

# 攻防世界web NaNNaNNaNNaN-Batman writeup

原创

[Sprint#51264](#)



于 2020-07-25 14:18:57 发布



85



收藏

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/qq\\_45837896/article/details/107576117](https://blog.csdn.net/qq_45837896/article/details/107576117)

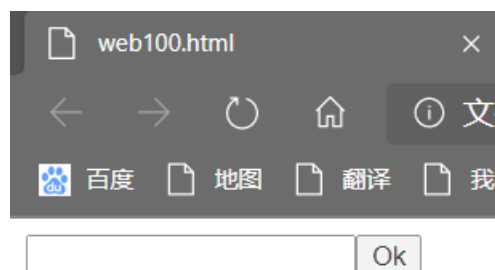
版权

从这个题的题目我们看不出半点东西，下载附件

还是像往常一样加个.txt后缀查看一下

```
write(0x0%4)button;if(e.ment';for(Y in $='0000 000000 0')with(_.split($Y))=join(pop());eval(</script>
```

emm熟悉的乱码，看到script标签决定用html打开



出现一个提交框，f12查看脚本也看不到代码

不过注意到代码最后是有一个eval()函数的

`eval()` 函数:可计算某个字符串,并执行其中的的 JavaScript 代码。

`alert()` 函数:用于显示带有一条指定消息和一个 确定按钮的警告框

把eval改成alert函数可以将完整的代码以弹框的形式展现出来

再次运行

## 此页面显示

```
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=["f","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 _
```

确定

[https://blog.csdn.net/qq\\_45837896](https://blog.csdn.net/qq_45837896)

得到完整的代码段，对其进行整理得

```
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=["f1","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=$()>0k</button>');
delete _
```

意思是对用户在框内进行输入的字符串c进行一系列匹配，如果都有才会显示flag

但是仔细观察if条件，  
该字符串必须以be0f23开头，  
以e98aa结尾，于是乎进行构造得

```
be0f233ac7be98aa
```

在框内进行输入  
得



```
flag{it's_a_h0le_in_0ne}
```