# securizar instalación PHP

- desactivar URL remota para inclusión de ficheros:

```
allow_url_fopen = Off
```

- registro de variables globales:

```
register_globals = Off
```

- restringir donde puede leer/escribir PHP:

```
open_basedir = /home/cfproyectos
```

- modo seguro:

```
safe_mode = Off
```

  - el acceso a ficheros no OWNED por apache no es posible
  - sin acceso a variables de entorno ni ejecución de binarios
  - ```
    safe_mode_gid = On
    ```
  - permite acceso a ficheros donde el GROUP OWNED sea apache
  - ```
    safe_mode_exec_dir = /home/cfproyectos/binarios
    ```
  - permite en modo seguro la ejecución de binarios dentro del directorio especificado (o symlinks)
  - ```
    safe_mode_alloweb_env_vars = PHP_
    ```
  - permite en modo seguro el acceso a ciertas variables de entorno
- Límites:
  - tiempo de ejecución máxima del script:

    ```
    max_execution_time = 30
    ```
  - tiempo máximo utilizado en parsear entrada:

    ```
    max_input_time = 60
    ```
  - memoria máxima usada por un script:

    ```
    memory_limit = 16M
    ```
  - tamaño de fichero máximo que se puede subir:

    ```
    upload_max_filesize = 2M
    ```
  - tamaño máximo de variables POST:

    ```
    post_max_size = 8M
    ```
- Limitar el acceso a ciertos nombres de archivos:

```
<filesmatch>
    Order allow,deny
    Deny from all
```
```

```
</filesmatch>
```

    - evitar acceso a ficheros que no se parsean por «norma» y que pueden contener información sensible: .inc .sql .mysql
    - evitar acceso a ficheros de backup del sistema: ~
- Mensajes de error y log:

```
display_errors = Off
log_errors = On
```

    - desactivar el volcado en pantalla
- ocultar la presencia de PHP:

```
expose_php = Off
```

    - en la cabecera HTTP
    - en la firma de apache
    - en la dirección: http://www.ejemplo.coms/script.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000