

# bugku-writeup-web-源代码

原创

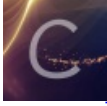
dark2019 于 2021-06-14 15:41:45 发布 60 收藏 2

分类专栏: [信息安全](#) 文章标签: [安全](#) [信息安全](#) [url](#)

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/qq\\_22597955/article/details/117905287](https://blog.csdn.net/qq_22597955/article/details/117905287)

版权



[信息安全](#) 专栏收录该内容

53 篇文章 1 订阅

订阅专栏

“bugku-web源代码 解题思路记录。”

题目: 看看源代码?

web13

WEB

未解决

分数: 20

金币: 2

题目作者: harry

一血: lsmzr

一血奖励: 1金币

解决: 3377

提示:

描述: 看看源代码?

<http://114.67.246.176:12428>

02:32:37

删除场景

延时场景

[https://blog.csdn.net/qq\\_22597955](https://blog.csdn.net/qq_22597955)

## 01—查看源码, 拼接URL

自动换行

```
1 <html>
2 <title>BUGKUCTF-WEB13</title>
3 <body>
4 <div style="display:none;"></div>
5 <form action="index.php" method="post" >
6 看看源代码? <br>
7 <br>
8 <script>
9 var p1 =
10 '%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' ;
11 var p2 =
12 '%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' ;
13 eval(unescape(p1) + unescape('%35%34%61%61%32' + p2));
14 </script>
15 <input type="input" name="flag" id="flag" />
16 <input type="submit" name="submit" value="Submit" />
17 </form>
18 再好好看看。
```

[https://blog.csdn.net/qq\\_22597955](https://blog.csdn.net/qq_22597955)

查看源码发现9,10,11行中提示需要拼接URL: `p1+'%35%34%61%61%32'+p3`, 然后解码。

## 02—解码

在线工具

SSL在线工具

SSL漏洞在线检测

工具网

买证书

### URL编码

url

```
%66%75%6e%63%74%69%6f%6e%20%63%68%65%63%6b%53%75%62%6d%69%74%28%29%7b%70%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%77%6f%72%64%22%29%3b%69%66%28%22%75%6e%64%65%66%69%6e%65%64%22%21%3d%67%49%70%65%6f%66%29%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%63%1%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%67%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%65%6e%74%3b
```

字符集

utf8(unicode编码)

编码

解码

```
function checkSubmit() {var a=document.getElementById("password");if("undefined"!=typeof a) {if ("07d709b2b54aa2aa648cf6e87a7114f1"==a.value)return 0;alert("Error");a.focus();return 1}} document.getElementById("levelQuest").onsubmit=checkSubmit;
```

[https://blog.csdn.net/kq\\_22597955](https://blog.csdn.net/kq_22597955)

使用url在线解码工具：<http://ctf.ssleye.com/url.html>，完成解码。

## 03—得到flag

### 看看源代码?

真实的flag: flag{58e101fa481bb5100269f9fae777a78a}

解码后得到密码，submit，得到flag。