bugkuCTF Writeup （Web）1-9

原创

Troublor 于 2018-01-23 21:47:32 发布 1719 收藏

分类专栏： CTF 文章标签： CTF bugku web

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/troublor/article/details/79144444

版权

CTF 专栏收录该内容

8 篇文章 1 订阅

订阅专栏

签到题

加群就行了，没卖什么关子:)

Web2

http://blog.csdn.net/troublor

花里胡哨的果断去看源码。。。

```
<!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">
 ▶#shadow-root (open)
 ▶<head>…</head>
 ▼<body id="body" onload="init()">
    <!--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>
      <canvas width="1022" height="635"> == $0
    </div>
  </body>
</html>
```

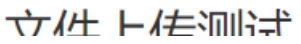
http://blog.csdn.net/troublor

flag就在这了

文件上传测试

http://blog.csdn.net/troublor

就按照上面说的，传一个php试试



http://blog.csdn.net/troublor

提交后说：非图片文件

那就是既要是图片又要是php了

暂时不知道它是怎么判断是图片是php文件的，先试试再说

用Fiddler抓包

先改一改文件扩展名试一试吧

```
POST http://103.238.227.13:10085/ HTTP/1.1
Host: 103.238.227.13:10085
Proxy-Connection: keep-alive
Content-Length: 729
Cache-Control: max-age=0
Origin: http://103.238.227.13:10085
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarybdGynKvQBciks6VZ
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3298.4 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://103.238.227.13:10085/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7

------WebKitFormBoundarybdGynKvQBciks6VZ
Content-Disposition: form-data; name="file"; filename="testmysql.php"
Content-Type: application/octet-stream

<?php
/*     Using "mysqli" instead of "mysql" that is obsolete.
*     Utilisation de "mysqli" □ la place de "mysql" qui est obsol□te.
* Change the value of parameter 3 if you have set a password on the root userid
* Changer la valeur du 3e param□tre si vous avez mis un mot de passe □ root
*/
$mysqli = new mysqli('127.0.0.1', 'root', '');

if ($mysqli->connect_error) {
    die('Connect Error (' . $mysqli->connect_errno . ') '
            . $mysqli->connect_error);
}
echo 'Connection OK';
$mysqli->close();
?>

------WebKitFormBoundarybdGynKvQBciks6VZ--
```

Find... (press Ctrl+Enter to highlight all)

Breakpoint hit. Tamper, then: Break on Response | Run to Completion | Choose Response...

Transformer | Headers | TextView | SyntaxView | ImageView | HexView | WebView | Auth | Caching | Cookies | Raw | JSON | XML

No Response body.

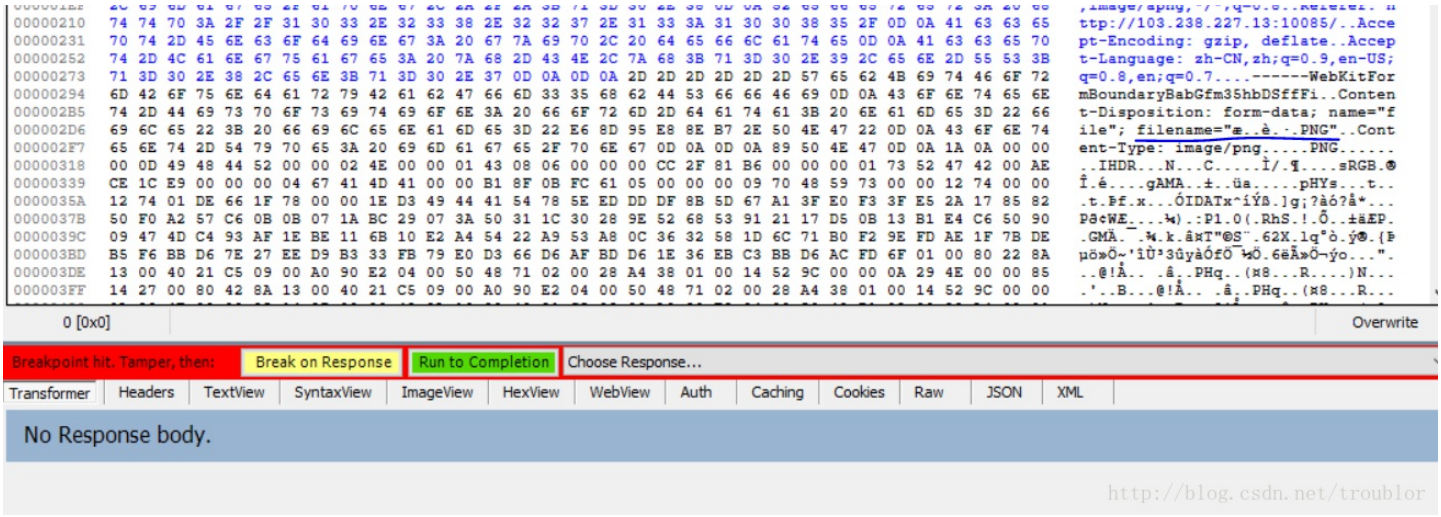
http://blog.csdn.net/troublor

后缀改成jpg之后，仍然提示是非图片文件，那反过来呢？

先上传一个图片，然后改成php后缀

Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML

```
00000000  50 4F 53 54 20 68 74 74 70 3A 2F 2F 31 30 33 2E 32 33 38 2E 32 32 37 2E 31 33 3A 31 30 30 38 35 2F   POST http://103.238.227.13:10085/
00000021  20 48 54 54 50 2F 31 2E 31 0D 0A 48 6F 73 74 3A 20 31 30 33 2E 32 33 38 2E 32 32 37 2E 31 33 3A 31    HTTP/1.1..Host: 103.238.227.13:1
00000042  30 30 38 35 0D 0A 50 72 6F 78 79 2D 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 6B 65 65 70 2D 61 6C 69 76   0085..Proxy-Connection: keep-aliv
00000063  65 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 38 31 38 31 0D 0A 43 61 63 68 65 2D 43 6F   e..Content-Length: 8181..Cache-Co
00000084  6E 74 72 6F 6C 3A 20 6D 61 78 2D 61 67 65 3D 30 0D 0A 4F 72 69 67 69 6E 3A 20 68 74 74 70 3A 2F 2F   ntrol: max-age=0..Origin: http://
000000A5  31 30 33 2E 32 33 38 2E 32 32 37 2E 31 33 3A 31 30 30 38 35 0D 0A 55 70 67 72 61 64 65 2D 49 6E 73   103.238.227.13:10085..Upgrade-Ins
000000C6  65 63 75 72 65 2D 52 65 71 75 65 73 74 73 3A 20 31 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20   ecure-Requests: 1..Content-Type:
000000E7  6D 75 6C 74 69 70 61 72 74 2F 66 6F 72 6D 2D 64 61 74 61 3B 20 62 6F 75 6E 64 61 72 79 3D 2D 2D 2D   multipart/form-data; boundary=---
00000108  2D 57 65 62 4B 69 74 46 6F 72 6D 42 6F 75 6E 64 61 72 79 42 61 62 47 66 6D 33 35 68 62 44 53 66 66   -WebKitFormBoundaryBabGfm35hbDSff
00000129  46 69 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 57 69 6E 64   Fi..User-Agent: Mozilla/5.0 (Wind
0000014A  6F 77 73 20 4E 54 20 31 30 2E 30 3B 20 57 4F 57 36 34 29 20 41 70 70 6C 65 57 65 62 4B 69 74 2F 35   ows NT 10.0; WOW64) AppleWebKit/5
0000016B  33 37 2E 33 36 20 28 4B 48 54 4D 4C 2C 20 6C 69 6B 65 20 47 65 63 6B 6F 29 20 43 68 72 6F 6D 65 2F   37.36 (KHTML, like Gecko) Chrome/
0000018C  36 35 2E 30 2E 33 32 39 38 2E 34 20 53 61 66 61 72 69 2F 35 33 37 2E 33 36 0D 0A 41 63 63 65 70 74   65.0.3298.4 Safari/537.36..Accept
000001AD  3A 20 74 65 78 74 2F 68 74 6D 6C 2C 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78 68 74 6D 6C 2B 78 6D 6C   : text/html,application/xhtml+xml
000001CE  2C 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78 6D 6C 3B 71 3D 30 2E 39 2C 69 6D 61 67 65 2F 77 65 62 70   ,application/xml;q=0.9,image/webp
```



然后就有flag了

Flag:42e97d465f962c53df9549377b513c7e

大概判断是否是php文件的时候只看的是文件扩展名，判断是否是图片只看的是文件的二进制内容吧

计算题

http://blog.csdn.net/troublor

第一感觉，这是？验证码？

来源:BugKu-ctf

http://blog.csdn.net/troublor

然后下意识就去点有颜色的那块，还真会变，真是验证码
心里盘算着这玩意儿要是个图片。。。还得识别图片中的数字不成
然而。。。。假的
这根本就是用CSS和JS给文字加的底色，还真像。。。。以假乱真
然后我就很好奇了，想去看看这以假乱真的“验证码的源码”。。。结果
点开js/code.js这个文件看源码，结果就看到了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{CTF-bugku-0032}");
        } else {
            alert("输入有误!");
        }
    });
});
```

http://blog.csdn.net/troublor

感觉有些强。。。好歹用ajax去服务器获取flag吧。。。放到静态文件里也太草率了

web基础$_GET

http://blog.csdn.net/troublor

php代码审计

```
$what=$_GET['what'];
echo $what;
if($what=='flag')
echo 'flag{****}';
```
g.csdn.net/troublor

这好像都算不上审计，发送一个get请求带上参数就可以了

```
http://120.24.86.145:8002/get/?what=flag
```

Flag在此

```
$what=$_GET['what'];
echo $what;
if($what=='flag')
echo 'flag{****}';
flagflag{bugku_get_su8kej2en}
```
://blog.csdn.net/troublor

web基础$_POST

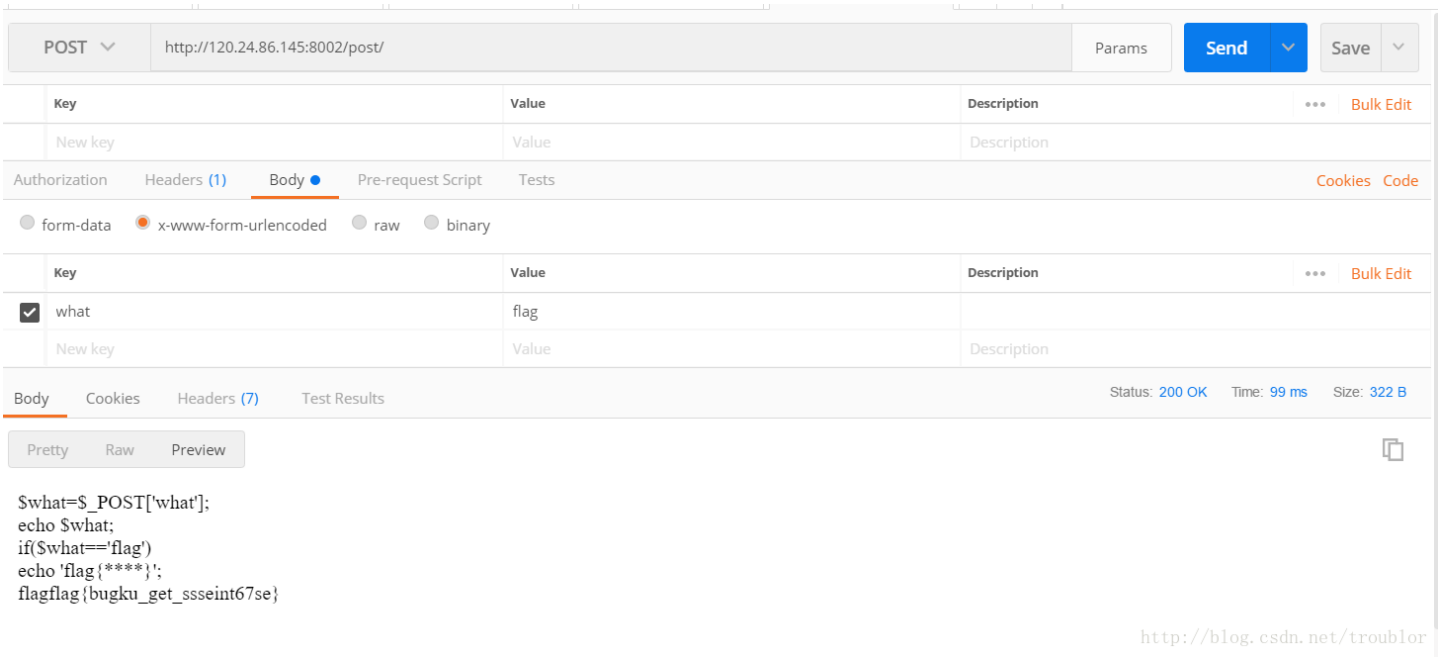
http://blog.csdn.net/troublor

还是代码审计

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

og.csdn.net/troublor

这次是要发post请求，用postman发一个就好了，得到flag



http://blog.csdn.net/troublor

矛盾

http://blog.csdn.net/troublor

这回是php代码审计了

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

csdn.net/troublor

既不能是数字，又要和1相等

双等号===弱类型

就这个了，只要get的参数是数字1开头后面都是字母比如“1aaaa”这样，双等号判断的时候要类型转换，1aaa就转换成1了，而它也很明显不是数字（!is_numeric）

payload:`http://120.24.86.145:8002/get/index1.php?num=1abc`

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

//blog.csdn.net/troublor

Web3

http://blog.csdn.net/troublor

一打开啥也没有，就让我找flag，果断看源码

```
105 alert("flag就在这里");
106 alert("来找找吧");
107 alert("flag就在这里");
108 alert("来找找吧");
109 alert("flag就在这里");
110 alert("来找找吧");
111 alert("flag就在这里");
112 alert("来找找吧");
113 alert("flag就在这里");
114 alert("来找找吧");
115 alert("flag就在这里");
116 alert("来找找吧");
117 alert("flag就在这里");
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 <!--&#75;&#69;&#89;&#123;&#74;&#50;&#115;&#97;&#52;&#50;&#97;&#104;&#74;&#75;&#45;&#72;&#83;&#49;&#49;&#73;&#73;&#73;&#125;—>
134 </script>
135 </head>
136 </html>
137
138
139
```

http://blog.csdn.net/troublor

最后那一堆Unicode编码的注释很可疑啊，一转换就发现是flag了

http://blog.csdn.net/troublor

SQL注入

http://blog.csdn.net/troublor

打开网页，满屏幕找注入点输入框。。。觉着不是我网卡没加载出来，就是藏在哪里了。半天也没找着。
尝试了一下才发现直接get请求带上id参数就是注入点了
试了一下最基本的`1' or 1='1'%23`
没有什么效果，去看源码，发现编码格式是GB2312，试了试宽字符注入，确实是。
然后就很标准了
`1%df' union select 1,2%23`发现查询是两列
`1%df' union select 1,database()%23`发现数据库名是sql5
`1%df' union select id,string from sql5.key%23` 达到了题目要求
然后就有点懵

http://blog.csdn.net/troublor

题目要求的那个字段不是KEY{...}这种格式啊
开始开脑洞：
数了数一共是偶数个，而且又都是十六进制字符，赶快去转ascii，结果这根本就超了ascii范围了，全是乱码
又想是不是别的什么编码。。。试了很多种发现都是乱码，这回懵了��
算了司马当活马医试试，强行加上KEY{}提交。。。
竟然过了。。。

第一次写WriteUp，也不知道格式是什么样，反正就瞎写了，想的啥就写啥，望大佬们不要嘲笑