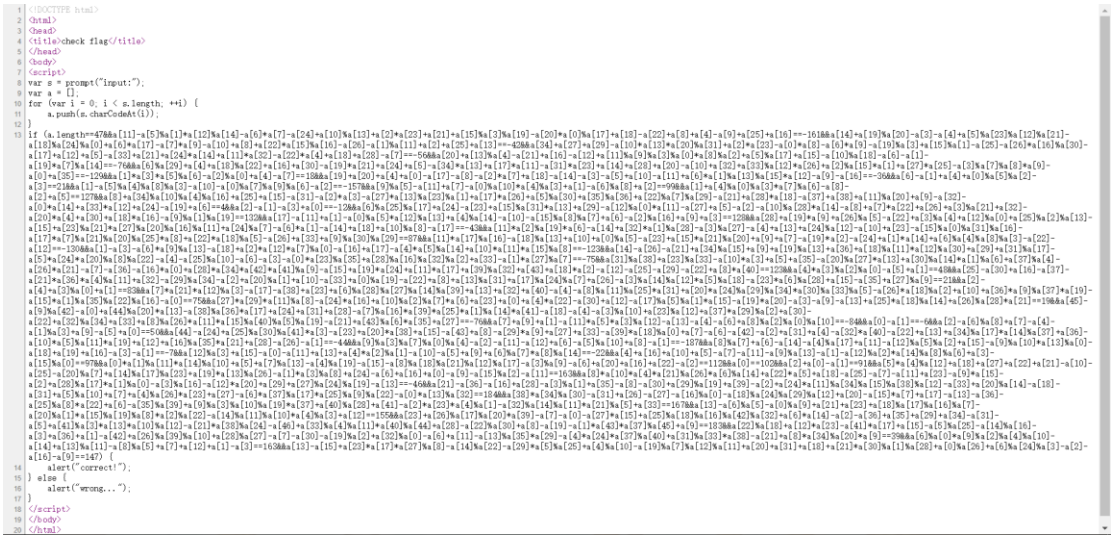
FLAG WriteUp

http://ctf5.shiyanbar.com/qwctf/flag-checker.html

题目为上述链接，打开后弹出如下提示框：

网页相关题，直接看源代码：



乍一看，一大坨代码好像乱码，仔细一看是一个 if 语句，只要输入字符串满足 if 调节即输出 "correct!"

于是我们整理并分析一下 if 语句：

```
var s = prompt("input:");
var a = [];
for (var i = 0; i < s.length; ++i) {
    a.push(s.charCodeAt(i));
}
if (a.length==47&&//
    a[0]==102&&//
    a[0]-a[1]==-6&&//
    a[2]+a[0]-a[1]==91&&//
    a[2]-a[1]-a[3]+a[0]==-12&&//
    a[2]-a[4]+a[3]%a[0]+a[1]==83&&
    a[4]*a[3]%a[2]%a[0]-a[5]+a[1]==48&&
    a[6]-a[1]+a[4]+a[0]%a[5]%a[2]-a[3]==21&&
    a[1]*a[3]*a[5]%a[6]-a[2]%a[0]+a[4]-a[7]==18&&
    a[1]+a[4]%a[0]%a[3]*a[7]%a[6]-a[8]-a[2]+a[5]==127&&
    a[2]-a[6]%a[8]+a[7]-a[4]-a[1]%a[3]+a[9]-a[5]+a[0]==50&&
    a[1]-a[5]%a[4]%a[8]%a[3]-a[10]-a[0]%a[7]%a[9]%a[6]-a[2]==-157&&
    a[9]%a[5]-a[11]+a[7]-a[0]%a[10]*a[4]%a[3]+a[1]-a[6]%a[8]+a[2]==99&&
    a[9]%a[3]%a[7]%a[0]%a[4]-a[2]-a[11]-a[12]+a[6]-a[5]%a[10]+a[8]-a[1]==-187&&
    a[7]+a[9]+a[1]-a[11]*a[5]*a[3]%a[12]-a[13]-a[4]-a[6]+a[8]%a[2]%a[0]%a[10]==-84&&
    a[6]%a[0]*a[9]%a[2]%a[4]%a[10]-a[14]+a[13]%a[11]-a[8]%a[5]+a[7]+a[12]+a[1]-a[3]==163&&
    a[12]%a[3]+a[15]-a[0]-a[11]+a[13]+a[4]*a[2]%a[1]-a[10]-a[5]+a[9]+a[6]%a[7]*a[8]%a[14]==-22&&
    a[4]+a[16]+a[10]+a[5]-a[7]-a[11]-a[9]%a[13]-a[1]-a[12]%a[2]*a[14]%a[8]%a[6]+a[3]-a[15]%a[0]==97&&
    a[17]-a[11]+a[1]-a[0]%a[5]*a[12]%a[13]+a[4]%a[14]-a[10]-a[15]%a[8]%a[7]+a[6]-a[2]%a[16]+a[9]+a[3]==128&&
    a[1]-a[3]-a[6]*a[9]%a[13]-a[18]+a[2]*a[12]*a[7]%a[0]-a[16]+a[17]-a[4]*a[5]%a[14]+a[10]*a[11]*a[15]%a[8]==-123&&
    a[8]%a[7]+a[6]-a[14]-a[4]%a[17]+a[11]-a[12]%a[5]%a[2]+a[15]-a[9]%a[10]*a[13]%a[0]-a[18]+a[19]+a[16]-a[3]-a[1]==-7&&
    a[19]+a[20]+a[4]+a[0]-a[17]-a[8]-a[2]*a[7]+a[18]-a[14]-a[3]-a[5]+a[10]-a[11]+a[6]*a[1]%a[13]%a[15]*a[12]-a[9]-a[16]==-36&&
    a[20]+a[13]%a[4]-a[21]+a[16]-a[12]+a[11]%a[9]%a[3]%a[0]*a[8]%a[2]+a[5]%a[17]+a[15]-a[10]%a[18]-a[6]-a[1]-a[19]*a[7]%a[14]==-76&&
    a[0]*a[1]%a[11]*a[14]%a[10]+a[5]+a[7]%a[13]-a[4]%a[19]-a[15]-a[8]%a[18]%a[21]%a[12]%a[17]-a[3]%a[9]-a[6]+a[20]+a[16]+a[22]-a[2]==
    a[13]-a[6]%a[5]-a[0]%a[9]+a[21]+a[23]+a[18]%a[17]%a[16]%a[7]-a[20]%a[1]*a[15]%a[19]%a[8]*a[2]%a[22]-a[14]%a[11]%a[10]*a[4]%a[3]+a
    a[11]*a[17]%a[16]-a[18]%a[13]+a[10]+a[0]%a[5]-a[23]+a[15]*a[21]%a[20]+a[9]+a[7]-a[19]*a[2]-a[24]+a[1]*a[14]+a[6]%a[4]%a[8]%a[3]-a
        a[11]-a[5]%a[1]*a[12]%a[14]-a[6]*a[7]-a[24]+a[10]%a[13]+a[2]*a[23]+a[21]+a[15]%a[3]%a[19]-a[20]*a[0]%a[17]+a[18]-a[22]+a[8]+a
    a[14]+a[19]%a[20]-a[3]-a[4]+a[5]%a[23]%a[12]%a[21]-a[18]%a[24]%a[0]+a[6]*a[17]-a[7]*a[9]-a[10]+a[8]+a[22]*a[15]%a[16]-a[26]-a[1]%
    a[5]*a[4]%a[12]+a[18]+a[27]+a[22]+a[21]-a[10]-a[25]-a[20]%a[7]+a[14]%a[17]%a[23]+a[19]*a[13]%a[26]-a[1]*a[3]%a[8]+a[24]-a[6]+a[16
    a[28]+a[19]*a[9]+a[26]%a[5]-a[22]+a[3]%a[4]+a[12]%a[0]+a[25]%a[2]%a[13]-a[15]+a[23]%a[21]*a[27]%a[20]%a[16]%a[11]+a[24]%a[7]-a[6]
```

详情可见 js.txt。

之后我们可以得出：

1） 用户输入的字符串的长度为 47

2） 后面的条件是一个方程组 (四十七元一次方程组)

我们简单分析一下这个方程组 ，其中我们不难发现 ：

a[0]=102

a[0]-a[1]=-6

a[2]+a[0]-a[1]=91

……

第 n 行的方程组会有 n 个未知数，将第 n 行的方程带入第 n + 1 个方程组中就可以解出一个新的未知数，也就是 a[n - 1]。

每个未知数前面的运算符都是加或减，而不是求余 (这才保证了能有唯一解)。

只要我们一个一个从上往下带入 ，每代入一次就可以解出一个新的未知数，这样一直解下去就可以了。

手动一个个算太复杂，我们可以将括号里的 if 条件当做字符串通过程序处理一下，转成运算式，详情可见 main.py 脚本。

处理生成的运算式生成新的脚本：result.py。运行即得到 flag。