bugkuctf web题的一些write up

原创

冷冻咸鱼 于 2019-07-24 13:56:30 发布 112 收藏

分类专栏： 1 文章标签： 1

本文链接：https://blog.csdn.net/qq_44384511/article/details/97121042

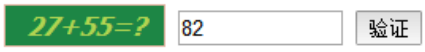
点进去发现是一张图片，先f12查看源代码，直接获得

开始第二题

点进去发现一张图片，要输入图片中计算结果，尝试了一下发现只能输入一位，f12后修改maxlength大于等于2即可

```
<span id="code" class="code" style="background: rg
<input type="text" class="input" maxlength="1">
<button id="check">验证</button>
```

输入答案获得flag



来源:BugKu-ctf

第三题

看题目就知道要用get方法，点进去审计代码

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

当what=flag时，显示出flag
所以用get方法提交what=flag，得到flag


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

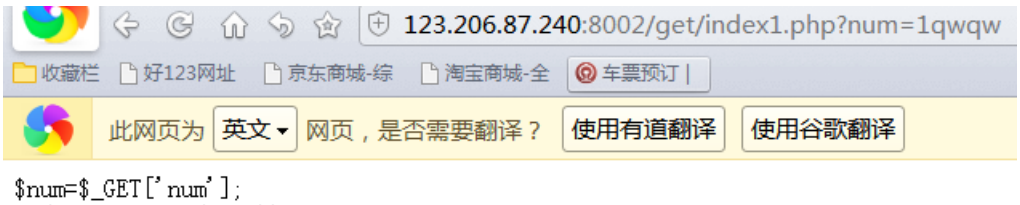
跟上一题几乎完全一样，只是提交数据的方法换成post

先审计代码

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

既要num不是数字，又要num==1

可以构造num=1开头的字符串



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


得到flag

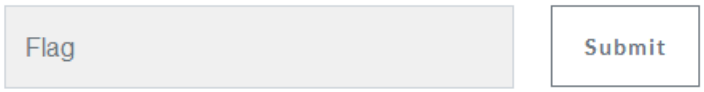
点进去，发现不停弹出对话框，直接禁用对话框，查看源代码，拉到底发现一串unicode码，解码后得到flag.

```
    alert("flag就在这里");
    alert("来找找吧");
    <!--&#75;&#69;&#89;&#123;&#74;&#50;&#115;&#97;&#52;&#50;&#97;&#104;&#74;&#75;&#45;&#72;&#83;&#49;&#49;&#73;&#73;&#73;&#125;-->
  </script>
</head>
<body>
```

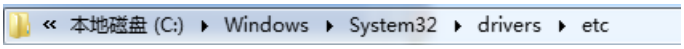
KEY{J2sa42ahJK-HS11III}

KEY{J2sa42ahJK-HS11III}

域名解析



按照题目要求



到此路径下找到hosts文件，编辑，在最后一行加上123.206.87.240 flag.baidu.com

```
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#   127.0.0.1       localhost
#   ::1             localhost
123.206.87.240 flag.baidu.com
```


如图

访问flag.baidu.com,得到flag

```
KEY{DSAHDSJ82HDS2211}
```

你必须让他停下来

进入后发现网页不停变化，可以发现某些时候flag会一闪而过，所以考虑采用burpsuite抓包（我是靠着多年单身手速复制到的），逐个查看抓到的包的响应，在某个包中得到flag

```
Raw Headers Hex HTML Render
<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{dummy_game_1s_s0_popular}</a></body>
</html>
```


本地包含

看名字，应该是flag包含在php文件中,进去审计代码

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

hello变量通过get方法接受值，并分级回显到网页上，尝试了一下hello=$GLOBALS,发现所有变量中均不含flag,猜测是写在注释中。所以我们可以通过对hello赋值为file('flag.php')来查看php文件的内容，获得flag

```
array(8) { [0]=> string(7) " string(2) " " [2]=> string(34) " $flag = "Too Young Too Simple"; " [3]=> string(2) " " [4]=> string(24) "// flag{bug-ctf-gg-99} " [5]=>
string(2) " " [6]=> string(2) " " [7]=> string(3) " ?>" } <?php
    include "flag.php";
    $a = @$_REQUEST['hello'];
    eval( "var_dump($a);");
    show_source(__FILE__);
?>
```

变量1

审计代码，第一句告诉了flag在变量中

flag In the variable ! <?php

error_reporting(0);

include "flag1.php";

highlight_file(**file**);

if(isset($_GET['args'])){

$args = KaTeX parse error: Expected group after '^' at position 36: …(!preg_match("/^\w+/",

$$args))die("argserror!");eval("var ump($args);");$$

}

?>

中间有一个正则表达式，只能输入数字和字母下划线，考虑用GLOBALS将所有变量显示出来，拿到flag

web5

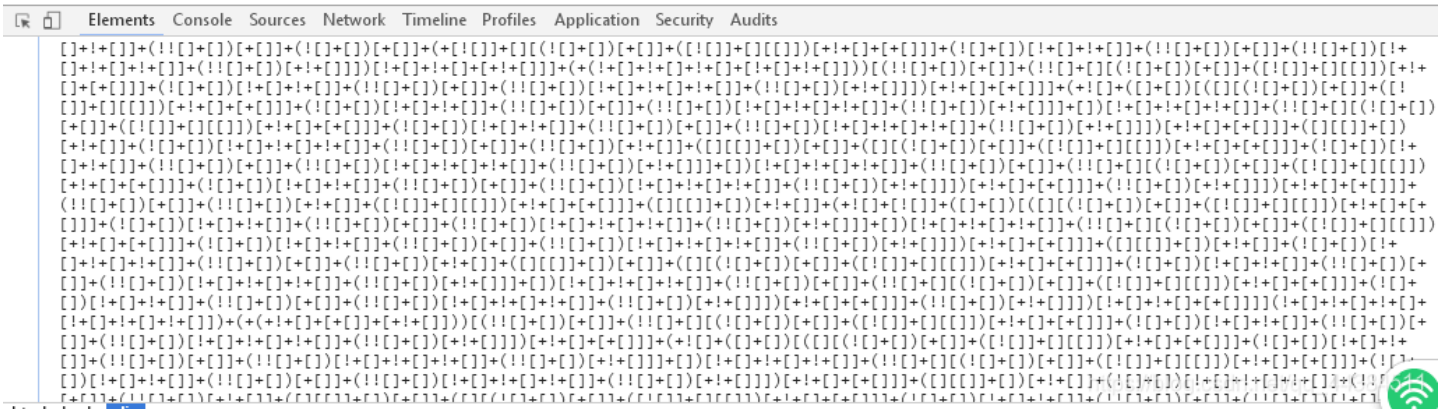
http://123.206.87.240:8002/web5/

字母大写

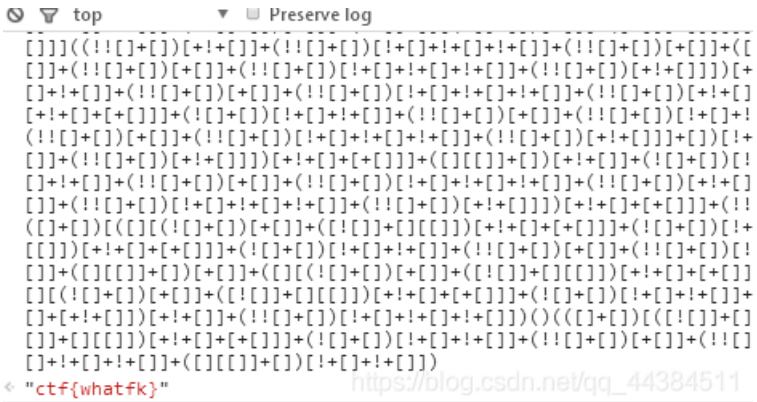
Flag

Submit

看标题是jspfuck，粗鄙之语，不明觉厉
进去有一个输入框，也不知道要干啥，f12查看源码，
发现一大串乱七八糟的东西



百度之后发现是jsp代码，通过控制台输入，得到flag



(不知道为什么后面看到的代码是错的，只好跑到别人的writeup里找了代码
头等舱

http://123.206.87.240:9009/hd.php

Flag Submit

看到头等舱，推测信息在消息头中，用burp suite抓包，找了请求头，没有发现flag,再去看响应头，发现了flag

```
Date: Thu, 25 Jul 2019 13:1
Content-Type: text/html
Connection: keep-alive
Keep-Alive: timeout=60
flag{Bugku_k8_23s_istra}:
Content-Length: 139
```

网站被黑

Challenge 4731 Solves ×

网站被黑

60

http://123.206.87.240:8002/webshell/

这个题没技术含量但是实战中经常遇到

Flag Submit

进去一看404,联想到标题网站被黑，猜测是网站目录下有其他文件，用扫描工具扫描网页

发现一个shell.php文件，点进去是一个登陆界面

直接用burp suite抓包暴力破解，破解得密码是hack,输入后得到flag

管理员系统

刚看到题目的时候以为是sql注入，尝试注入了一下，结果。。。

管理员系统

Username:

Password:

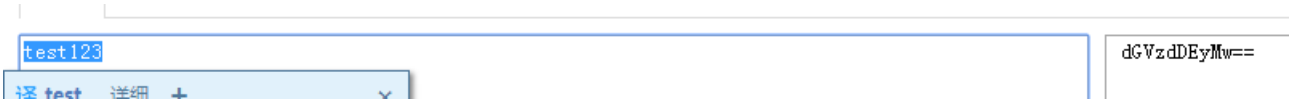
Submit Reset

IP禁止访问，请联系本地管理员登陆，IP已被记录.

f12查看源代码

发现一串疑似base64的字符串，试着解密一下

果然有点东西



猜测是登录密码，联想到提示中的本地管理员，猜测账号是admin