Akeeba Kickstart – Insecure setup detected

Akeeba Kickstart has detected that its file name is `kickstart.php` which can be easily guessed, and you are not using a password to protect access to it.

You have two options to fix this problem.

Option 1. Use a password (recommended)

Create a file named `kickstart.json.php` in the same directory as Kickstart. Put the following contents into that file:

```
<?php die(); ?>
{
        "password": "$2y$10$[illegible]"
}
```

Then, reload this page. You will be asked for a password. Enter `Akeeba123` and click the button to unlock Kickstart.

Option 2. Rename this file (legacy method; discouraged)

Please change the file name to something which does not include any of the following terms:

- `kickstart`
- `ks`
- `akeeba`

It is best to use a completely random filename. For example, you can rename this file to `j2d6aydkjwc2ffw.php`. Then you can access this file by replacing `kickstart.php` with the new name in the address bar of your browser.

If your site has a `.htaccess` or `web.config` file please remember to rename, or remove it to avoid it blocking access to your (renamed) Kickstart file. If you are using the NginX web server, please note that your server configuration may be blocking access to your (renamed) Kickstart file; in this case, you will need to edit your site's configuration.

Why do you need to do that?

Due to its nature, Akeeba Kickstart will execute commands sent to it by anybody accessing it. If Kickstart on your site has a well-known or easy-to-guess name, it is easy for an attacker to restart and hijack your restoration session. If you are using neither a password-protected JPS archive, nor a password-protected installer, the attacker can override your administrator / super user password with their own and take over your site. This is especially true if you forget to click on the Clean Up button at the end of the restoration, leaving Kickstart and your backup archive behind.

Using a strong password to protect access to Kickstart makes abusing Kickstart impractical for an attacker. Using a completely arbitrary filename for Kickstart makes it much harder for the attacker to guess which URL they need to visit to access Kickstart, mitigating this risk.