**SRC-2022-346 | 麦当劳供应商和商家均存在token未授权直接登陆+token可解密遍历+token设计缺陷**

**处理进度**

* 审核中
* 已确认
* 已修复
* 已忽略

**基本信息**

提交时间：2022-01-25 01:07:51

漏洞类型：Web漏洞

危害等级评定：无影响

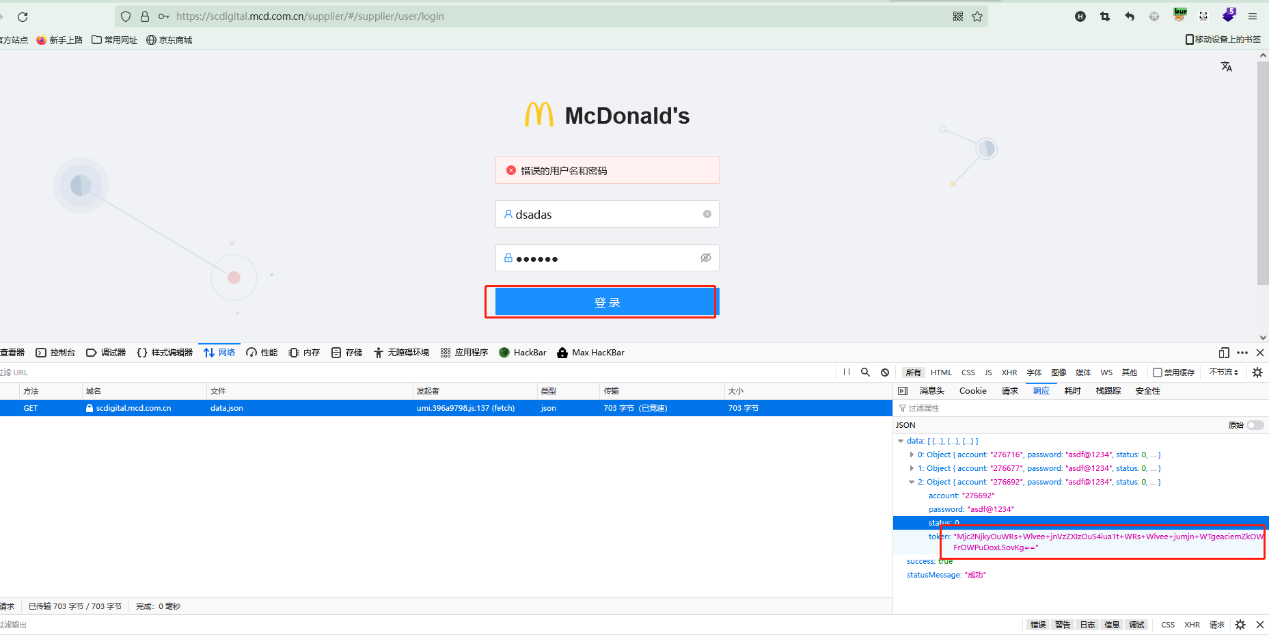
安全币评定：评定中

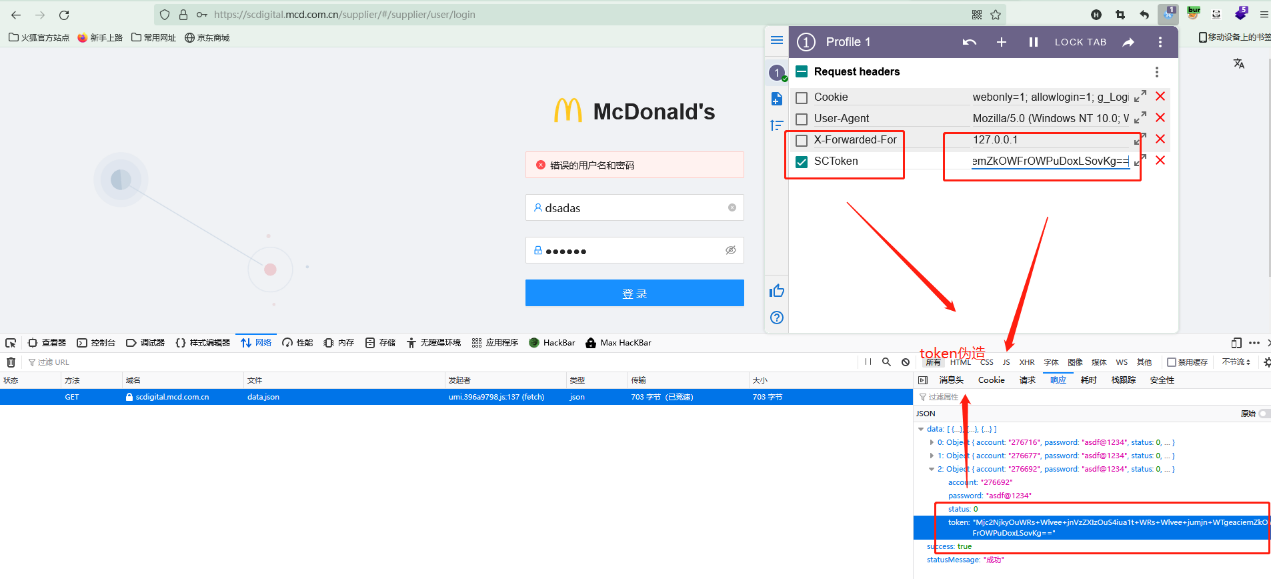
**漏洞详情**

1. 一下两个链接为供应商和商家，均存在此漏洞

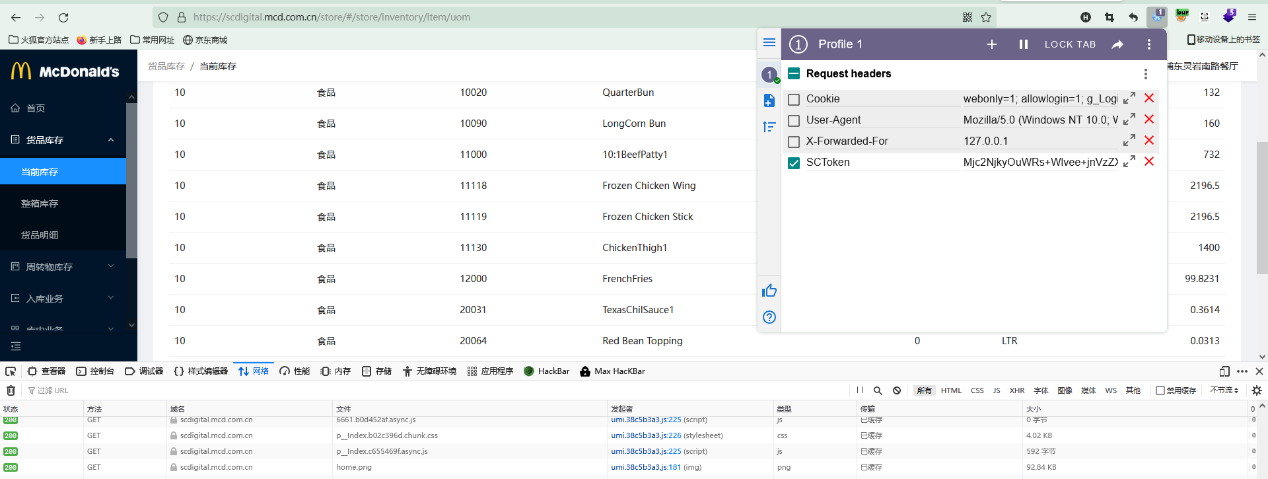
https://scdigital.mcd.com.cn/store/#/store/

https://scdigital.mcd.com.cn/supplier/#/supplier/

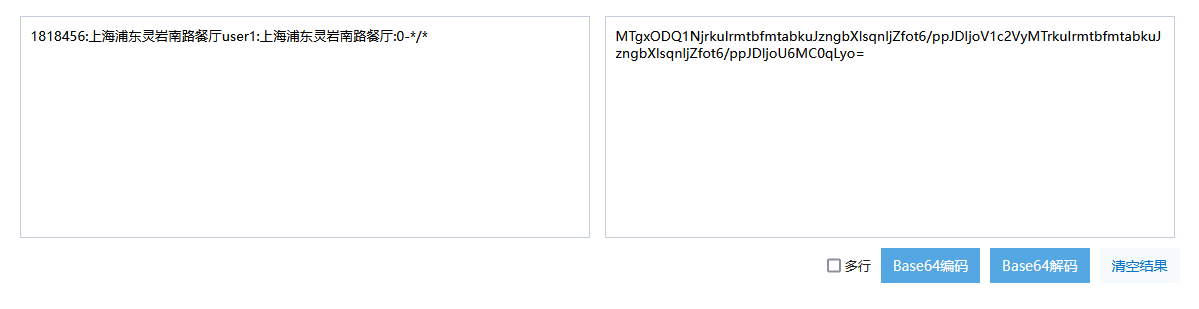
1. 我们在登陆框随便输入账号密码，点击登陆，返回数据里面就有token

2.接下来就是伪造token，我们在请求头里面填上token，但token名要改为SCToken3.

3.把url路径的login改为index，直接访问，发现有商家名，能正常访问库存，token未授权访问成功



3.然后我们来解密遍历token



4.    token能成功通过base64解密出来，id也出来了，我们可以直接遍历token的id来达到爆破登陆的效果

5.最后说一下token设计缺陷

6.我们先用正常token或账号登陆，登陆成功后我们更改token

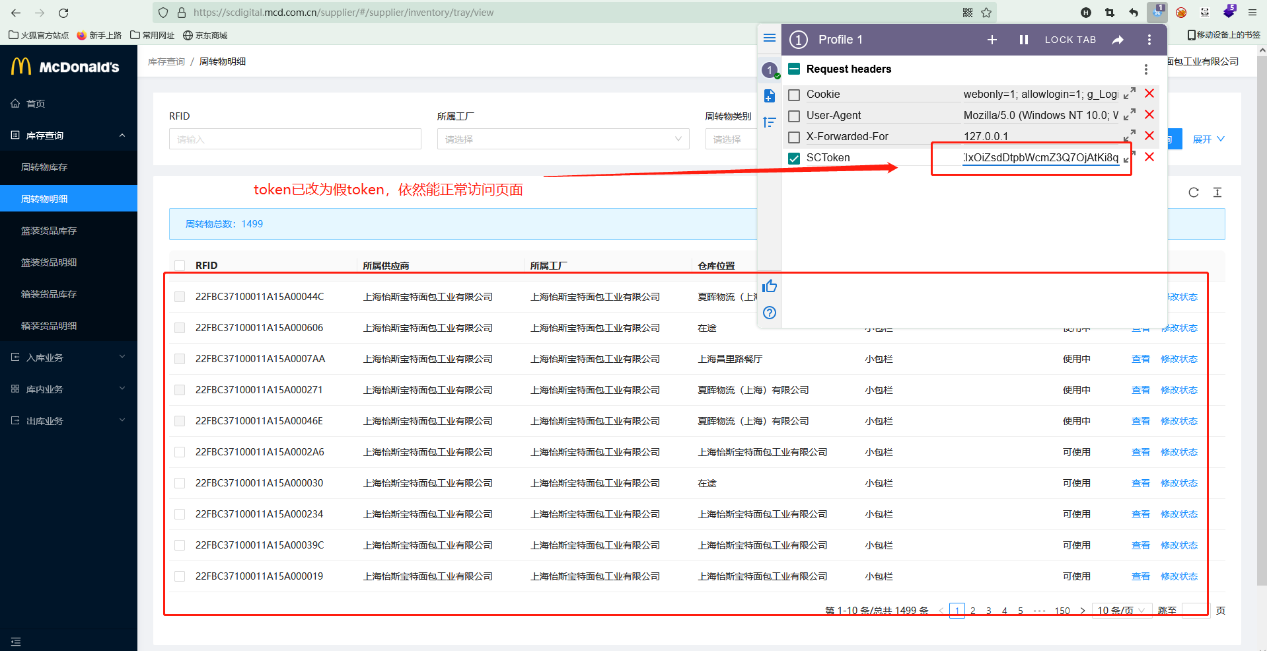
7.token中的商户名称和tokenid可以乱改，我们还是能照常操作

8.下面是我自定义的不存在的token：

    MTombHQ7aW1nJmd0O3VzZXIxOiZsdDtpbWcmZ3Q7OjAtKi8q



9.我们先登陆进后台后，再把正常token替换为此token，依然能正常操作页面



10.这里可能会问，我token值随便改是不是也能正常操作，我试了下是不行的，但是只要按上图给出的规则即可随便伪造并操作页面