

## 一. 从 0 开始之 XSS challenge0

### Try to alert(1)

```
function charge(input) {  
    var stripTagsRE = /script/gi;  
    input = input.replace(stripTagsRE, '');  
  
    return '<article>' + input + '</article>';  
}
```

`</article><svg/onload=alert(1)<article>`

SSSSSSSSSSSSSuccess!!请带着payload找HeartSky(QQ 869794781)或  
C014(QQ 779041017)

控制台 调试器 样式编辑器 性能 内存 网络

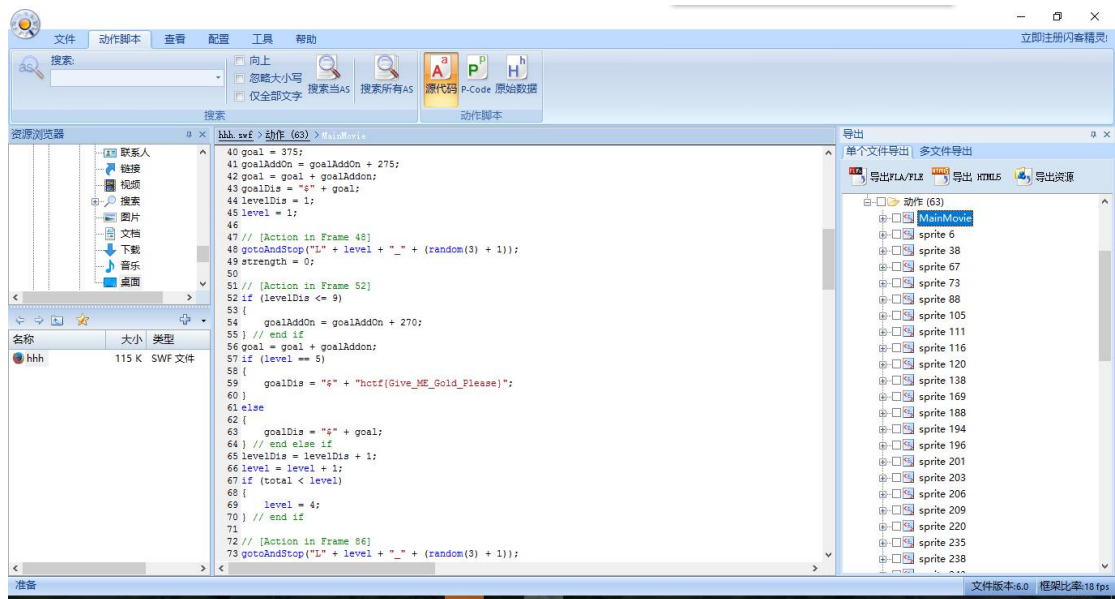
就需要先闭合<article>标签嘛然后使用不含 script 的语句完成 alert 就好了。

## 二. re 从零开始的逆向之旅: Gold Miner

讲真这个真的是童年回忆，然后就开始玩玩到第六关那边金额是 flag 的开头 :



然后用反编译软件查看代码:



Get flag.

审 Wp 的 dalao 鸡年大吉……嗯

Acaleph