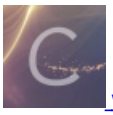
writeup-khaleesi

原创

charlie_heng 于 2016-12-02 10:26:28 发布 256 收藏

分类专栏： web安全



描述：
She is the only surviving child of King Aerys II Targaryen, who was ousted from the Iron Throne during Robert's Rebellion.

题目链接：http://218.2.197.234:2033/index.html

打开页面，先看到khaleesi的图片。。冰与火之歌。。。
先按F12看一下有什么东西，

Yea I know I'm so hot and that can be cause lack of attention<3
Oh my dragons! My beautiful dragons…

有两句话。。意义不明。。。。

看一下页面，发现有一大串js代码，首先有一个字符串数组_0x5e57，然后输出一下发现前两句就是上面的，后面的就是split，substring之类的，把代码复制到sublime那里，然后格式化一下

拉到代码的最下面，发现有一个迷之alert，那里应该是弹flag的地方，先试下直接扔控制台，但是显示有错误，还是老老实实写吧，看了一下if的内容，很多都是直接用_0x5e57里面的东西来调用，然后翻译了一下

```
    if (location["hash"]["substring"](1)["split"](decodeURIComponent("-")))
     {
                var els = new EncryptedLocalSt orage(arr_list["substring"](location["hash"]["substring"](1)
                if (location["hash"]["substring"](1)["split"](decodeURIComponent("-"))[0] == ((7 ^ 15) - 1)
                && location["hash"]["substring"](1)["split"](decodeURIComponent("-"))[1] == (7 ^ 22)) { ale
    };
```

查了下js里面的location，发现是获取#后面的东西，获取之后用"-"来分割成数组

于是就可以构造地址了http://218.2.197.234:2033/index.html#7-17

成功拿到flag

Flag:YouNeedToFallInLoveKhaleesiTobeH4ck3r