CTF中phpinfo应注意什么

原创

IMNU_S1mple 于 2021-10-04 20:50:45 发布 1161 收藏

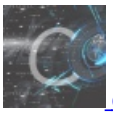
分类专栏： ctf ctfshow 文章标签： php linux

本文链接：https://blog.csdn.net/qq_45891669/article/details/120607230

ctf 同时被 2 个专栏收录

2 篇文章 0 订阅

订阅专栏



ctfshow

3 篇文章 0 订阅

订阅专栏

#CTF中 phpinfo应注意什么

1.allow_url_fopen和allow_url_include

Directive	Local Value	Master Value
allow_url_fopen	On	On
allow_url_include	Off	Off

协议	测试PHP版本	allow_url_fopen	allow_url_include	用法
file://	>=5.2	off/on	off/on	?file=file://D:/soft/phpStudy/WWW/phpcode.txt
php://filter	>=5.2	off/on	off/on	?file=php://filter/read=convert.base64-encode/resource=./index.php
php://input	>=5.2	off/on	on	?file=php://input 【POST DATA】 <?php phpinfo()?>
zip://	>=5.2	off/on	off/on	?file=zip://D:/soft/phpStudy/WWW/file.zip%23phpcode.txt
compress.bzip2://	>=5.2	off/on	off/on	?file=compress.bzip2://D:/soft/phpStudy/WWW/file.bz2 【or】 ?file=compress.bzip2:///file.bz2
compress.zlib://	>=5.2	off/on	off/on	?file=compress.zlib://D:/soft/phpStudy/WWW/file.gz 【or】 ?file=compress.zlib:///file.gz
data://	>=5.2	on	on	?file=data://text/plain,<?php phpinfo()?> 【or】 ?file=data://text/plain;base64,PD9waHAgcGhwaW5mbygpPz4= 也可以： ?file=data:text/plain,<?php phpinfo()?> 【or】

这个配置选项可以知道在PHP文件包含中可以使用哪些伪协议

2.PHP版本

Core

PHP Version	7.3.8

3.open_basedir

open_basedir	/www/admin/localhost_80/wwwroot/:/tmp/:/proc/	*no value*

这个配置选项可以知道PHP将访问目录限制在哪个目录下

4.disable_functions

display_errors	On	On

可以在命令执行的时候，看那些函数被禁了

5.session

session.save_path：session的上传目录

在linux系统中，session文件一般保存在以下几个目录：

```
/var/lib/php/
/var/lib/php/sessions/
/tmp/
/tmp/sessions/
```

session.save_path	*no value*	*no value*

session.upload_progress.name：上传进度

session.upload_progress.name	PHP_SESSION_UPLOAD_PROGRESS	PHP_SESSION_UPLOAD_PROGRESS

查看官方文档可以发现，如果在POST请求中设置同名变量，他的值会被记录到session中，它的值可控，

那么我们文件包含时，只需包含session文件就可以达到文件包含的漏洞

Session 上传进度

注意: 此特性自 PHP 5.4.0 后可用。

当 session.upload_progress.enabled INI 选项开启时，PHP 能够在每一个文件上传时监测上传进度。 这个信息对上传请求自身并没有什么帮助，但在文件上传时应用可以发送一个POST请求到终端（例如通过XHR）来检查这个状态

当一个上传在处理中，同时POST一个与INI中设置的session.upload_progress.name同名变量时，上传进度可以在 $_SESSION 中获得。 当PHP检测到这种POST请求时，它会在 $_SESSION 中添加一组数据, 索引是 session.upload_progress.prefix 与 session.upload_progress.name连接在一起的值。 通常这些键值可以通过读取INI设置来获得，例如

```php
<?php
$key = ini_get("session.upload_progress.prefix") . ini_get("session.upload_progress.name");
var_dump($_SESSION[$key]);
?>
```


session.name：会话名称，它的值存在cookie中，可控，作为sess_PHPSESSID被包含

session.name：会话名称，它的值存在cookie中，可控，作为sess_PHPSESSID被包含

session.name	PHPSESSID	PHPSESSID

session_name

(PHP 4, PHP 5, PHP 7, PHP 8)
session_name — 读取/设置会话名称

说明

```
session_name(string $name = ?): string
```

session_name() 函数返回当前会话名称。 如果指定 **name** 参数， **session_name()** 函数会更新会话名称， 并返回 *原来的* 会话名称。

如果使用 **name** 指定了新字符串作为会话 cookie 的名字， **session_name()** 函数会修改 HTTP 响应中的 cookie （如果启用了 session.transid，还会输出会话 cookie 的内容）。 一旦在 HTTP 响应中发送了 cookie 的内容之后， 调用 **session_name()** 函数会产生错误。 所以，一定要在调用 session_start() 函数之前 调用此函数。

请求开始的时候，会话名称会被重置并且存储到 session.name 配置项。 因此，要想设置会话名称，那么对于每个请求，都需要在 调用 session_start() 函数 之前调用 **session_name()** 函数。

session.upload_progress.cleanup：当文件上传结束后，PHP将会立即清空对应session文件中的内容

session.upload_progress.cleanup	On	On

session.upload_progress.enabled：表示upload_progress功能开始，也意味着当浏览器向服务器上传一个文件时，php将会把此次文件上传的详细信息(如上传时间、上传进度等)存储在session当中

session.upload_progress.enabled	On	On

session.upload_progress.prefix：PHP初始化session时，会产生一个键值，格式为配置文件中session.upload_progress.prefix的值+我们传入的PHP_SESSION_UPLOAD_PROGRESS的值，该值会被写入session文件，按照如上所写，这个sess_PHPSESSID文件中值应为upload_progress_+PHP_SESSION_UPLOAD_PROGRESS

6.flag

甚至有些题目不严谨，flag可以直接在phpinfo中搜到

FLAG	ctfshow{0cfe1bc7-9abd-4a7b-94f3-0be2c6320e72}