Bugku writeup

原创

老青蛙38324 于 2019-03-03 15:30:48 发布 190 收藏

文章标签： Bugku writeup

本文链接：https://blog.csdn.net/weixin_44119209/article/details/88088674

Bugku题目writeup（一）

一些小的体会

在做**ctf**题目时要选择合适的浏览器，火狐或者是谷歌，一些常用插件搞搞清楚，前期做题靠工具，后期做题靠实力，注意自身知识的积累与总结

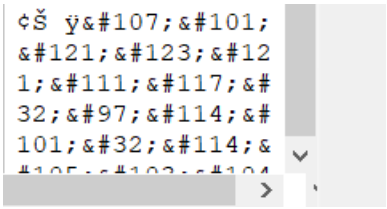
一.杂项

1.签到题

关注得到**flag**

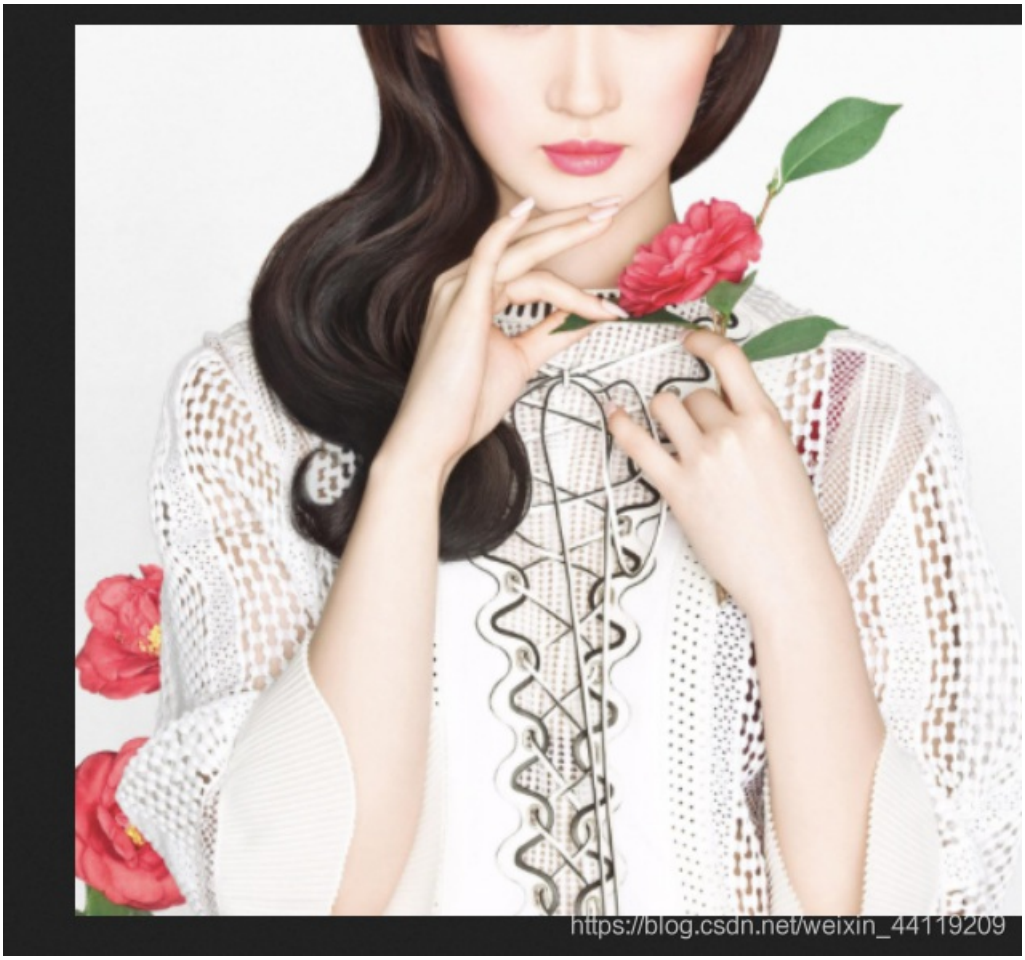
2.这是一张单纯的图片

用**winhex**打开图片，发现一串数字，**ascll**码转码，得到**flag**



3.猜

百度有一个智能识图功能，识别一下，刘亦菲的大名就出来了



二.WEB

1.web2

打开网站一堆滑稽，**F12**，得到**flag**。

```
<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>
```

![在这里插入图片描述](https://img-blog.csdnimg.cn/20190303152156568.png?x-oss-process=image/watermark,type_ZmFuZ3poZW5naGVpdGk,shadow_10,text_aHR0cHM6Ly9ibG9nLmNzZG4ubmV0L3dlaXhpbl80NDExOTIwOQ==,size_16,color_FFFFFF,t_70)

2.计算器

发现框内只能输入一位数字，**F12**打开开发者工具，修改网页**html**，改成相应的位数，输入答案，得到**flag**。

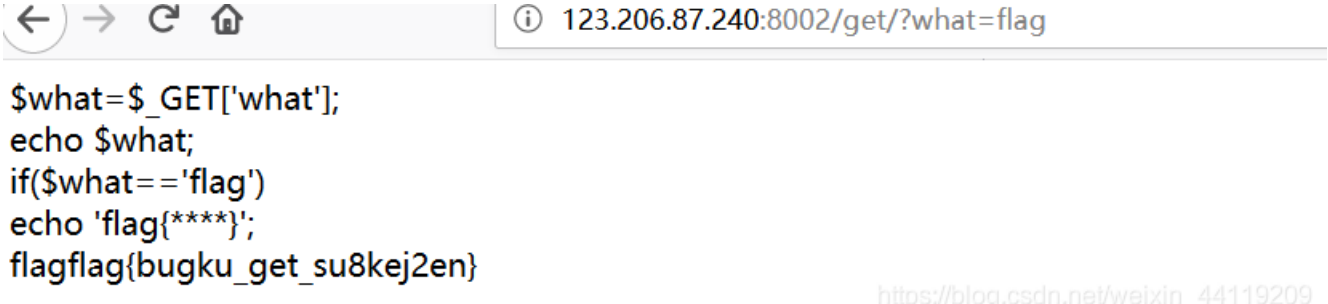
43+61=? 1 验证

查看器 控制台 调试器 样式编辑器 性能 内存 网络 存储

```
DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/
    border:1px solid #e2b4a2;
    background: #e2b4a2;
}

.input {
    width: 100px;

}
</style>

</head>

<body>

<span id="code" class="code" style="background: rgb(254, 137, 236) none repeat scroll 0% 0%;
141);">43+61=?</span> <input type="text" class="input" maxlength="3">
<button id="check">验证</button>
```


3.web基础get

读懂代码，还是要好好学习语言，构造？**what=flag**得到**flag**

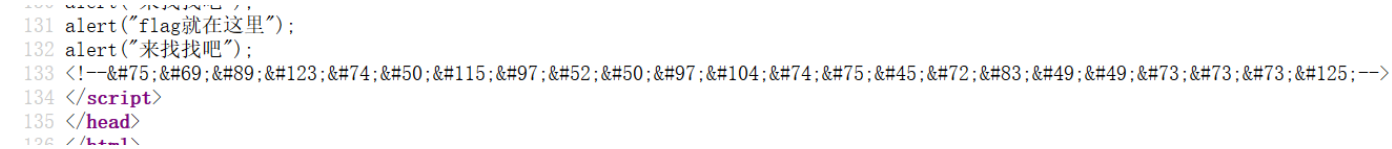


4.矛盾

从**php**代码中可读出矛盾，**php**判断字符串以**1**开头即可判断等值，构造**num=1**，**zl**表示字符串连接即可

5.web3

打开网页对话框一只弹出，阻止，查看一下页面源代码，在最后发现一串编码，解码得到**flag**



6.web5

提交随便一个密码，出现再好好看看，**burpsuite**直接抓包，出现一些字符，百度后发现为**jother**编码，谷歌**console**回车得到**flag**


HTTP/1.1 200 OK
Server: nginx
Date: Sun, 03 Mar 2019 07:13:33 GMT
Content-Type: text/html
Connection: close
Content-Length: 12539
<html>
<body>
<div
style="display:none;">
Type a search term
0 matc