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

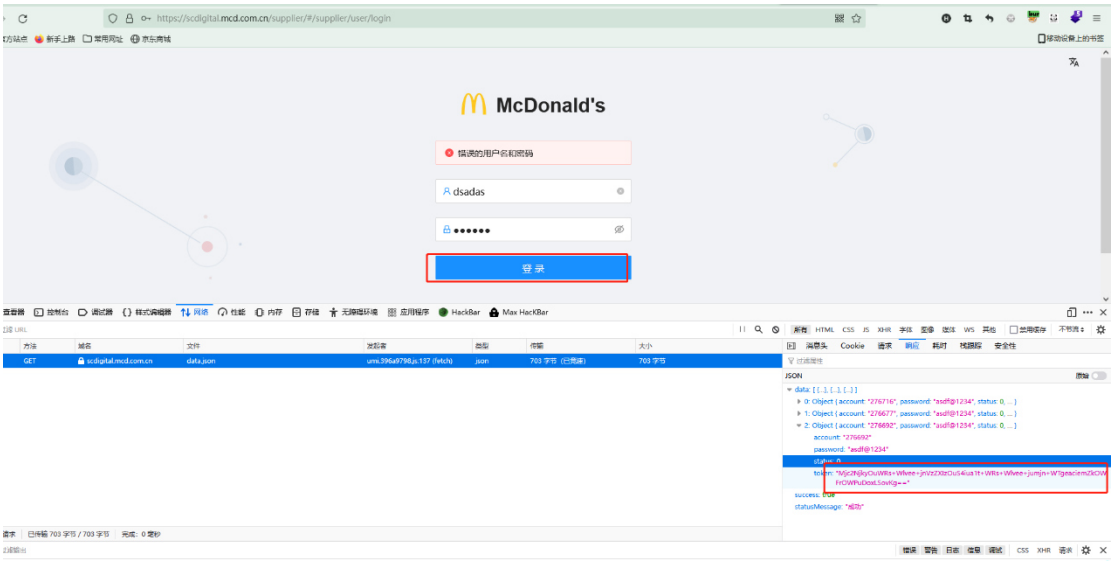
漏洞详情

1. 一下两个链接为供应商和商家，均存在此漏洞

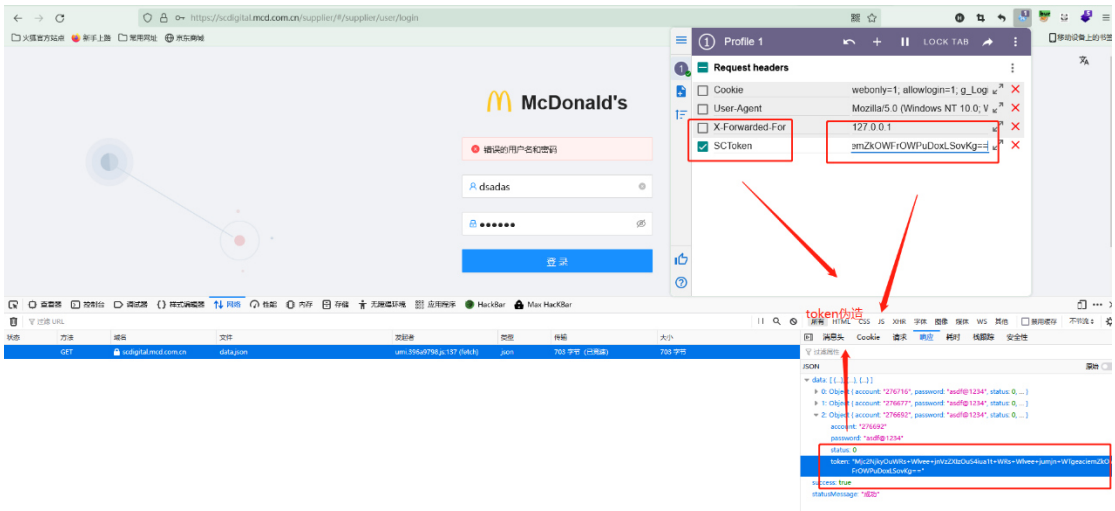
   https://scdigital.mcd.com.cn/store/#/store/

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

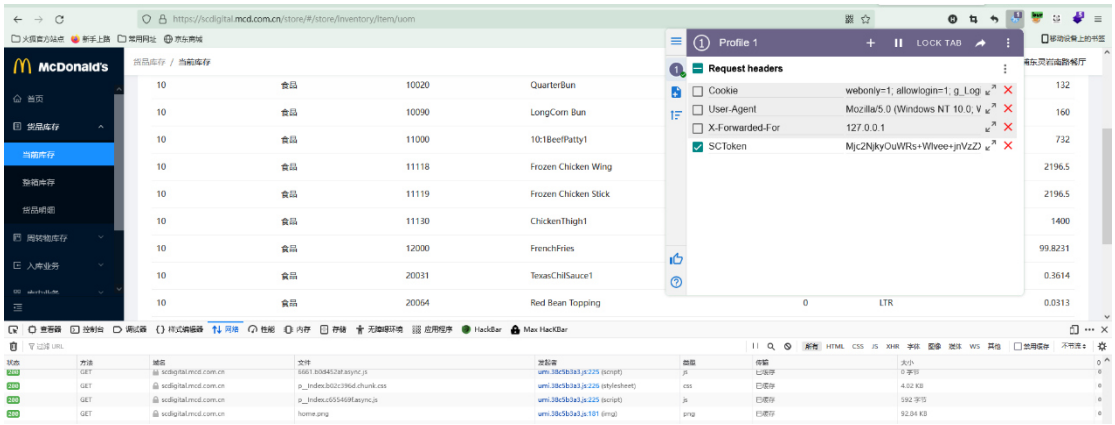
1. 我们在登陆框随便输入账号密码，点击登陆，返回数据里面就有 token



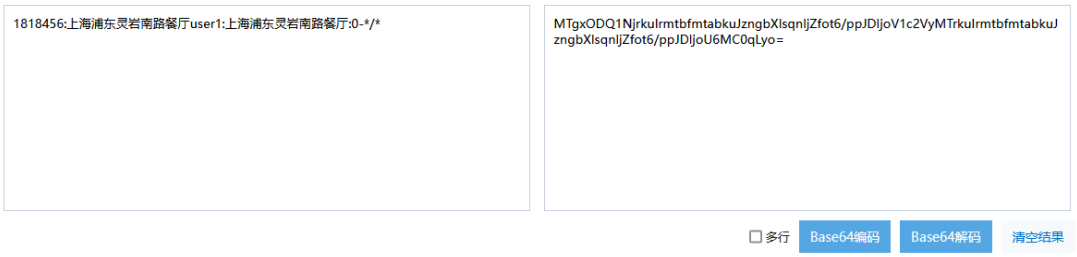
2. 接下来就是伪造 token，我们在请求头里面填上 token，但 token 名要改为 SCToken3.



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

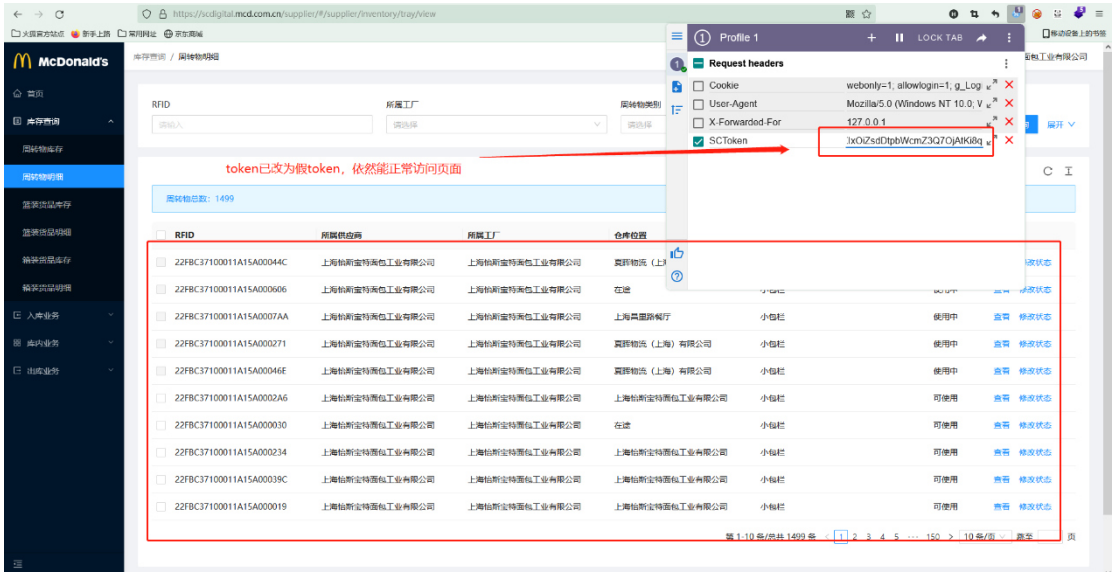
6. 我们先用正常 token 或账号登陆，登陆成功后我们更改 token

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：

MTombHQ7aW1nJmdOO3VzZXIxOiZsdDtpbWcmZ3Q7OjAtKi8q

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