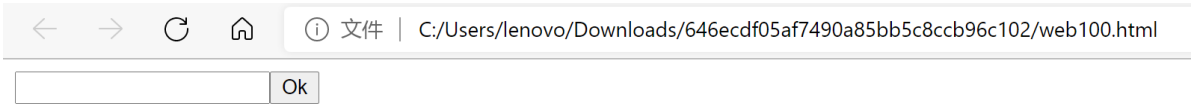
# NaNNaNNaNNaN-Batman

XCTF-web高手进阶区 题目来源：tinyctf-2014

点开题目只给了一个附件，下载之后点开

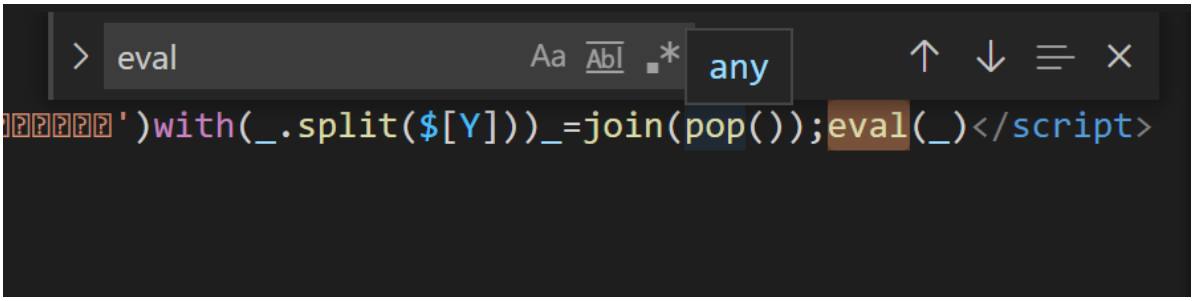

本质上是js代码，不过很多字符显示是乱码（据说用sublime打开可以显示出不太一样的乱码）

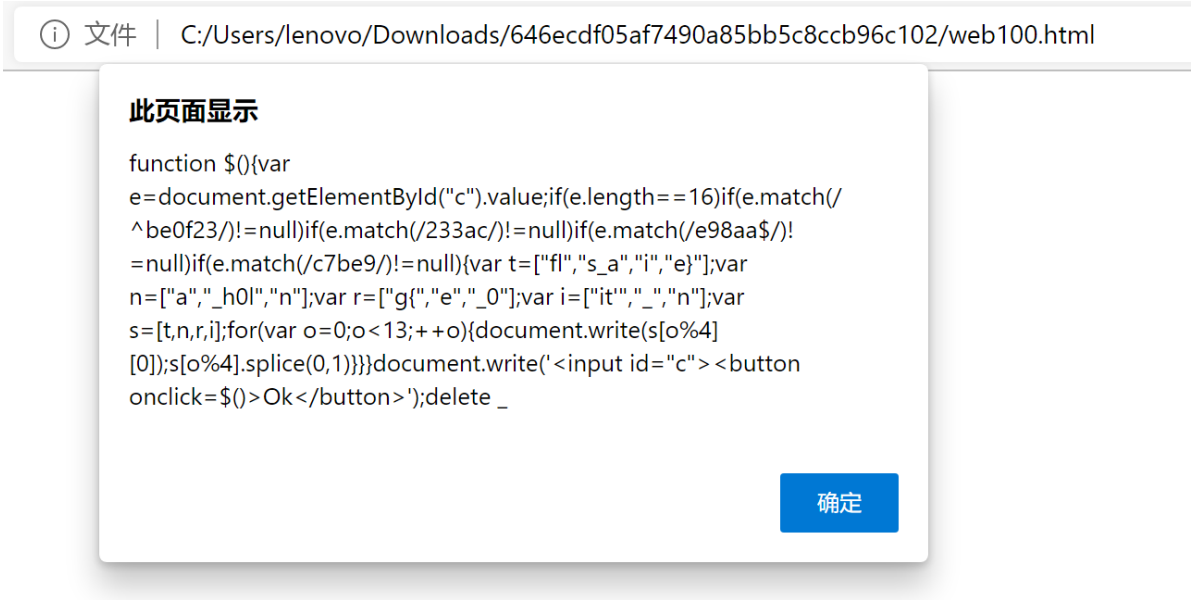
把后缀改成html点开之后发现是个输入框




想办法把代码变成可阅读的状态

**有很多种方法**，我使用的是把eval函数替换成alert




可以完整的看到这段代码的关键部分了。

## 方法一

把代码改回去，进行一下代码阅读可以发现是针对输入进行了一个判断，要满足以下几个条件：

**1、字符长度是16**

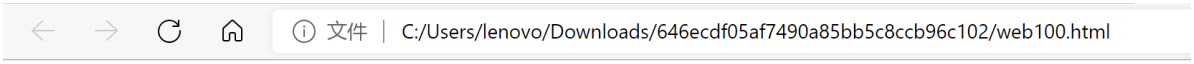
**2、开头是be0f23**

**3、包括233ac**

**4、结尾是e98aa**

**5、包括c7be9**

那么将以上要求拼凑以下就能得到输入的字符串：be0f233ac7be9e98aa

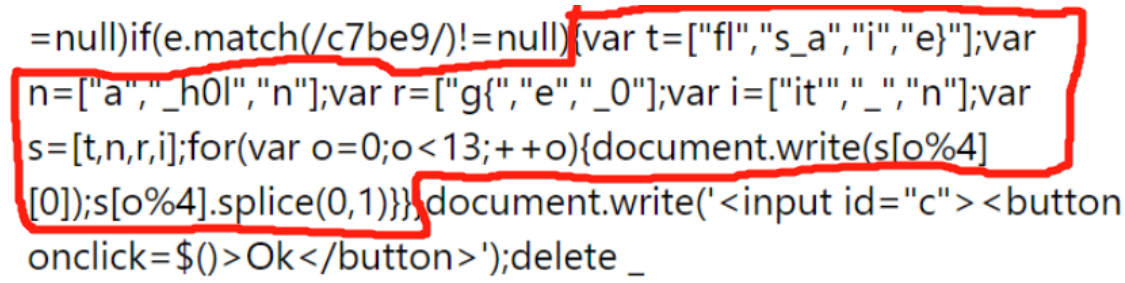



flag{it's_a_h0le_in_0ne}

输入之后点击OK就会显示flag

# 方法二

以上是老实人的方法，不老实的人可以直接通过代码的这个位置进行flag的拼凑




可以看出来是按照t,n,r,i的顺序按序拼接数组中的字符

注：splice() 方法向/从数组中添加/删除项目，然后返回被删除的项目。在这里就是删除读取数组的第一个元素后返回该数组。

拼接好了之后就可以知道字符是：

flag{it's_a_h0le_in_0ne}

# 方法三

当然还有更不老实的方法，就是直接把方法二中圈出来的部分去控制台跑一下，也不用审计了（。

```
<script>
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)}
</script>
```

一些知识点：

为什么*eval*改成*alert*就可以输出正常代码？

答：eval是js的执行函数，会执行代码。这里执行了_变量中的内容也就是''中的内容，但是，要注意的是，它并没有执行$()函数，仅仅执行了字符串而已（从而导致乱码），因而页面html页面没有任何显示，只显示了input标签的内容。
alert则是使用浏览器进行解析。文档中不能显示就是编码的问题，但是虽然编码不一样，这个函数的内容是没有变的，alert的时候直接显示了一个变量内容，可以理解为以能显示的编码显示出来。

也可以改成console.log函数，可以实现同样的显示正常代码的效果