

ACTF2020 新生赛 -- WP

原创

会下雪的晴天 于 2020-05-18 17:01:24 发布 2341 收藏 3

分类专栏: [CTF做题记录](#) 文章标签: [信息安全](#)

会下雪的晴天

本文链接: https://blog.csdn.net/weixin_43578492/article/details/106194761

版权



[CTF做题记录](#) 专栏收录该内容

33 篇文章 1 订阅

订阅专栏

做题思路记录，同时感谢赵师傅和Y1NG的环境与源码

文章目录

[\[ACTF2020 新生赛\]Include](#)

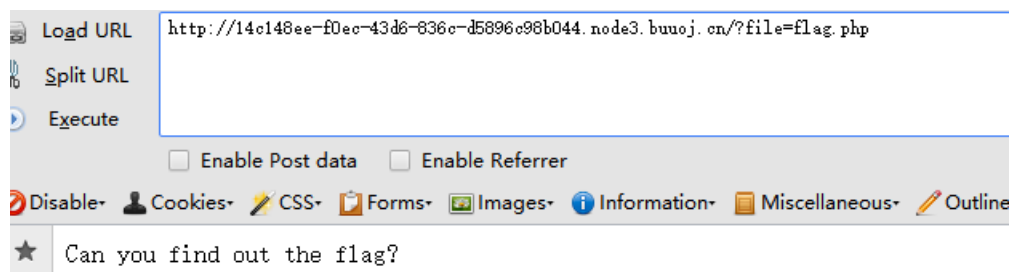
[\[ACTF2020 新生赛\]Exec](#)

[\[ACTF2020 新生赛\]BackupFile](#)

[\[ACTF2020 新生赛\]Upload](#)

[ACTF2020 新生赛]Include

主页显示是一个链接，点进去看看，URL出现file=，结合题目判断为文件包含



用伪协议读flag.php，一般语句为 `php://filter/read=convert.base64-encode/resource=xxx`

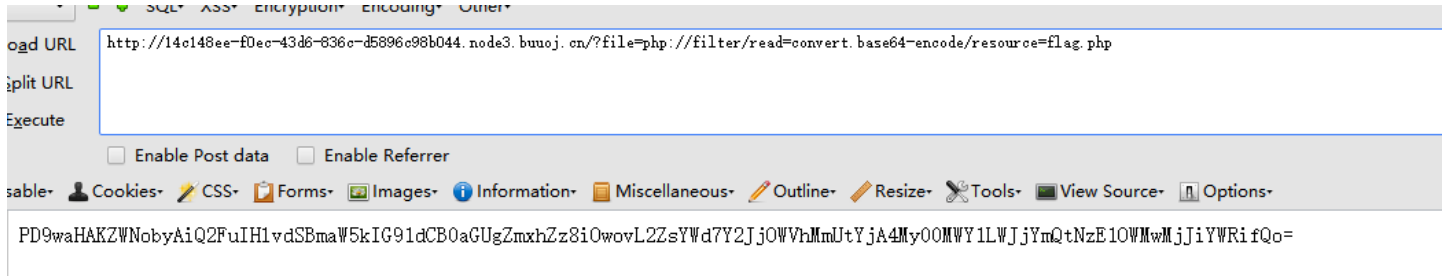
php:// 输入输出流

php://filter (本地磁盘文件进行读取) 元封装器, 设计用于“数据流打开”时的“筛选过滤”应用, 对本地磁盘文件进行读写

read=convert.base64-encode读出来的文件base64加密

resource=xxx读取文件路径 (相对/绝对)

文件读取可以参考这篇文章



解密即可

明文:

```
<?php
echo "Can you find out the flag?";
//flag{cbc9ea2e-b083-41f5-bcbd-7159c022badb}
```

BASE64编码 >

< BASE64解码

BASE64:

```
PD9waHAKZWNobyAiQ2FuIH1vdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7Y2JjOWVhMmUtYjA4My00MmY1LWJjYmQtNzE1OWMwMjJiYWVfQ0=
```

[ACTF2020 新生赛]Exec

exec, 这不是php里面命令执行的函数嘛, 主页是个ping的api

PING

https://blog.csdn.net/weixin_43578492

看到ping首先想到命令执行漏洞, 此题似乎没有任何过滤, 直接淦就完了

先看看flag在不在本目录 (因为搜索耗时太长) `127.0.0.1 | ls`, 用 `|` 可以只输出后面命令执行的结果, 如果想都输出可以用 `||`, `;`

PING

`index.php` https://blog.csdn.net/weixin_43578492

并没有, 那就找吧, `127.0.0.1 | find / -name flag`, 多等一会, 这是从根目录开始find的

PING

`/flag` https://blog.csdn.net/weixin_43578492

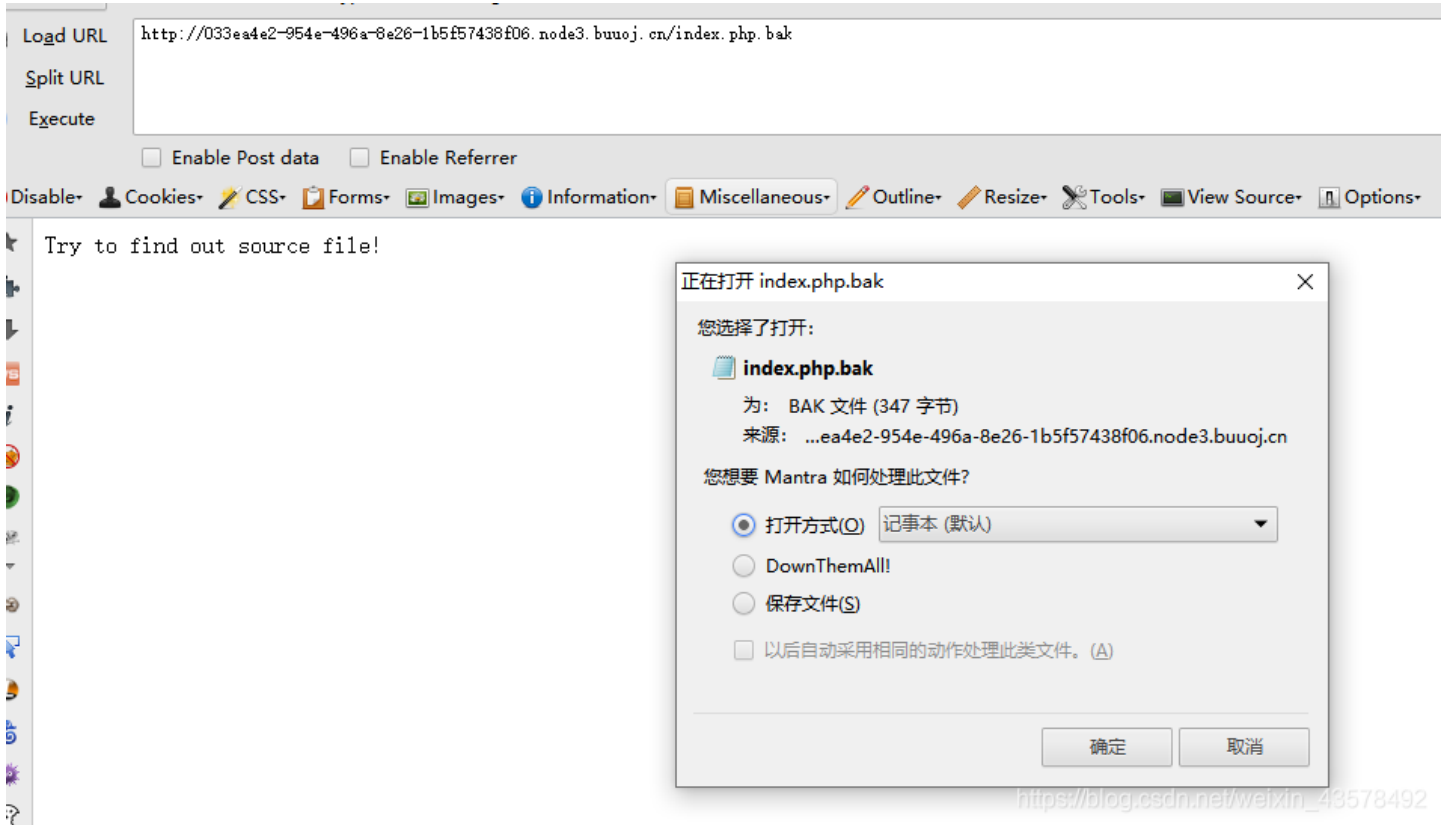
找到了, 直接cat就好

`flag{e98c1290-d4f6-4ac5-bf6b-fa99bd395fce}`

[ACTF2020 新生赛]BackupFile

题目就已经提示了是文件备份

常见文件备份有 `.swp`(vim未正常退出备份) `.bak` `.back`
暂时就知道这么多，持续更

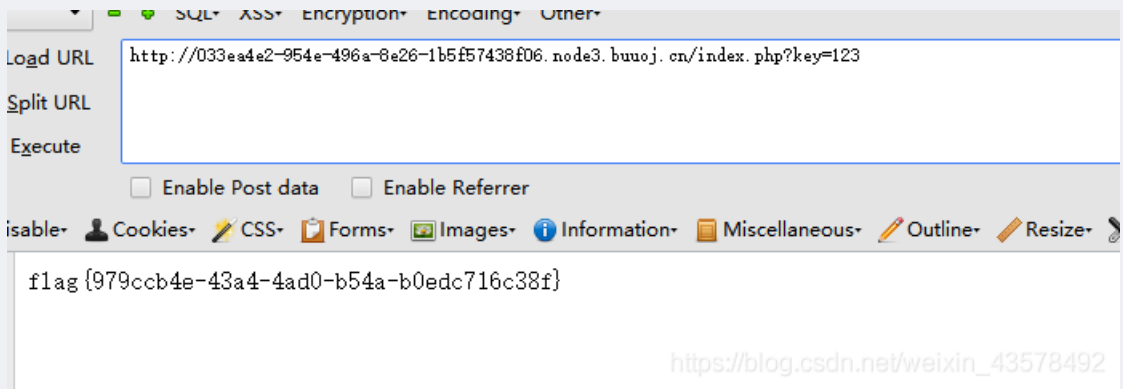


下载后给了源码

```
<?php
include_once "flag.php"; // 包含flag文件

if(isset($_GET['key'])) { // 获取key参数
    $key = $_GET['key'];
    if(!is_numeric($key)) { // 判断key是否为数值OR数字字符串，不仅可以检查10进制，16进制也可以
        exit("Just num!"); // 不是则退出脚本
    }
    $key = intval($key); // 获取变量整数数值
    $str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
    if($key == $str) { // 弱比较
        echo $flag;
    }
}
else {
    echo "Try to find out source file!";
}
?>
```

弱比较：如果比较一个数字和字符串或者比较涉及到数字内容的字符串，则字符串会被转换成数值并且比较按照数值来进行，在比较时该字符串的开始部分决定了它的值，如果该字符串以合法的数值开始，则使用该数值，否则其值为0。所以直接传入key=123就行
参考：<https://www.cnblogs.com/Mrsm1th/p/6745532.html>



[ACTF2020 新生赛]Upload

鼠标悬浮在小灯泡上出现上传处

嘿伙计，你发现它了！

upload



https://blog.csdn.net/weixin_43578492

先传个一句话试试，看看源码是不是前端限制

该文件不允许上传，请上传jpg、png、gif结尾的图片噢！

确定

https://blog.csdn.net/weixin_43578492

找到了，前端限制，可以在console里面把函数置空，也可以在bp里面改后缀，我是在console里面弄得，发现后端也有限制

```
nonono~ Bad file!
```



改改后缀试试，php3,php4,php5,pht,phtml,先上传了个图片，看看给不给路径

```
Upload Success! Look here~ ./uplo4d/466d378c88b2afdf41740ae155cbcca4.gif
```

pht也能上传成功，但是不能连上，应该是没配置这个选项，最终用的phtml后缀，上antword

```
/flag  
(www-data:/var/www/html/uplo4d) $ cat /flag  
flag{14445565-1981-4ca1-884c-168748c5b450}  
(www-data:/var/www/html/uplo4d) $
```