

i春秋broken

转载

[weixin_30701575](#) 于 2019-09-11 14:05:00 发布 184 收藏

原文链接: <http://www.cnblogs.com/wosun/p/11505931.html>

版权

点开一个附带超链接的网页，直接点击file跳转到broken网页

网页里面是一个jsfuck代码

Jsfuck代码的执行方法

- ①复制
- ②打开firefox浏览器
- ③按下F12
- ④选择上方的控制台
- ⑤在下方粘贴是jsfuck代码
- ⑥按下回车即可运行

这里有一篇jsfuck的介绍<https://gitee.com/mirrors/jsfuck>

亦或者直接访问<http://www.jsfuck.com/#> 在线加密解密

```
• false      => ![]
• true       => !![]
• undefined  => [] [[]]
• NaN        => +[![]]
• 0          => +[]
• 1          => +!+[]
• 2          => !+[]+!+[]
• 10         => [+!+[]]+[+[]]
• Array      => []
• Number     => +[]
• String     => []+[]
• Boolean    => ![]
• Function   => []["filter"]
• eval       => []["filter"]["constructor"](CODE)()
• window     => []["filter"]["constructor"]("return this")()
```

按照这个解码表审查题中的jsfuck代码发现[]没有闭合,头部的地方有问题，看到开头出现两个[[，所以先将文件的[[改为[[


```
(1) [...]
  0: "var flag=\"flag{f_f_l_u_a_c_g_k}\";alert('flag is not here');"
  length: 1
  <prototype>: []
    ▶ concat: function concat()
    ▶ constructor: function Array()
    ▶ copyWithin: function copyWithin()
    ▶ entries: function entries()
    ▶ every: function every()
    ▶ fill: function fill()
    ▶ filter: function filter()
    ▶ find: function find()
    ▶ findIndex: function findIndex()
    ▶ flat: function flat()
    ▶ flatMap: function flatMap()
    ▶ forEach: function forEach()
    ▶ includes: function includes()
    ▶ indexOf: function indexOf()
    ▶ join: function join()
    ▶ keys: function keys()
    ▶ lastIndexOf: function lastIndexOf()
      length: 0
    ▶ map: function map()
    ▶ pop: function pop()
    ▶ push: function push()
    ▶ reduce: function reduce()
    ▶ reduceRight: function reduceRight()
    ▶ reverse: function reverse()
    ▶ shift: function shift()
    ▶ slice: function slice()
    ▶ some: function some()
    ▶ sort: function sort()
    ▶ splice: function splice()
    ▶ toLocaleString: function toLocaleString()
    ▶ toSource: function toSource()
    ▶ toString: function toString()
    ▶ unshift: function unshift()
    ▶ values: function values()
```

直接去掉（）和开头的[[改写代码得到flag

转载于:<https://www.cnblogs.com/wosun/p/11505931.html>