【攻防世界】九 --- NaNNaNNaNNaN-Batman

原创

通地塔 于 2020-12-23 20:35:25 发布 85 收藏

分类专栏： 攻防世界 文章标签： 网络安全

本文链接：https://blog.csdn.net/qq_43168364/article/details/111596291

题目 — NaNNaNNaNNaN-Batman

一、writeup

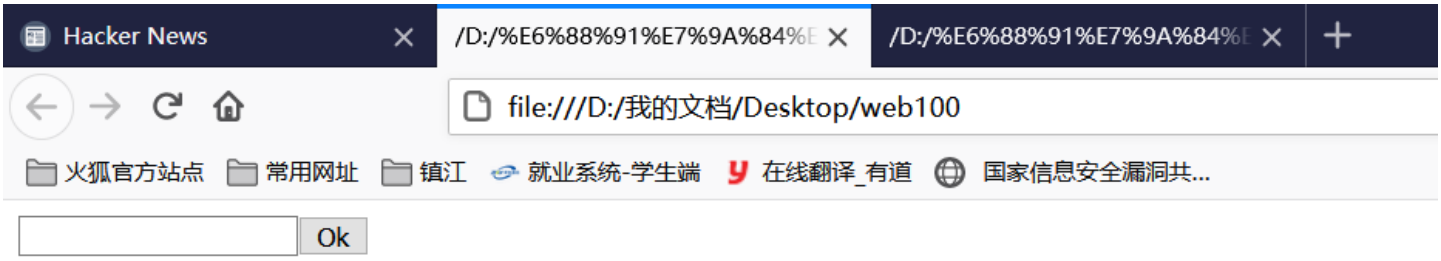
给了一个文件，用sublime打开

```
<script>_='function $(){<0x02>e=<0x04>getEle<0x0f>ById("c").value;<0x0e>length==16<0x05>^be0f2
3<0x01>233ac<0x01>e98aa$<0x01>c7be9<0x07>){<0x02>t<0x08>fl<0x03>s_a<0x03>i<0x03>e}<0x06>n
<0x08>a<0x03>_h0l<0x03>n<0x06>r<0x08>g{<0x03>e<0x03>_0<0x06>i<0x08>it\'<0x03>_<0x03>n<0x06>s=[
t,n,r,i];for(<0x02>o=0;o<13;++o){  <0x0b>[0]);<0x0b>.splice(0,1)}}}    \'<input
id="c"><<0x0c> onclick=$()>Ok</<0x0c>>\');delete _<0x01><0x07><0x05><0x02>var
<0x03>","<0x04>docu<0x0f>.<0x05>)<0x0e>match(/<0x06>"];<0x02><0x07>/)!=null<0x08>=["
<0x04>write(<0x0b>s[o%4]<0x0c>button<0x0e>if(e.<0x0f>ment';for(Y in
$='<0x0f><0x0e><0x0c><0x0b>
<0x08><0x07><0x06><0x05><0x04><0x03><0x02><0x01>')with(_.split($[Y]))_=join(
pop());eval(_)</script>
```


这个文件甚是混乱，整理之后可得以下内容

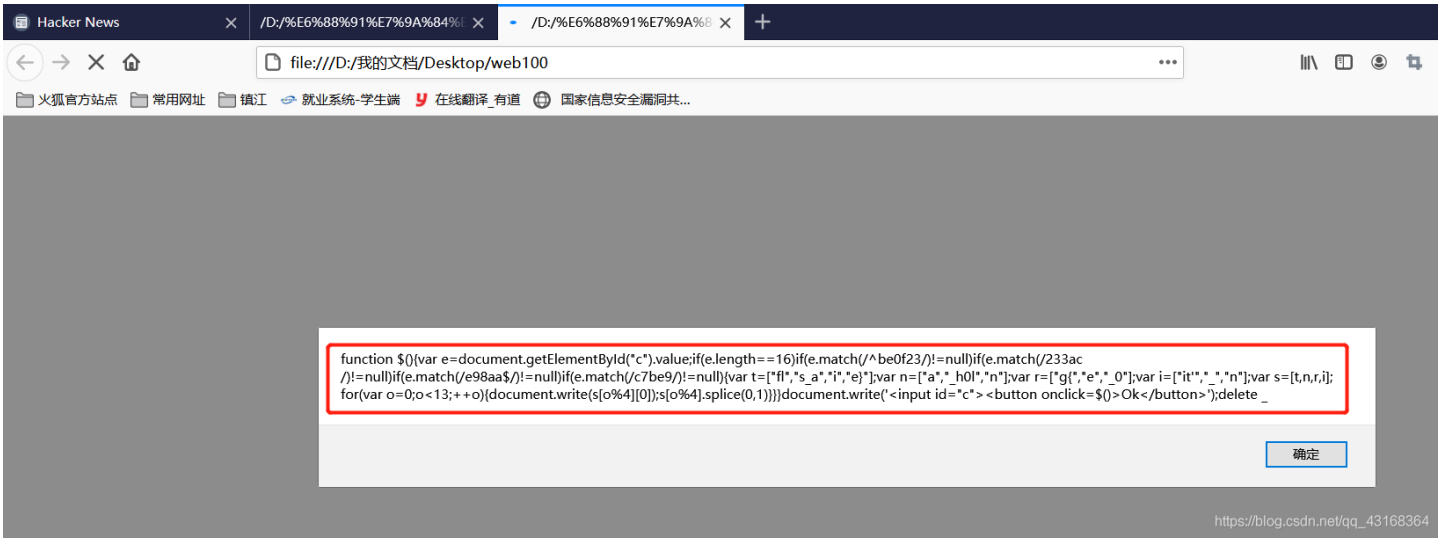
```
<script>
_='function $(){e=getEleById("c").value;length==16^be0f23233ace98aa$c7be9){tfls_aie}na_h0lnrg{e_0iit\'_ns=[t,n,r
,i];for(o=0;o<13;++o){ [0]);.splice(0,1)}}} \'<input id="c">< onclick=$()>Ok</>\');  delete _var ","docu.)match(
/"];/)!=null=[" write(s[o%4]buttonif(e.ment';

for(Y in $=' ')with(_.split($[Y]))_=join(pop());

eval(_)

</script>

//  为乱码无法显示
// _ 为变量名，由三部分组成，1 - 一个名为 $() 的函数，2 - 一个<input>标签，3 - 其他部分
// eval函数执行了 _ 变量中的内容
```

通过**浏览器**打开文件，只显示了**_中的第二部分**内容。函数$()没有被执行（应该是执行了，只不过有乱码），这里不论输入什么都没有反应



仅仅执行了字符串而已（从而导致乱码），因而 html页面 没有任何显示，**只显示了input标签的内容**，但是我们想让源代码正常显示出来，不进行执行，那么，我们就用到了alert弹窗（将eval函数改为alert），将 _ 变量的源码完整显示出来

显示出了源码



代码如下，进行审计

```
function $() {
 var e = document.getElementById("c").value;
 // e的长度是16
 if (e.length == 16)
  // e以 be0f23 开头，以 e98aa 结尾，中间包含 233ac 和 c7be9
  if (e.match(/^be0f23/) != null)
   if (e.match(/233ac/) != null)
    if (e.match(/e98aa$/) != 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>');
delete _
```

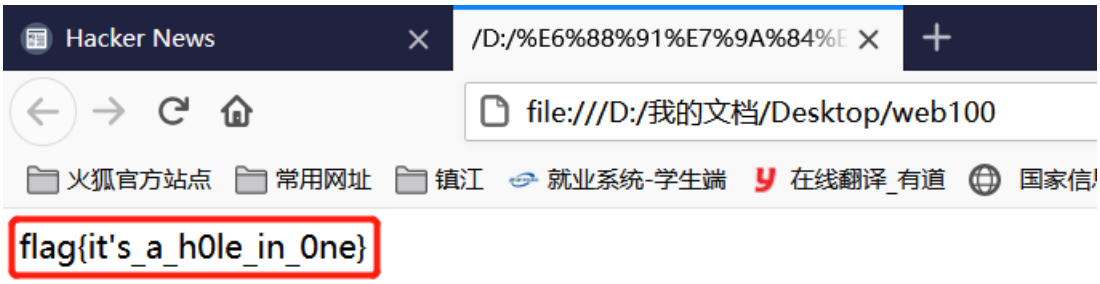
关键点：

- e的长度是16
- e以 be0f23 开头，以 e98aa 结尾，中间包含 233ac 和 c7be9

因此可以构造出e，长度刚好16

```
be0f23    233ac  c7be9   e98aa
be0f      233a   c7b     e98aa
be0f233ac7be98aa
```

再到最初的页面ok一下即可看到flag



二、知识点

- js代码审计