百度杯ctf2月场web-include

原创

G-Radiation 于 2017-03-14 20:59:56 发布 1932 收藏 1

分类专栏： CTF 文章标签： ctf 百度杯 writeup

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/u012985855/article/details/62055853

版权


CTF 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

打开题目链接，显示如下内容:

显示的代码如下：

```php
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
    include($_REQUEST['path']);
}else{
    include('phpinfo.php');
}
```

可以知道这是个文件包含的题目，只要我们去读出包含有flag的文件就可以了，由于我们不知道包含于哪个文件，所以我们可以构造以下请求（由于我不知道谷歌应该咋模拟，就先使用一个其他蒲工具吧，懒得开firefox，打开太慢）:

此处用到的是php://input，输入流，通过post请求提交一段php代码用来遍历目录(我选择直接执行系统命令来得快~~~)，然后可以看到我画箭头的地方显示了该目录下的所有文件，可以知道那个dle345aac.php就是含有flag的文件，起初我使用的是`?path=dle345aac.php`去直接包含它，但是并没有显示任何的东西，于是我就使用`php://filter`再次构造如下的请求:

可以看到这个文件通过base64的形式显示了出来，我们解密一下:

可以看到，结果出来了~~~

原文链接:https://b.zlweb.cc/baidu-ctf-2-web-include.html