. For example hacker scans the wp-config.php files and symlinks these files to view the db information.

This can be avoided to keep the permissions of config files so that other linux users are not able to access it.

Here is the command which will scan all wp-config.php files on server and changes permissions to 0600.

```
find /home/*/public_html -name "wp-config.php" -type f -exec chmod -v 0600 {} \;
```

Change Default PHP-FPM settings on cPanel/WHM Server

1. Create the file /var/cpanel/ApachePHPFPM/system_pool_defaults.yaml
2. Add you custom settings

   ```
   php_admin_value_error_reporting : E_ALL & ~E_NOTICE & ~E_DEPRECATED & ~E_STRICT
   php_admin_value_disable_functions : show_source,system,exec,shell_exec,passthru,popen
   pm_max_children : 3
   pm_max_requests : 10
   pm_min_spare_servers : 5
   pm_max_spare_servers : 15
   pm_process_idle_timeout : 10
   ```

3. Remove existing config files using following command

   ```
   rm -rf /var/cpanel/userdata/*/*.php-fpm.yaml
   ```

4. Rebuild New config files using following command

   ```
   /scripts/php_fpm_config --rebuild
   ```

5. You may need to enable the php-fpm for the sites from whm again.