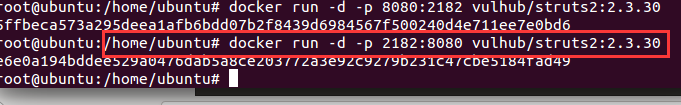
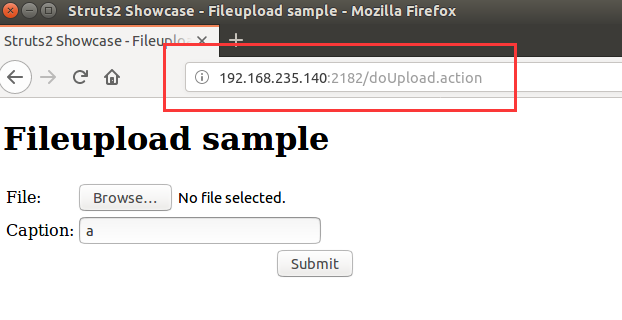
**一：环境配置**

**Step1：打开docker,开启**vulhub/struts2:2.3镜像

dockers run -d -p 8080:8080 vulhub/struts2:2.3 启动镜像容器，映射本地的2182端口。

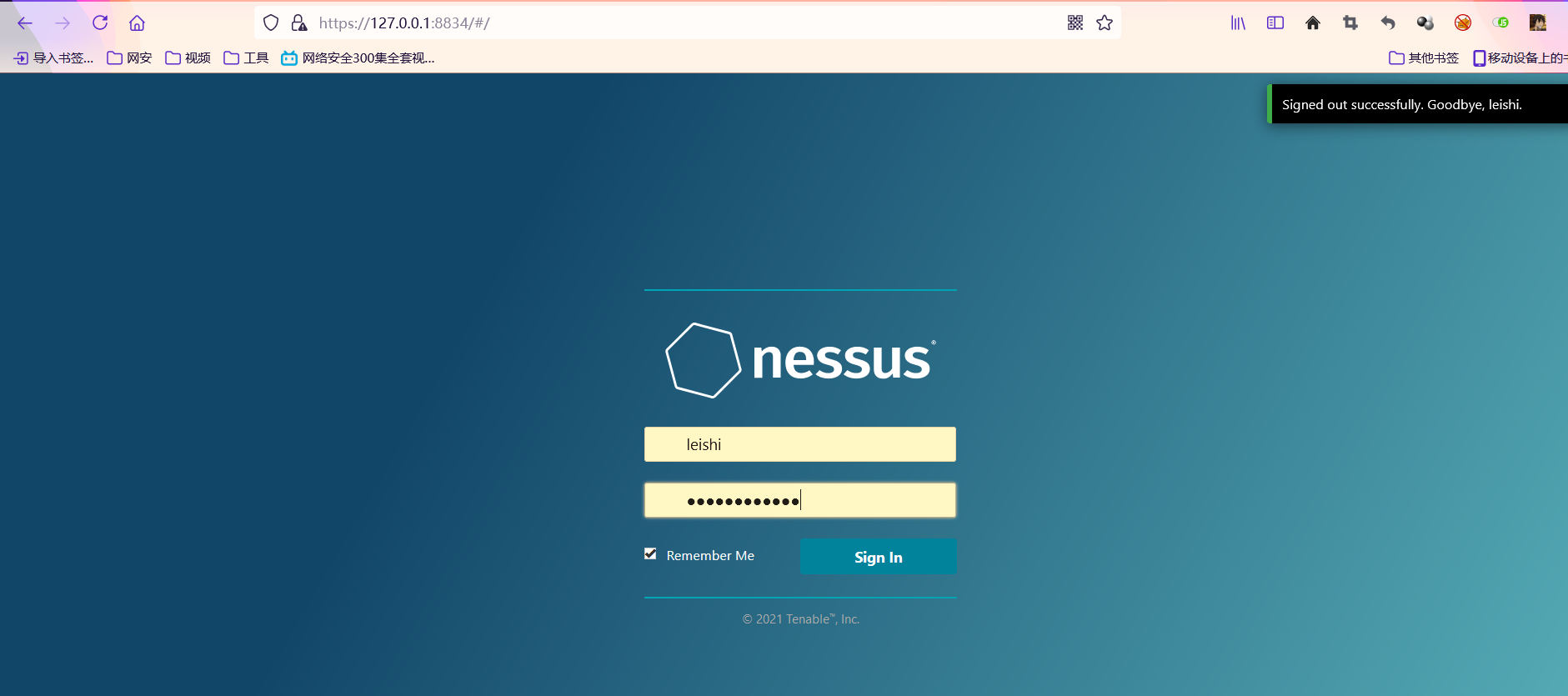


**Step2:查看能否访问端口**

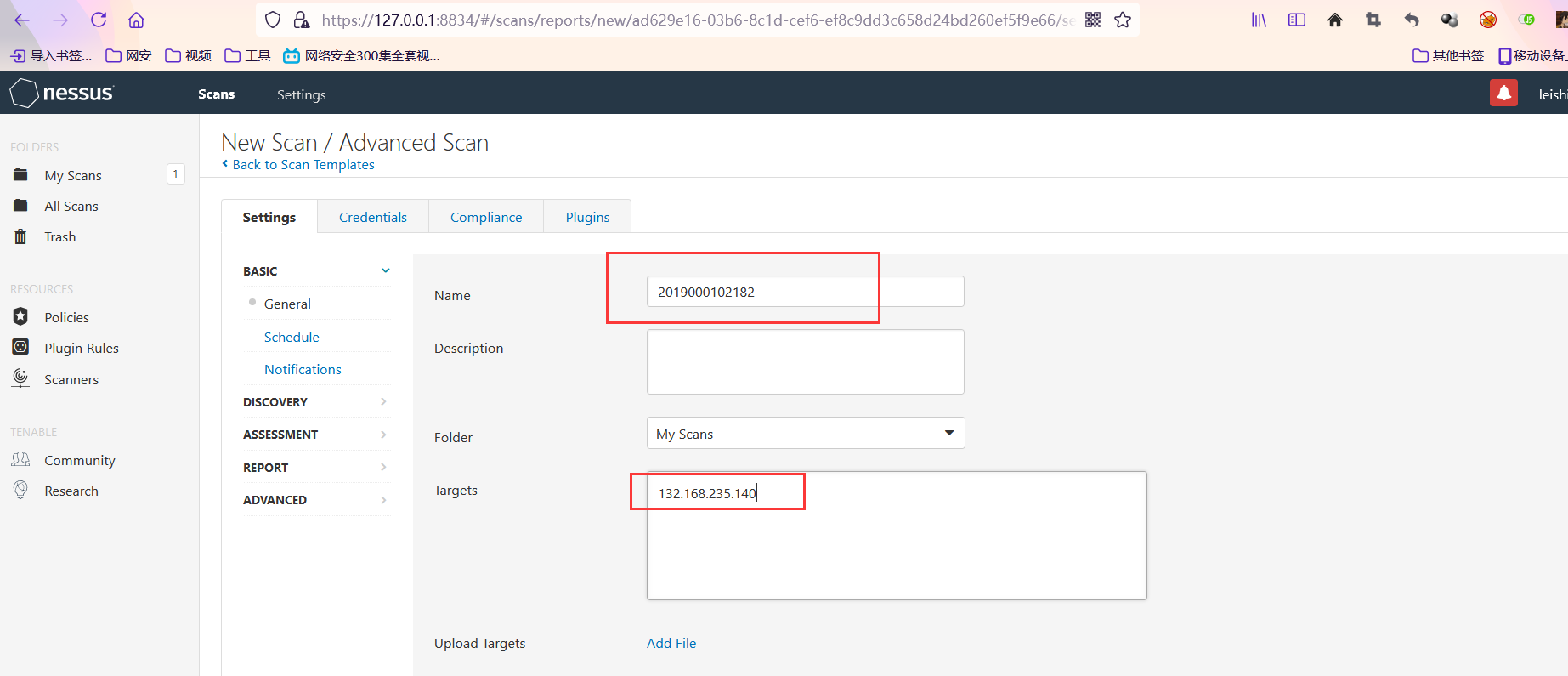


**三：Nessus扫描**

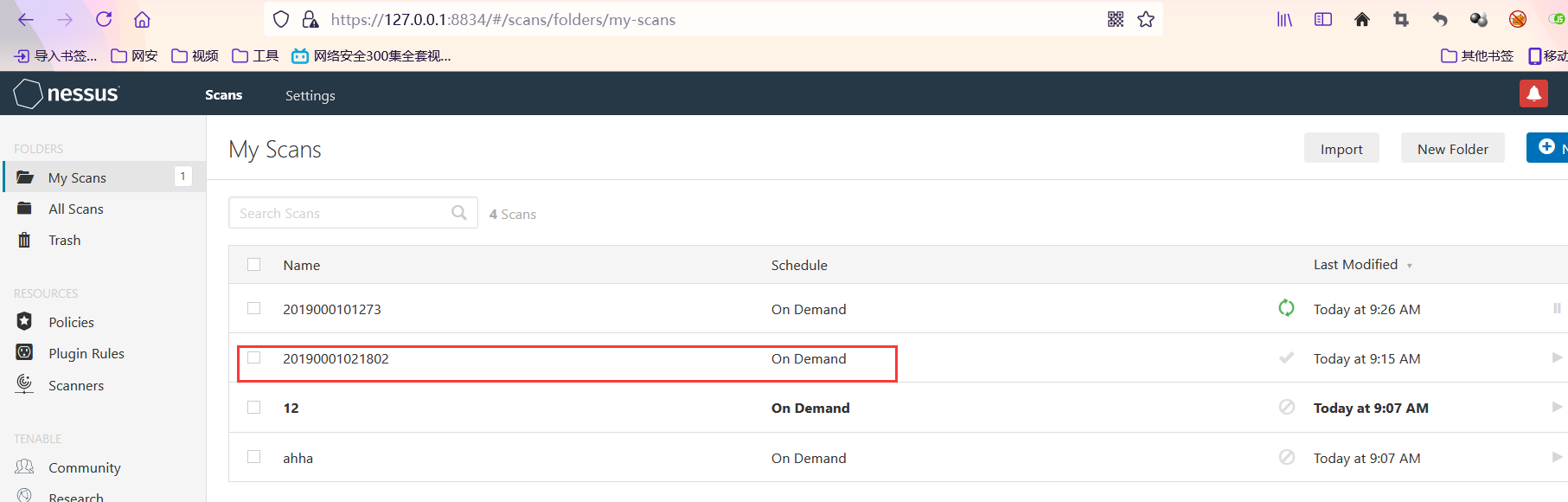
1. 登录窗口



# 2.点击New Scan / Advanced Scan



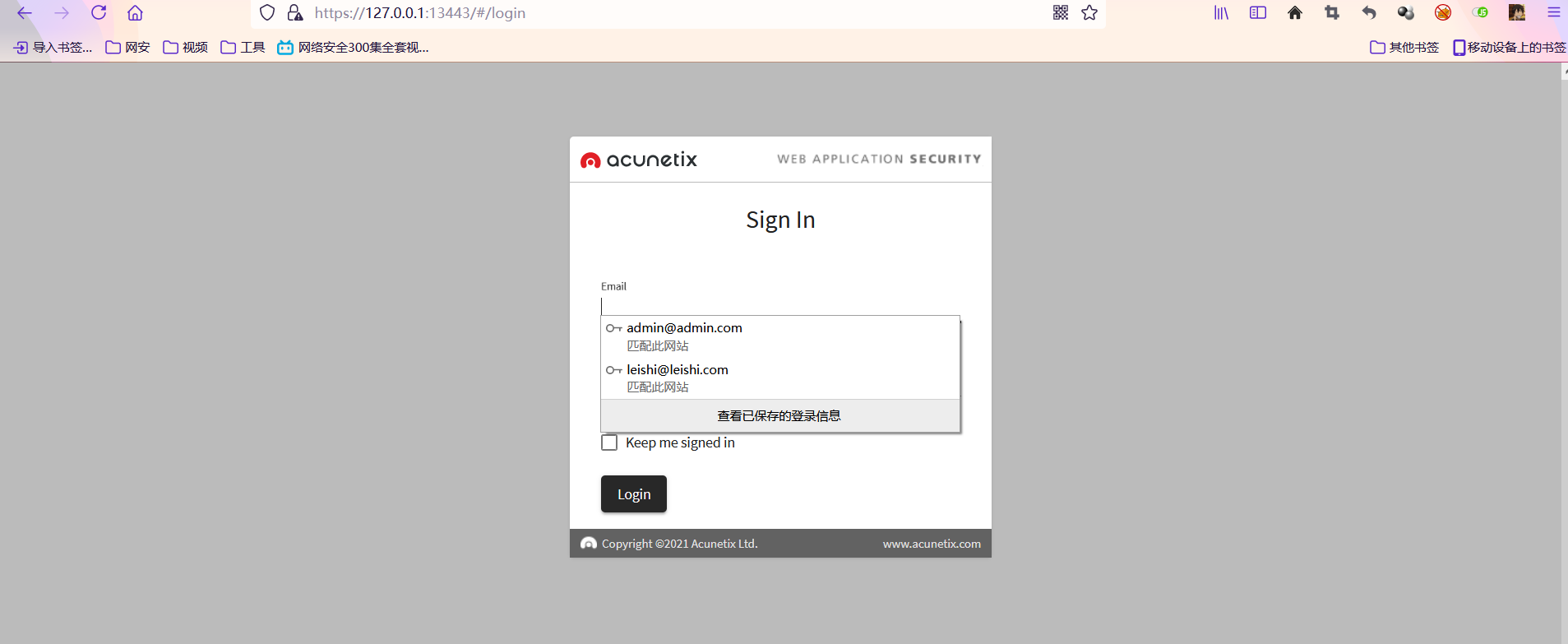
**3.开始扫描**



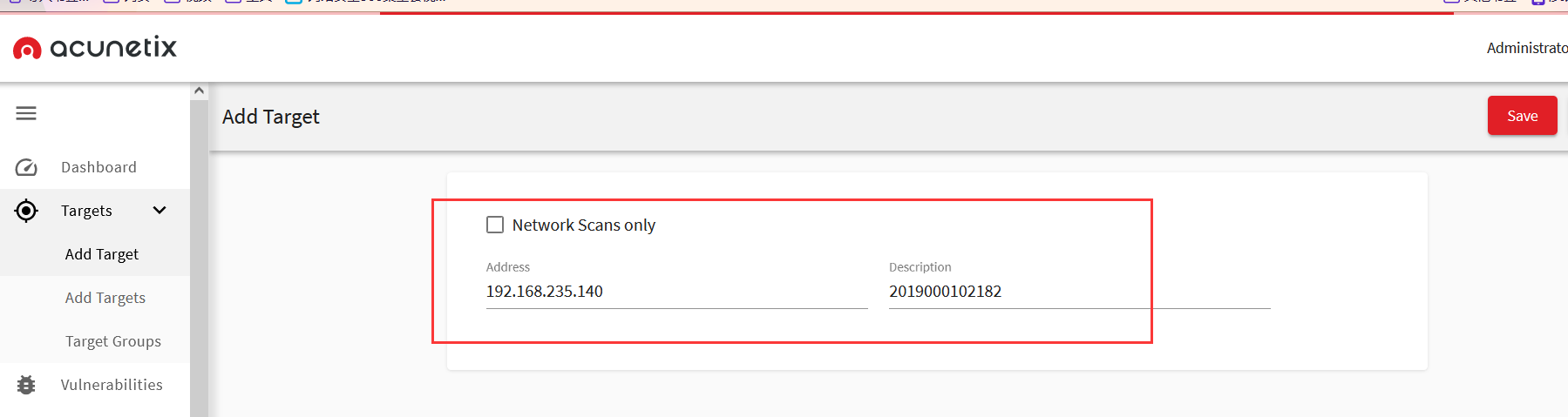
**4.不知为何原因，cve-2017-5638没有扫出来**

**四：Awvs扫描**

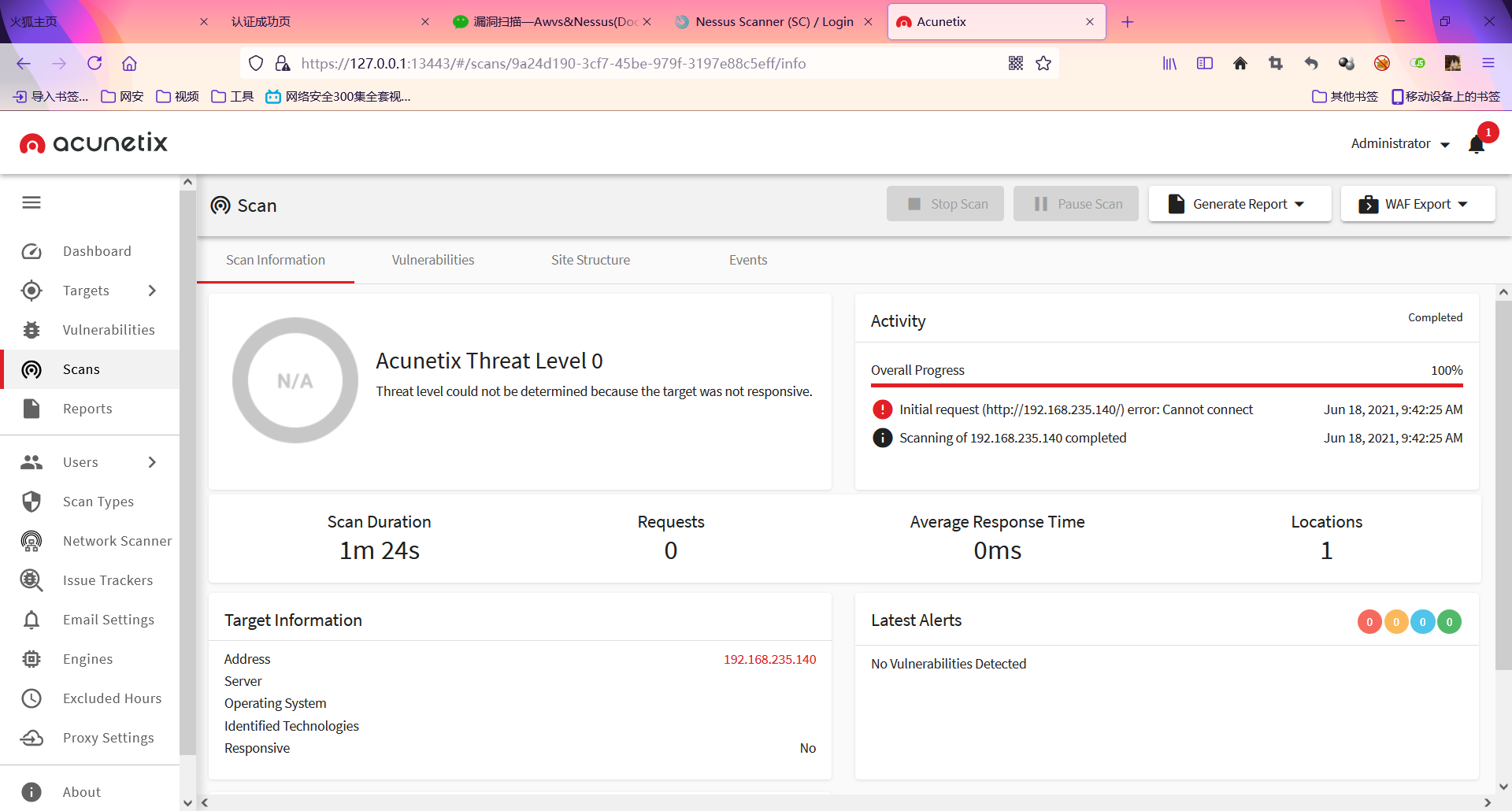
1. **打开awvs**



**2.建立攻击目标**



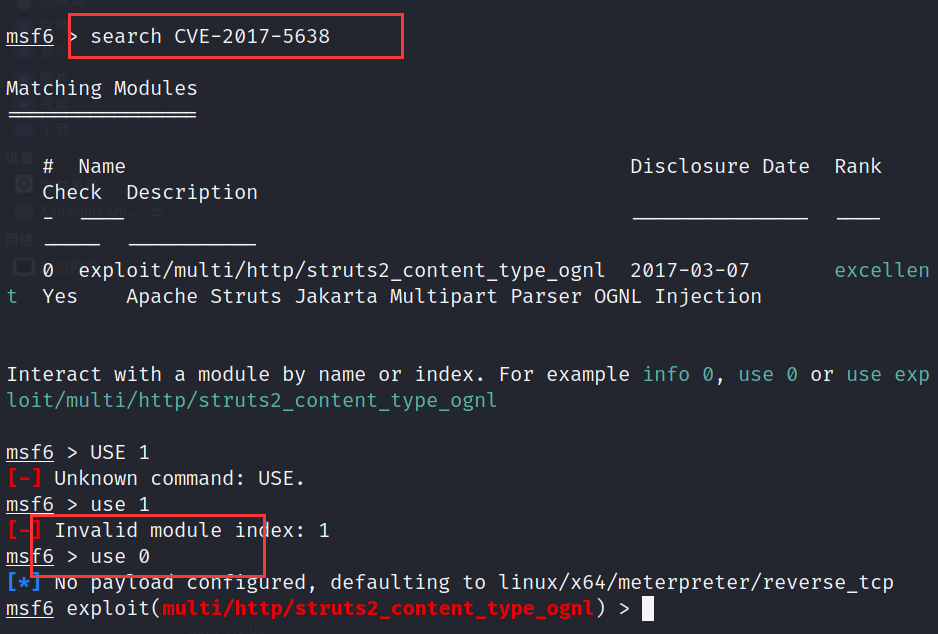
1. **不知道是少了什么插件，同样的配置，但其他同学能扫出来，但我的却扫不出，由于考试时间有限，扫描结果就不说了**

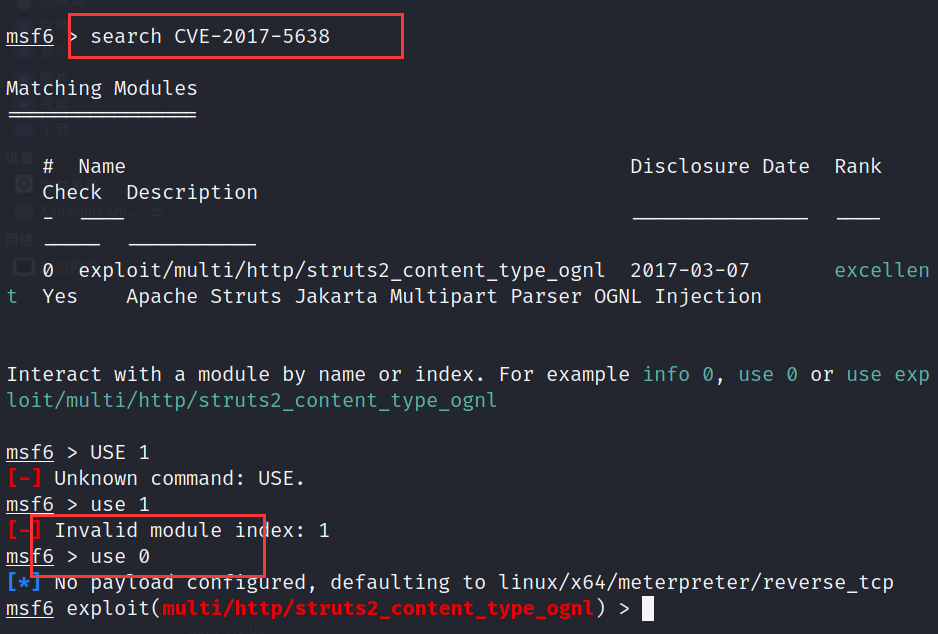


**五：漏洞利用**

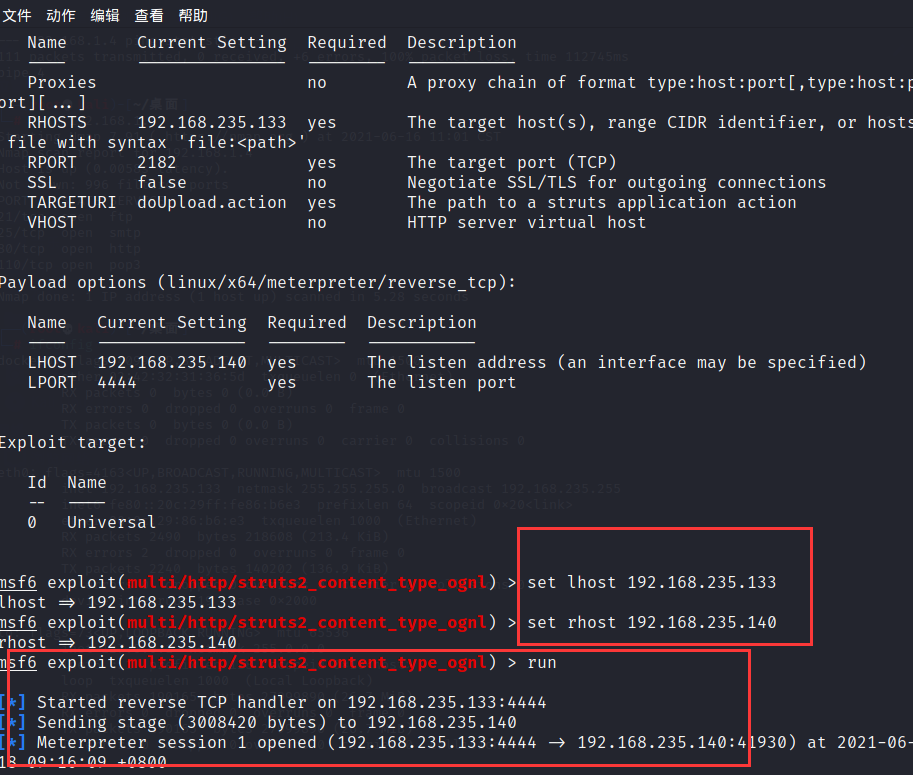
**1.扫描主机，查看是否存在CVE-2017-5638漏洞**

**2.打开kali的metasploit工具来攻击**

1. 直接搜索CVE-2017-5638漏洞模块
2. ****
3. **选择模块** use exploit/multi/http/struts2\_content\_type\_ognl

****

1. **Show options:配置攻击参数**

****

**5.成功**

