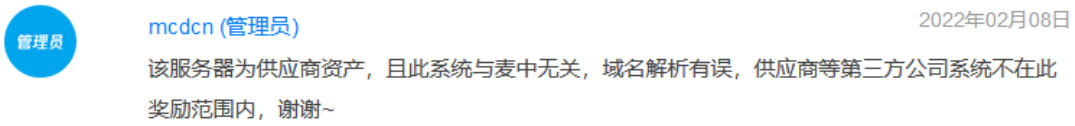
SRC-2022-600 | 麦当劳餐厅云鼎智能系统存在任意用户登陆漏洞

处理进度

- 审核中
- 已确认
- 已修复
- 已忽略



-

基本信息

提交时间：2022-01-29 15:02:40

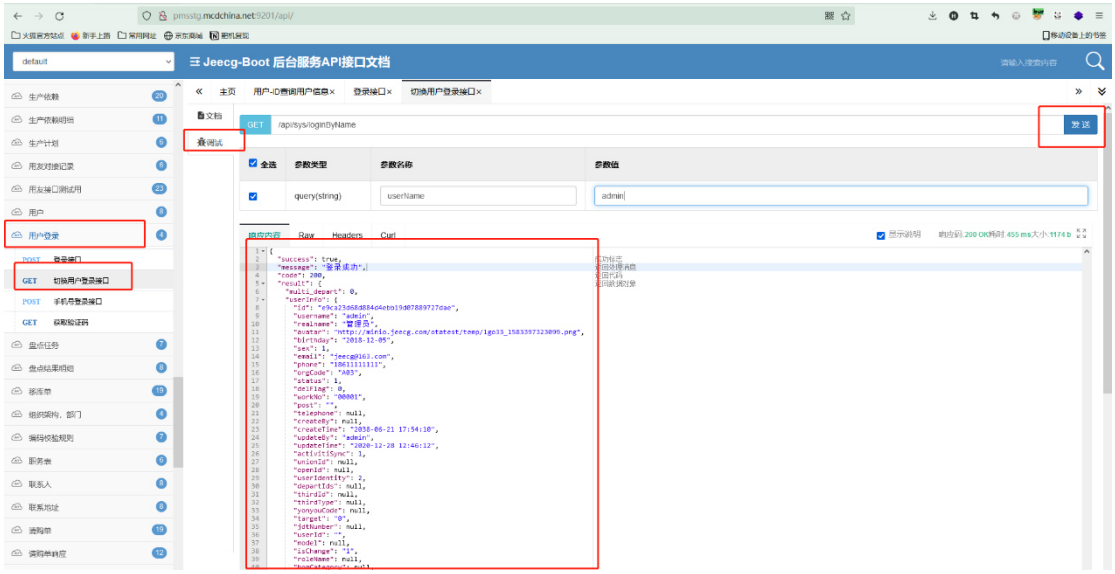
漏洞类型：默认分类

危害等级评定：无影响

安全币评定：评定中

漏洞详情

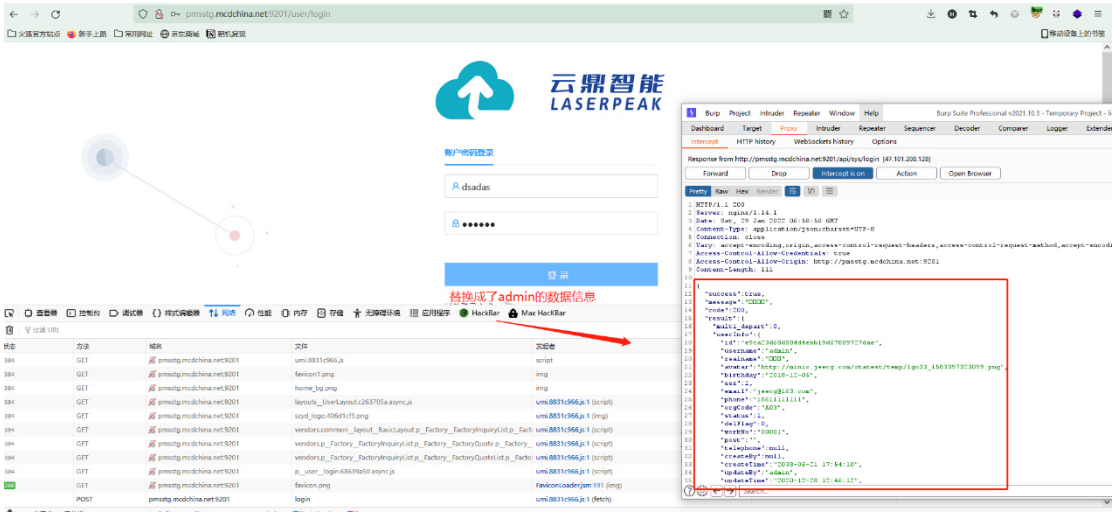
1. 漏洞 url:http://pmsstg.mcdchina.net:9201
2. 我们先来到：http://pmsstg.mcdchina.net:9201/api/
3. 第一步，找到用户登陆->切换用户登陆口->调试->在参数值里面输入 admin->点击发送，最后就会返回 admin 的数据信息



4. 第二步，我们复制 admin 的数据信息，来到登陆口

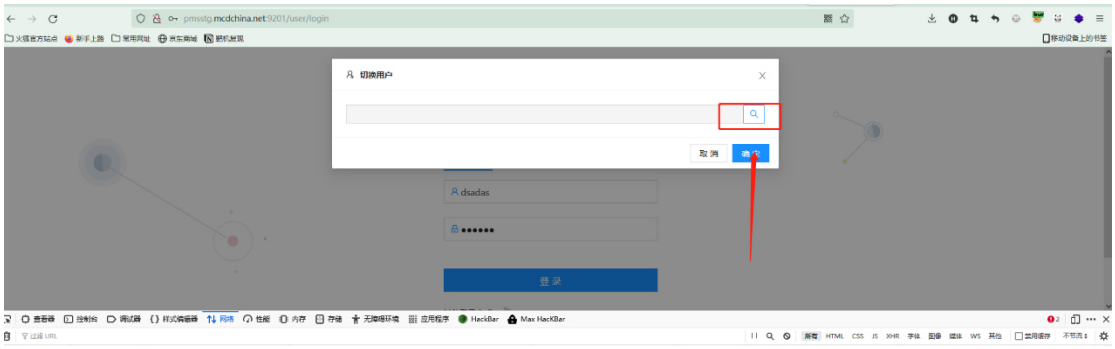
5. 随便输入账号密码，点击登陆并抓包，我们抓取返回包

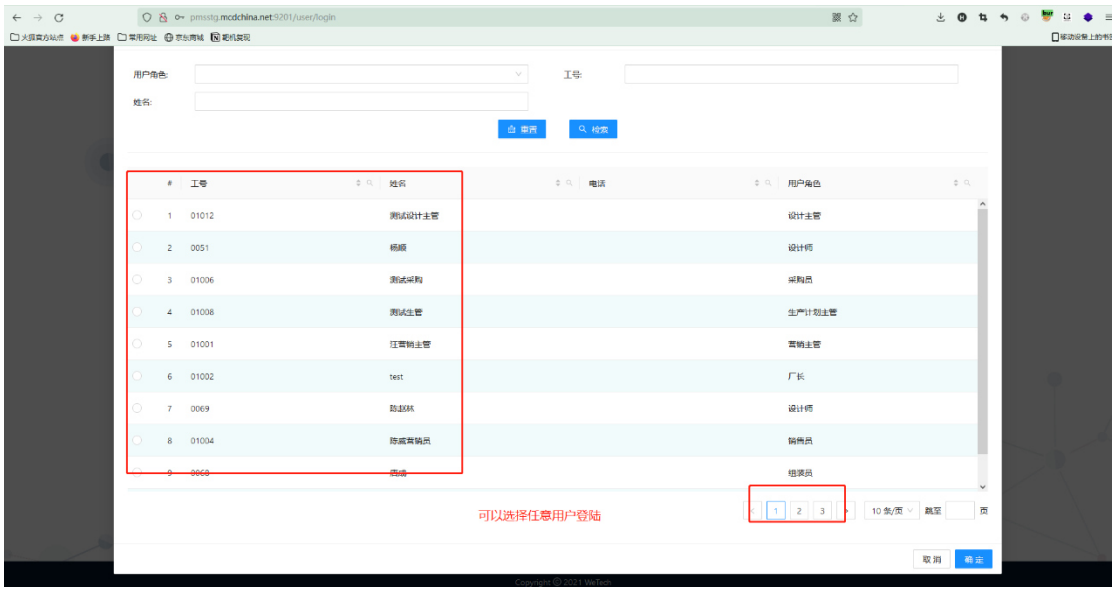
6. 把返回包的数据替换成 admin 的数据信息



7. 点击放大镜，就能开始选择登陆的角色，这里可以选择任意角色登陆

8. 我就选择厂长角色登陆，最后成功登陆





9. 成功登陆！！