# linux的apache2.4限定某个目录禁止解析PHP及user\_agent与PHP相关配置

**限定某个目录禁止解析PHP**

对于使用PHP语言编写的网站，有一些目录是有需求上传文件的，比如服务器可以上传图片，并且没有做防盗链，所以就会被人家当成了一个图片存储服务器，并且盗用带宽流量。如果网站代码有漏洞，让黑客上传了一个用PHP代码写的木马，由于网站可以执行PHP程序，最终会让黑客拿到服务器权限，为了避免这种情况发生，我们需要把能上传文件的目录直接禁止解析PHP代码（不用担心会影响网站访问，若这种目录也需要解析PHP，那说明程序员不合格）

**1. 修改虚拟主机配置文件**

[root@gary-tao ~]*# vim /usr/local/apache2.4/conf/extra/httpd-vhosts.conf*

核心配置文件内容:

<Directory /data/wwwroot/111.com/upload>

php\_admin\_flag engine off //这一段就可以禁止解析PHP代码

<FilesMatch (.\*)\.php(.\*)> //这一段就是让php的文件访问受到限制，防止php文件的源代码被查看

Order allow,deny

Deny **from** all

</FilesMatch>

</Directory>

[root@gary-tao 111.com]*# /usr/local/apache2.4/bin/apachectl -t*

Syntax OK //测试语法

[root@gary-tao 111.com]*# /usr/local/apache2.4/bin/apachectl graceful //加载配置*

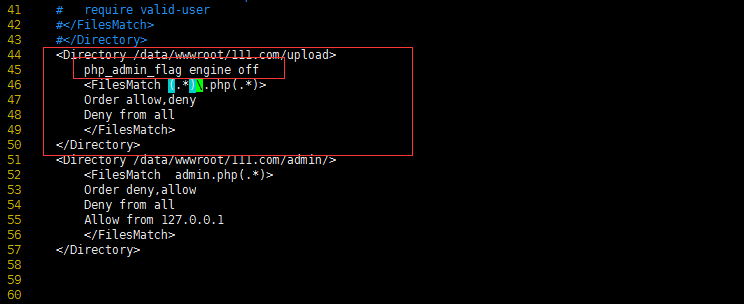
[root@gary-tao 111.com]*# mkdir upload //创建一个upload目录*

[root@gary-tao 111.com]*# ls*

123.php admin index.php qq.png upload

[root@gary-tao 111.com]*# cp 123.php upload/*

**修改后示例图**



**2. 使用curl测试时返回403**

[root@gary-tao 111.com]*# curl -x172.16.111.100:80 'http://111.com/upload/123.php' -I //直接不给访问权限*

HTTP/1.1 403 Forbidden

**Date: Tue, 26 Dec 2017 06:19:17 GMT**

**Server: Apache/2.4.29 (Unix) PHP/7.1.6**

**Content-Type: text/html; charset=iso-8859-1**

测试需要把下面配置先禁止掉：

<FilesMatch (.\*)\.php(.\*)>

Order allow,deny

Deny **from** all

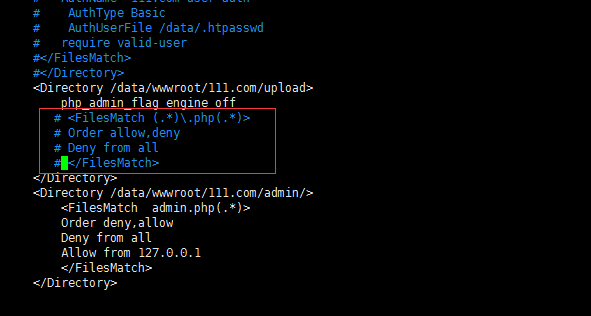
</FilesMatch>

[root@gary-tao 111.com]*# /usr/local/apache2.4/bin/apachectl -t*

Syntax OK

[root@gary-tao 111.com]*# /usr/local/apache2.4/bin/apachectl graceful*

**修改后示例图：**



禁止掉后使用curl后的测试结果：

[root@gary-tao 111.com]# curl -x127.0.0.1:80 'http://111.com/upload/123.php' //下例信息说明123.php不能正常解析

**<?php**

**echo** "123.php";

**?>**

**限制user\_agent**

user\_agent可以理解为浏览器标识，针对user\_agent来限制一些访问，比如可以限制一些不太友好的搜索引擎“爬虫”，你之所以能在百度搜到一些论坛，就是因为百度会派一些“蜘蛛爬虫”过来抓取网站数据。“蜘蛛爬虫”抓取数据类似于用户用浏览器访问网站，当“蜘蛛爬虫”太多或者访问太频繁，就会浪费服务器资源。另外，也可以限制恶意请求，这种恶意请求我们通常称作cc攻击，他的原理很简单，就是用很多用户的电脑同时访问同一个站点，当访问量或者频率达到一定层次，会耗尽服务器资源，从而使之不能正常提供服务。这种cc攻击其实有很明显的规律，其中这些恶意请求的user\_agent相同或者相似，那我们就可以通过限制user\_agent发挥防攻击的作用。

**1. 针对user\_agent来做访问限制的核心配置文件内容**

[root@gary-tao 111.com]*# vim /usr/local/apache2.4/conf/extra/httpd-vhosts.conf*

核心配置文件内容

<IfModule mod\_rewrite.c>

RewriteEngine on

RewriteCond %{HTTP\_USER\_AGENT} .\*curl.\* [NC,OR] //OR是或者的意思，user\_agent匹配curl或者匹配baidu.com

RewriteCond %{HTTP\_USER\_AGENT} .\*baidu.com.\* [NC] //NC是忽略大小写

RewriteRule .\* - [F] //F是Forbidden

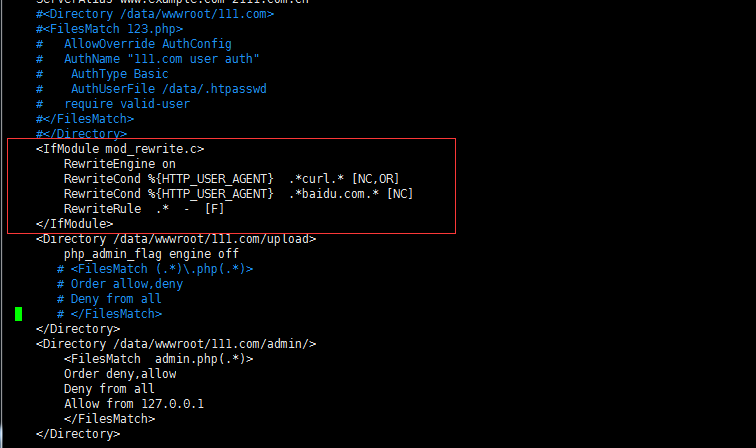
</IfModule>

[root@gary-tao 111.com]*# /usr/local/apache2.4/bin/apachectl -t*

Syntax OK

[root@gary-tao 111.com]*# /usr/local/apache2.4/bin/apachectl graceful*

**修改配置示例如下图：**



**2.使用curl测试如下：**

[root@gary-tao 111.com]# curl -x127.0.0.1:80 'http://111.com/upload/123.php'

**<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">**

<html><head>

<title>403 Forbidden</title>

</head><body>

<h1>Forbidden</h1>

<p>You don't have permission to access /upload/123.php

on this server.<br />

</p>

</body></html>

[root@gary-tao 111.com]# curl -x127.0.0.1:80 'http://111.com/upload/123.php' -I

HTTP/1.1 403 Forbidden

Date: Tue, 26 Dec 2017 07:03:42 GMT

Server: Apache/2.4.29 (Unix) PHP/7.1.6

Content-Type: text/html; charset=iso-8859-1

**3.指定user\_agent，如果不指定user\_agent，那么curl作为user\_agent会被限制访问，从上面测试可以看出。**

示例如下：

[root@gary-tao 111.com]*# curl -A "xietao xietao" -x127.0.0.1:80 'http://111.com/upload/123.php' -I*

HTTP/1.1 200 OK

**Date: Tue, 26 Dec 2017 07:08:20 GMT**

**Server: Apache/2.4.29 (Unix) PHP/7.1.6**

**Last-Modified: Tue, 26 Dec 2017 06:16:53 GMT**

**ETag: "19-561383aa99f09"**

**Accept-Ranges: bytes**

**Content-Length: 25**

**Cache-Control: max-age=0**

**Expires: Tue, 26 Dec 2017 07:08:20 GMT**

**Content-Type: application/x-httpd-php**

[root@gary-tao 111.com]*# tail /usr/local/apache2.4/logs/111.com-access\_20171226.log //查看日志*

127.0.0.1 - - [26/Dec/2017:14:25:40 +0800] "HEAD http://111.com/upload/123.php HTTP/1.1" 200 - "-" "curl/7.29.0"

127.0.0.1 - - [26/Dec/2017:14:26:52 +0800] "GET http://111.com/upload/123.php HTTP/1.1" 200 25 "-" "curl/7.29.0"

172.16.111.1 - - [26/Dec/2017:14:29:07 +0800] "GET / HTTP/1.1" 200 12 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.221 Safari/537.36 SE 2.X MetaSr 1.0"

172.16.111.1 - - [26/Dec/2017:14:29:16 +0800] "GET /123.php HTTP/1.1" 200 7 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.221 Safari/537.36 SE 2.X MetaSr 1.0"

172.16.111.1 - - [26/Dec/2017:14:29:31 +0800] "GET /uploab/123.php HTTP/1.1" 404 212 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.221 Safari/537.36 SE 2.X MetaSr 1.0"

172.16.111.1 - - [26/Dec/2017:14:29:43 +0800] "GET /upload/123.php HTTP/1.1" 200 25 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.221 Safari/537.36 SE 2.X MetaSr 1.0"

172.16.111.1 - - [26/Dec/2017:14:29:44 +0800] "GET /upload/123.php HTTP/1.1" 200 25 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.221 Safari/537.36 SE 2.X MetaSr 1.0"

127.0.0.1 - - [26/Dec/2017:15:03:15 +0800] "GET http://111.com/upload/123.php HTTP/1.1" 403 223 "-" "curl/7.29.0"

127.0.0.1 - - [26/Dec/2017:15:03:42 +0800] "HEAD http://111.com/upload/123.php HTTP/1.1" 403 - "-" "curl/7.29.0"

127.0.0.1 - - [26/Dec/2017:15:08:20 +0800] "HEAD http://111.com/upload/123.php HTTP/1.1" 200 - "-" "xietao xietao"

**解释说明：**

常用配置选项：

使用参数 -A 指定了它的user\_agent后就可以访问。  
使用参数 -e 指定referer  
使用参数 -x 相对省略本地绑定hosts  
使用参数 -I 查看状态码

**php相关配置**

虽然PHP是以httpd一个模块的形式存在，但是PHP本身也有自己的配置文件。

**1. 查看PHP配置文件位置**

[root@gary-tao 111.com]*# ls*

123.php admin index.php qq.png upload

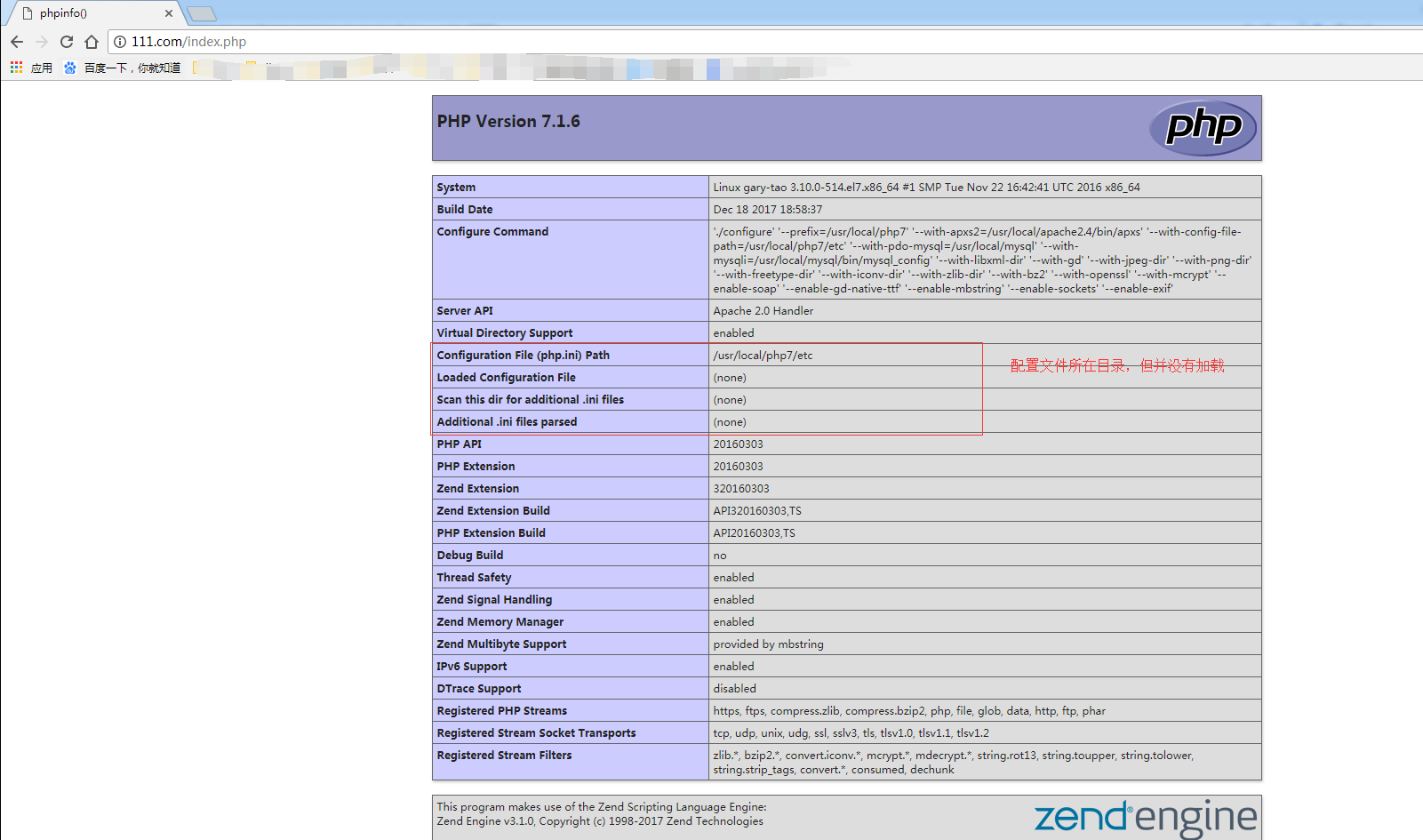
[root@gary-tao 111.com]*# vi index.php //编辑index文件，输入以下内容,保存退出。*

<?php

phpinfo();

**?>**

* 浏览器访问：<http://111.com/index.php>



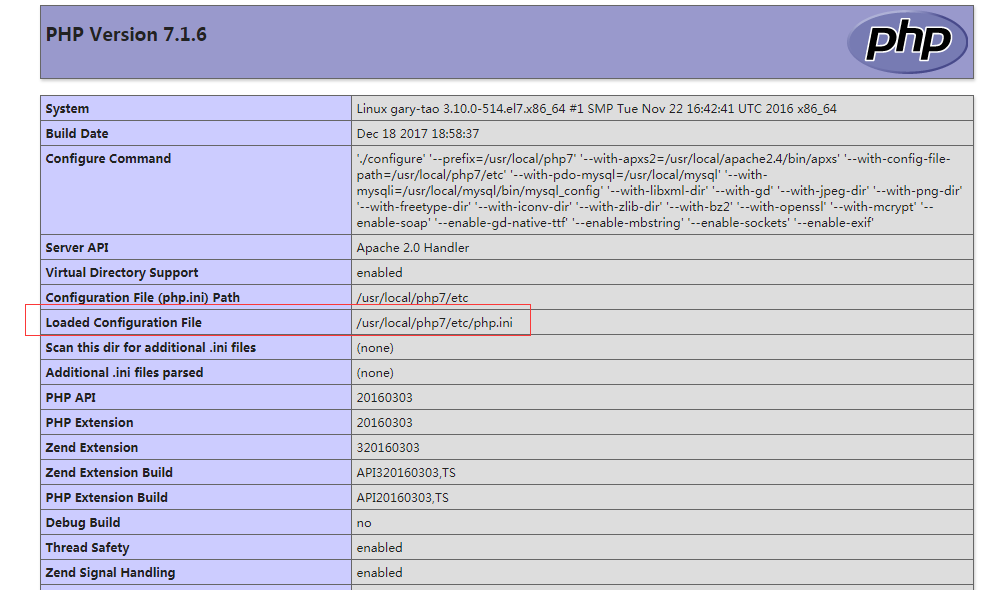
* 复制源码包里开发配置文件

[root@gary-tao 111.com]*# cd /usr/local/src/php-7.1.6*

[root@gary-tao php-7.1.6]*# cp php.ini-development /usr/local/php7/etc/php.ini*

[root@gary-tao php-7.1.6]*# /usr/local/apache2.4/bin/apachectl graceful //重新加载配置*

结果如下图：



**解释说明：**

php.ini为PHP的配置文件，可以看出其在/usr/local/php7/etc/php.ini。

**2.PHP的disable\_functions**

PHP有诸多的内置的函数，有一些函数（比如exec）会直接调取linux的系统命令，如果开放将会非常危险，因此，基于安全考虑应该把一些存在安全风险的函数禁掉。

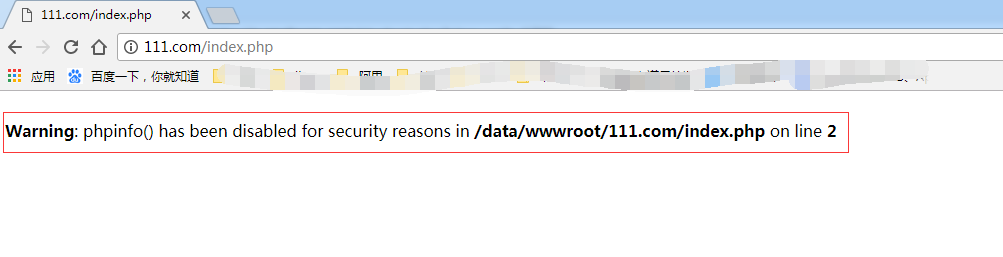
示例如下：

[root@gary-tao php-7.1.6]*# vim /usr/local/php7/etc/php.ini //搜索disable\_functions,编辑加上如下函数*

**eval**,assert,popen,passthru,escapeshellarg,escapeshellcmd,passthru,**exec**,**system**,**chroot**,scandir,chgrp,**chown**,escapeshellcmd,escapeshellarg,shell\_exec,proc\_get\_status,ini\_alter,ini\_restore,dl,pfsockopen,openlog,syslog,**readlink**,**symlink**,leak,popepassthru,stream\_socket\_server,popen,proc\_open,proc\_close，phpinfo

[root@gary-tao php-7.1.6]*# /usr/local/apache2.4/bin/apachectl graceful //重新加载配置*

**因为加上了phpinfo函数，所以访问index.php时结果如下：**



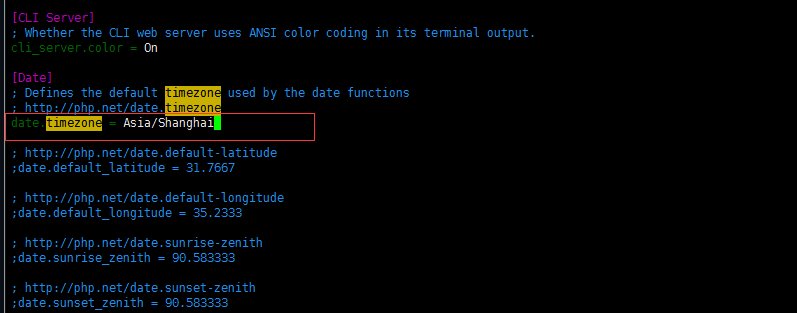
**3.定义date.timezone，如果不定义会导致有告警信息**

[root@gary-tao php-7.1.6]*# vim /usr/local/php7/etc/php.ini //找到date.timezone*

定义如下：

date.timezone = Asia/Shangahi(或Chongqing）

**示例图如下：**



**4. 配置 error\_log**

PHP的日志对于程序员来讲非常重要，它是排查问题的重要手段。

如果加上了phpinfo函数后，浏览器上访问http://111.com/index.php 就会有信息输出，这样也暴露的地址目录，相对来说也不安全，我们需要把报错信息也隐藏掉，操作如下：

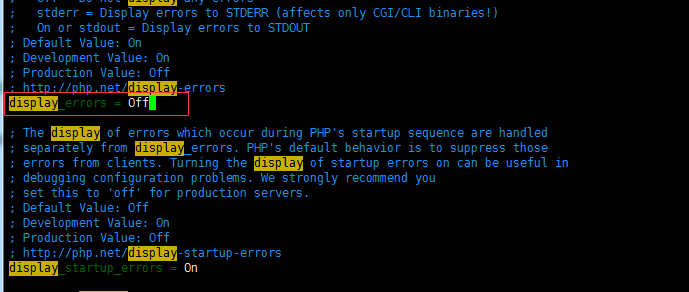
[root@gary-tao php-7.1.6]*# vim /usr/local/php7/etc/php.ini //搜索display\_errors*

定义如下：

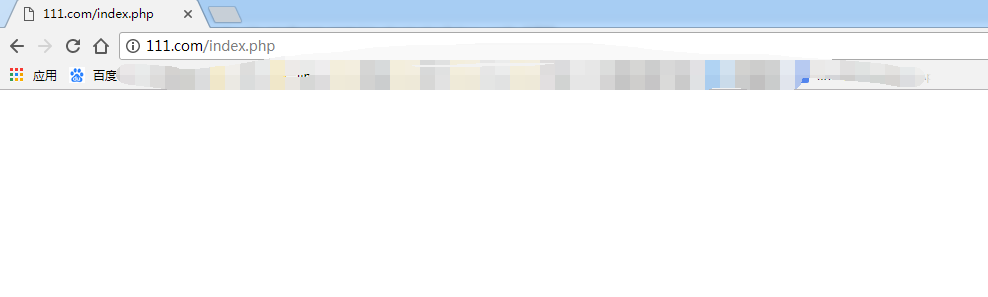
display\_errors = Off

[root@gary-tao php-7.1.6]*# /usr/local/apache2.4/bin/apachectl graceful*

**修改示意图**



**浏览访问结果如下：**



**使用curl测试如下：**

[root@gary-tao php-7.1.6]*# curl -A "xietao xietao" -x127.0.0.1:80 'http://111.com/index.php'*

[root@gary-tao php-7.1.6]*# curl -A "xietao xietao" -x127.0.0.1:80 'http://111.com/index.php' -I*

HTTP/1.1 200 OK

**Date: Tue, 26 Dec 2017 09:02:01 GMT**

**Server: Apache/2.4.29 (Unix) PHP/7.1.6**

**X-Powered-By: PHP/7.1.6**

**Cache-Control: max-age=0**

**Expires: Tue, 26 Dec 2017 09:02:01 GMT**

**Content-Type: text/html; charset=UTF-8**

**总结：配置了display\_errors = Off后，浏览器访问没有任何输出信息，一片空白，使用curl输出也是一样，这样我们就无法判断是否有问题，所以需要配置错误日志。**

修改配置日志示例如下：

[root@gary-tao php-7.1.6]*# vim /usr/local/php7/etc/php.ini*

定义如下：

//搜索log\_errors 改为 log\_errors =On

//搜索error\_log 改为 /tmp/php/php\_errors.log

//搜索error\_reporting 改为 error\_reporting = E\_ALL & ~E\_NOTICE

//搜索display\_errors 改为 display\_errors = Off

[root@gary-tao php-7.1.6]*# /usr/local/apache2.4/bin/apachectl -t*

Syntax OK

[root@gary-tao php-7.1.6]*# /usr/local/apache2.4/bin/apachectl graceful*

[root@gary-tao php-7.1.6]*# curl -A "xietao xietao" -x127.0.0.1:80 'http://111.com/index.php'*

[root@gary-tao php-7.1.6]*# ls /tmp/*

pear php\_errors.log systemd-private-c13d62a36c594e09a55010e8f304eb60-vmtoolsd.service-1qgl8W

[root@gary-tao php-7.1.6]*# ls -l /tmp/php\_errors.log*

-rw-r--r-- 1 daemon daemon 290 12月 26 17:13 /tmp/php\_errors.log

[root@gary-tao php-7.1.6]*# ps aux |grep httpd*

root 5358 0.0 1.4 260000 14804 ? Ss 12月19 0:37 /usr/local/apache2.4/bin/httpd -k graceful

daemon 14250 0.0 1.3 546828 13604 ? Sl 17:13 0:00 /usr/local/apache2.4/bin/httpd -k graceful

daemon 14251 0.0 1.1 546828 11580 ? Sl 17:13 0:00 /usr/local/apache2.4/bin/httpd -k graceful

daemon 14252 0.0 1.8 682124 18552 ? Sl 17:13 0:00 /usr/local/apache2.4/bin/httpd -k graceful

root 14340 0.0 0.0 112680 972 pts/0 S+ 17:15 0:00 grep --color=auto httpd

[root@gary-tao php-7.1.6]*# grep error\_log /usr/local/php7/etc/php.ini*

; server-specific log, STDERR, **or** a location specified **by** the error\_log

; Set maximum length **of** log\_errors. In error\_log information about the source **is**

error\_log = /tmp/php\_errors.log

;error\_log = syslog

; OPcache error\_log file name. Empty string assumes "stderr".

;opcache.error\_log=

[root@gary-tao php-7.1.6]*# touch /tmp/php\_errors.log ; chmod 777 /tmp/php\_errors.log //因为日志用户是daemon，日志是随着httpd的服务启动，为了保证PHP的错误日志所在目录存在，并且有权限为可写。*

[root@gary-tao php-7.1.6]*# cat /tmp/php\_errors.log*

[26-Dec-2017 17:13:35 Asia/Shanghai] PHP Warning: phpinfo() has been disabled **for** security reasons **in** /data/wwwroot/111.com/index.php on line 2

[26-Dec-2017 17:13:47 Asia/Shanghai] PHP Warning: phpinfo() has been disabled **for** security reasons **in** /data/wwwroot/111.com/index.php on line 2

**模拟一个错误演示：**

[root@gary-tao php-7.1.6]*# vim /data/wwwroot/111.com/2.php //编辑如下内容*

<?php

echo 1234.php;

adfadgagagag

[root@gary-tao php-7.1.6]*# curl -A "xietao xietao" -x127.0.0.1:80 http://111.com/2.php*

[root@gary-tao php-7.1.6]*# curl -A "xietao xietao" -x127.0.0.1:80 http://111.com/2.php -I*

HTTP/1.0 500 Internal Server Error

**Date: Tue, 26 Dec 2017 09:32:20 GMT**

**Server: Apache/2.4.29 (Unix) PHP/7.1.6**

**X-Powered-By: PHP/7.1.6**

**Connection: close**

**Content-Type: text/html; charset=UTF-8**

出现状态码500，这说明我们访问的页面是存在错误的，此时需要查看PHP的错误日志来判定错误原因，如下：

[root@gary-tao php-7.1.6]*# !cat*

cat /tmp/php\_errors.log

[26-Dec-2017 17:13:35 Asia/Shanghai] PHP Warning: phpinfo() has been disabled **for** security reasons **in** /data/wwwroot/111.com/index.php on line 2

[26-Dec-2017 17:13:47 Asia/Shanghai] PHP Warning: phpinfo() has been disabled **for** security reasons **in** /data/wwwroot/111.com/index.php on line 2

[26-Dec-2017 17:32:08 Asia/Shanghai] PHP Parse error: syntax error, unexpected 'php' (T\_STRING), expecting ',' **or** ';' **in** /data/wwwroot/111.com/2.php on line 2

[26-Dec-2017 17:32:20 Asia/Shanghai] PHP Parse error: syntax error, unexpected 'php' (T\_STRING), expecting ',' **or** ';' **in** /data/wwwroot/111.com/2.php on line 2

**5.配置open\_basedir**

前言

一个服务器上跑很多网站，小公司为节省成本采用的做法，这样操作是会有一些弊端：多个网站跑在同一个服务器上，如果其中一个网站被黑，很有可能会连累到其他站点，为了避免这种尴尬的事情发生，我们应当作一些预防手段。  
PHP有一个概念叫作open\_basedir，它的作用是将网站限定在指定目录里，就算该站点被黑了，黑客只能在该目录下面有所作为，而不能左右其他目录。如果你的服务器上只有一个站点，那可以直接在php.ini中设置open\_basedir参数。但如果服务器上跑的站点比较多，那在php.ini中设置就不合适了，因为在php.ini中只能定义一次，也就是说所有站点都一起定义限定的目录，那这样似乎起不到隔离多个站点的目的。

**1.使用php.ini设置open\_basedir举例演示：**

* 条件：把这个open\_basedir地址目录的111.com目录下改成错误的1111.com

得到如下日志结果，示例如下：

[root@gary-tao php-7.1.6]*# vim /usr/local/php7/etc/php.ini //编辑添加open\_basedir目录地址*

定义如下

open\_basedir = /data/wwwroot/1111.com:/tmp

[root@gary-tao php-7.1.6]*# /usr/local/apache2.4/bin/apachectl graceful*

[root@gary-tao php-7.1.6]*# curl -A "xietao xietao" -x127.0.0.1:80 http://111.com/2.php -I*

HTTP/1.0 500 Internal Server Error

Date: Tue, 26 Dec 2017 11:44:40 GMT

Server: Apache/2.4.29 (Unix) PHP/7.1.6

X-Powered-By: PHP/7.1.6

Connection: close

Content-Type: text/html; charset=UTF-8

[root@gary-tao php-7.1.6]*# vi /data/wwwroot/111.com/2.php //编辑定义如下，保存退出*

<?php

echo 123;

[root@gary-tao php-7.1.6]*# curl -A "xietao xietao" -x127.0.0.1:80 http://111.com/2.php -I*

HTTP/1.0 500 Internal Server Error

Date: Tue, 26 Dec 2017 11:47:23 GMT

Server: Apache/2.4.29 (Unix) PHP/7.1.6

X-Powered-By: PHP/7.1.6

Connection: close

Content-Type: text/html; charset=UTF-8

[root@gary-tao php-7.1.6]*# !cat*

cat /tmp/php\_errors.log

[26-Dec-2017 17:13:35 Asia/Shanghai] PHP Warning: phpinfo() has been disabled **for** security reasons **in** /data/wwwroot/111.com/index.php on line 2

[26-Dec-2017 17:13:47 Asia/Shanghai] PHP Warning: phpinfo() has been disabled **for** security reasons **in** /data/wwwroot/111.com/index.php on line 2

[26-Dec-2017 17:32:08 Asia/Shanghai] PHP Parse error: syntax error, unexpected 'php' (T\_STRING), expecting ',' **or** ';' **in** /data/wwwroot/111.com/2.php on line 2

[26-Dec-2017 17:32:20 Asia/Shanghai] PHP Parse error: syntax error, unexpected 'php' (T\_STRING), expecting ',' **or** ';' **in** /data/wwwroot/111.com/2.php on line 2

[26-Dec-2017 19:44:40 Asia/Shanghai] PHP Warning: Unknown: open\_basedir restriction **in** effect. File(/data/wwwroot/111.com/2.php) **is** **not** within the allowed path(s): (/data/wwwroot/1111.com:/tmp) **in** Unknown on line 0

[26-Dec-2017 19:44:40 Asia/Shanghai] PHP Warning: Unknown: failed to open stream: Operation **not** permitted **in** Unknown on line 0

[26-Dec-2017 19:44:40 Asia/Shanghai] PHP Fatal error: Unknown: Failed opening required '/data/wwwroot/111.com/2.php' (include\_path='.:/usr/local/php7/lib/php') **in** Unknown on line 0

[26-Dec-2017 19:47:23 Asia/Shanghai] PHP Warning: Unknown: open\_basedir restriction **in** effect. File(/data/wwwroot/111.com/2.php) **is** **not** within the allowed path(s): (/data/wwwroot/1111.com:/tmp) **in** Unknown on line 0

[26-Dec-2017 19:47:23 Asia/Shanghai] PHP Warning: Unknown: failed to open stream: Operation **not** permitted **in** Unknown on line 0

[26-Dec-2017 19:47:23 Asia/Shanghai] PHP Fatal error: Unknown: Failed opening required '/data/wwwroot/111.com/2.php' (include\_path='.:/usr/local/php7/lib/php') **in** Unknown on line 0

* 条件：把这个open\_basedir地址目录改成正确的111.com

[root@gary-tao php-7.1.6]*# vim /usr/local/php7/etc/php.ini*

定义如下

open\_basedir = /data/wwwroot/111.com:/tmp

[root@gary-tao php-7.1.6]*# /usr/local/apache2.4/bin/apachectl graceful*

[root@gary-tao php-7.1.6]*# curl -A "a" -x127.0.0.1:80 http://111.com/2.php -I*

HTTP/1.1 200 OK

**Date: Tue, 26 Dec 2017 11:57:59 GMT**

**Server: Apache/2.4.29 (Unix) PHP/7.1.6**

**X-Powered-By: PHP/7.1.6**

**Cache-Control: max-age=0**

**Expires: Tue, 26 Dec 2017 11:57:59 GMT**

**Content-Type: text/html; charset=UTF-8**

**2.针对不同的虚拟主机去限制不同的open\_basedir。**

[root@gary-tao ~]*# vim /usr/local/apache2.4/conf/extra/httpd-vhosts.conf*

定义如下：

php\_admin\_value open\_basedir "/data/wwwroot/111.com:/tmp/"

[root@gary-tao ~]*# /usr/local/apache2.4/bin/apachectl -t*

Syntax OK

[root@gary-tao ~]*# /usr/local/apache2.4/bin/apachectl graceful*

[root@gary-tao ~]*# !curl*

curl -A "a" -x127.0.0.1:80 http://111.com/2.php -I

HTTP/1.1 200 OK

Date: Tue, 26 Dec 2017 12:34:57 GMT

Server: Apache/2.4.29 (Unix) PHP/7.1.6

X-Powered-By: PHP/7.1.6

Cache-Control: max-age=0

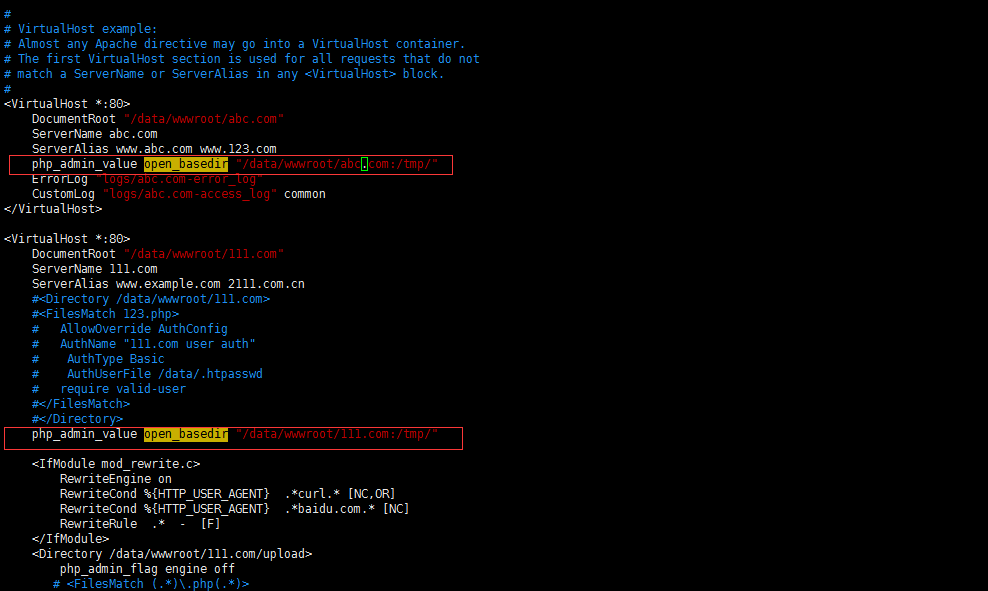
Expires: Tue, 26 Dec 2017 12:34:57 GMT

Content-Type: text/html; charset=UTF-8

[root@gary-tao ~]*# curl -A "a" -x127.0.0.1:80 http://111.com/2.php*

123[root@gary-tao ~]*#*

**修改示例图：**



版权声明：原创作品，如需转载，请与作者联系。否则将追究法律责任