

bugku web 13 writeup

原创

[T0mrwi1b3t](#) 于 2020-12-04 17:38:20 发布 69 收藏

分类专栏: [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/weixin_50597969/article/details/110666587

版权



[bugku](#) 同时被 2 个专栏收录

9 篇文章 0 订阅

订阅专栏



[web](#)

19 篇文章 0 订阅

订阅专栏

bugku web13

题目信息

解题思路

FLAG

题目信息

web13 已解决

分数: 20 金币: 2

题目作者: [harry](#)

一血: [ismzr](#)

一血奖励: 1金币

解决: 1526

提示:

描述: [看看源代码?](#)

https://blog.csdn.net/weixin_50597969

看看源代码?

解题思路

先随便输一个

看看源代码?

在好好看看。

F12查看源代码

其实先查看源代码最好

关键代码如下:

```
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%22%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));
```

返现有一串的URL编码字符

考虑在线转换（传送门

```
var p1 = 'function checkSubmit(){var a=document.getElementById("password");if("undefined"!==typeof a){if("67d709b2b';  
var p2 = 'aa648cf6e87a7114f1'==a.value)return!0;alert("Error");a.focus();return!1}}document.getElementById("levelQuest").onsubmit=checkSubmit;';  
eval(unescape(p1) + unescape('54aa2' + p2));
```

接着把两个字符串拼在一起输入框中点击submit

67d709b2b54aa2aa648cf6e87a7114f1

看看源代码?

真实的flag: flag{1314a88d4ec5e08de538222e39e88ff9}

这样就爆出了FLAG

FLAG

flag{1314a88d4ec5e08de538222e39e88ff9}
