配置完全需要重启php-fpm才能生效

php.ini 配置可能会被 php-fpm 覆盖掉，也可能会被具体执行的php脚本覆盖掉。

优先级别由低至高如下，php.ini < php-fpm.conf < \*.php

(1) 控制php脚本能访问的目录  
　　使用open\_basedir选项能够控制PHP脚本只能访问指定的目录，这样能够避免PHP脚本访问  
　　不应该访问的文件，一定程度上限制了phpshell的危害，我们一般可以设置为只能访问网站目录：  
　　open\_basedir = /usr/local/nginx/html

(2) 打开magic\_quotes\_gpc来防止SQL注入  
　　SQL注入是非常危险的问题，小则网站后台被入侵，重则整个服务器沦陷，  
　　所以一定要小心。php.ini中有一个设置：  
　　magic\_quotes\_gpc = Off  
这个默认是关闭的，如果它打开后将自动把用户提交对sql的查询进行转换，  
　　比如把 ' 转为 \'等，这对防止sql注射有重大作用。所以我们推荐设置为：  
　　magic\_quotes\_gpc = On

(3) 错误信息控制  
　　 log\_errors = On  开启日志

error\_reporting = E\_ALL & ~E\_DEPRECATED & ~E\_STRICT 错误级别  
　 display\_errors = Off    关闭暴露日志信息

log\_errors\_max\_len = 1024 日志文件可存储大小

error\_log = /usr/local/php\_errors.log 日志地址

(4) 设置PHP的扩展库路径【可不配 有默认路径】

extension\_dir=""  
(5) 设置PHP的mysql动态库  
 extension=mysqli.so extension=pdo\_mysql.so  
(6) 设置PHP的时区  
 date.timezone = PRC  
(7) 开启opcache

zend\_extension = opcache

opcache.enable=1

opcache.enable\_cli=1

opcache.memory\_consumption=128

opcache.max\_accelerated\_files=2000

（8）设置PHP脚本允许访问的目录（需要根据实际情况配置）  
 open\_basedir = /usr/share/nginx/html;  
（9）会话安全  
 [session.use\_only\_cookies](https://www.php.net/manual/zh/session.configuration.php#ini.session.use-only-cookies)=1 【只使用 cookie 来记录会话 ID】

[session.use\_strict\_mode](https://www.php.net/manual/zh/session.configuration.php#ini.session.use-strict-mode)=1 【启用 session.use\_strict\_mode 是必不可少】