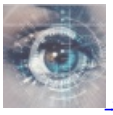
XCTF攻防世界 Web高手进阶区 NaNNaNNaNNaN-Batman writeup

原创

Senimo_ 于 2020-03-30 14:30:22 发布

分类专栏： 各CTF平台 Writeup 文章标签： web XCTF攻防世界 Web高手进阶区 writeup NNaNNaN-Batman

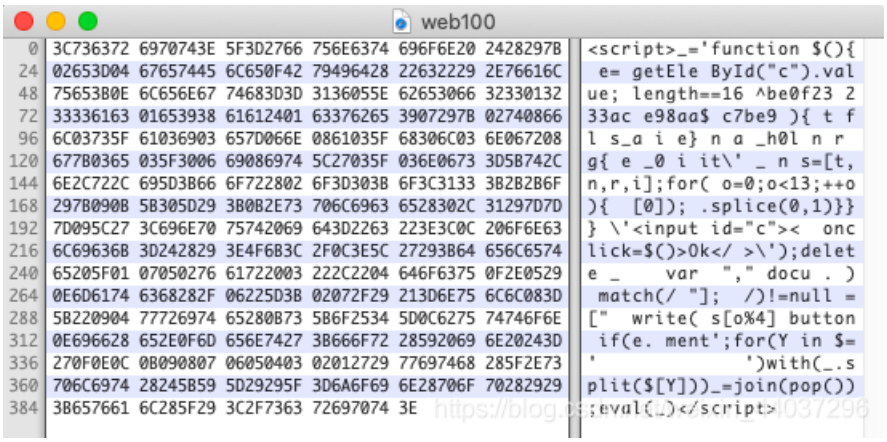


XCTF攻防世界 Web高手进阶区 NaNNaNNaNNaN-Batman writeup

NaNNaNNaNNaN-Batman
难度系数： 2.0
题目来源： tinyctf-2014
题目描述：暂无
题目附件： 附件1

下载附件，解压得到：`web100`文件：

因为没有文件后缀名，放入到**Hex Fiend**中查看：



可以看到其中有`<script>`标签，填上后缀名`.html`，使用浏览器打开：

得到一个输入框，查看网页源码：

```
// 经整理后的源码：

function $(){
var e=document.getElementById("c").value;
if(e.length==16)
 if(e.match(/^be0f23/)!=null)
  if(e.match(/233ac/)!=null)
   if(e.match(/e98aa$/)!=null)
    if(e.match(/c7be9/)!=null){
     var t=["fl","s_a","i","e}"];
     var n=["a","_h0l","n"];
     var r=["g{","e","_0"];
     var i=["it'","_","n"];
     var s=[t,n,r,i];
     for(var o=0;o<13;++o){
      document.write(s[o%4][0]);s[o%4].splice(0,1)
      }
     }
    }
    document.write('<input id="c"><button onclick=$()>Ok</button>');
```

方法一：

满足给出的正则表达式，`^`为开始，`$`为结束，即构造：

```
be0f(23)233ac(c)7b(e9)e98aa
be0f233ac7be98aa
```

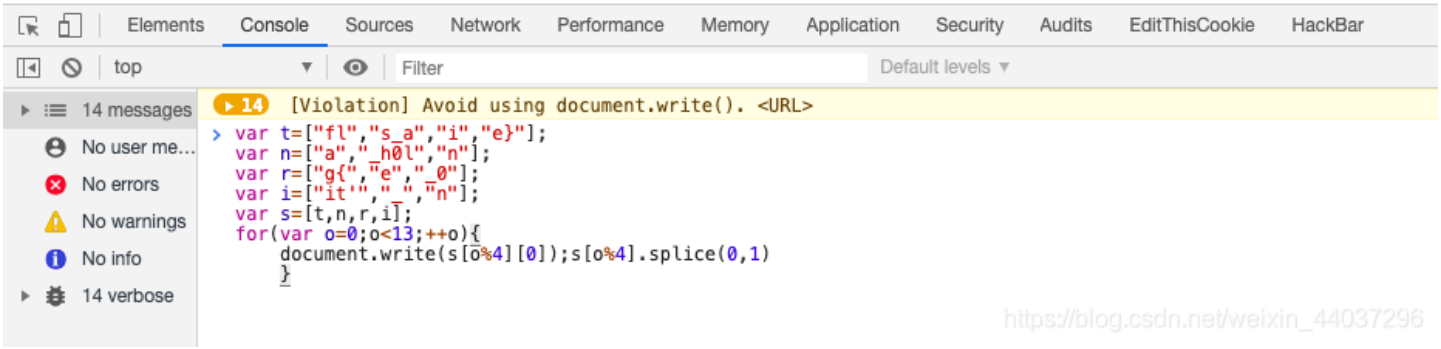
去掉拼接完`()`中的字符串，将其长度控制在`16`位，输入字符串，得到`flag`：

flag{it's_a_h0le_in_0ne}

方法二：

因为输入的字符串由`JavaScript`判断，所以直接在控制台执行结果的代码即可：

```
var t=["fl","s_a","i","e}"];
var n=["a","_h0l","n"];
var r=["g{","e","_0"];
var i=["it'","_","n"];
var s=[t,n,r,i];
for(var o=0;o<13;++o){
 document.write(s[o%4][0]);s[o%4].splice(0,1)
 }
```



在浏览器控制台执行如上代码，得到`flag`：

flag{it's_a_h0le_in_0ne}