

web5-writeup

打开题目

Challenge

4278 Solves

×

web5
60

JSPFUCK??????答案格式CTF{**}

<http://123.206.87.240:8002/web5/>

字母大写

Flag

Submit

点击访问,出现输入框, 随便输入点字符串, 点击提交, 提示(在好好看看)

JSPFUCK??????答案格式CTF{*****}

Submit

在好好看看。

查看源代码，出现了一大串(!+())[]，根据题目提示，这应该是一串JSFuck编码

[illegible]

JSFuck []()!+

JSFuck是一种基于JavaScript原子部分的深奥教育编程风格。它只使用六个不同的字符来编写和执行代码。

它不依赖于浏览器，因此您甚至可以在Node.js上运行它。

简单来说JSFuck可以让你只用6个字符[]()!+来编写JavaScript程序。

用途:

- ①脚本注入时防止过滤
 - ②一定程度加密关键代码（不适合加密大量代码，毕竟太长了）
 - ③把包含的字符做到极致（`[]()!+`）
 - ④转换后本质依然是JavaScript，通过JavaScript的一些特性生成。
- 了解更多可以访问：<https://github.com/aemkei/jsfuck>

我们直接将JSFuck复制下来利用浏览器的Console执行，或者在线工具进行转换

(<http://www.jsfuck.com/>)

The screenshot shows the JSFuck website interface. At the top, there is a form with the following HTML code:

```
4 <form action="index.php" method="post" >
5   JSPFUCK?????答案格式CTF{*****}<br>
6   <br>
7   <input type="input" name="flag" id="flag" />
8   <input type="submit" name="submit" value="Submit" />
9 </form>
10 在好好看看。
```

Below the form, there is a console output showing the result of the conversion:

```
"ctf{whatfk}"
```

The website also includes a description of JSFuck, its usage instructions, and a list of links and alternatives.

将得到的值进行提交，提示（唉吆，已经非常非常接近了。。。）

JSPFUCK??????答案格式CTF{*****}

唉吆，已经非常非常接近了。。。)

将得到的值换成大写（题目提示），提交

```
C:\Users\xiaowei>python3
Python 3.7.0 (v3.7.0:1bf9cc5093, Jun 27 2018, 04:59:51) [MSC v.1914 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>> print('ctf{whatfk}'.upper())
CTF{WHATFK}
>>> _
```

JSPFUCK??????答案格式CTF{*****}

您的智商已爆表！恭喜！