## EdgeGallery v1.1 Spirnt2渗透测试记录

## EdgeGallery v1.1 Sprint2 Penetration Test Record

**Sprint 2：**

[【ATP】ATP测试用例扩充到总数14个](https://gitee.com/OSDT/dashboard?issue_id=I2NU9C)

测试用例：信息收集（暂无测试用例）

测试方法：尽可能收集应用详细/敏感信息。

测试过程：

应尽可能少的暴露安全措施细节（如使用的工具名称）。  
暴露扫描工具名称可能导致攻击者①寻找该工具是否存在已知漏洞，②自行安装相同工具提前扫描来研究绕过该项测试的方法。  
建议病毒扫描用例中不要显示扫描工具名称“xxx”

**测试结论**：**Not PASS**

**不通过原因：应用暴露了过多的安全措施细节。**

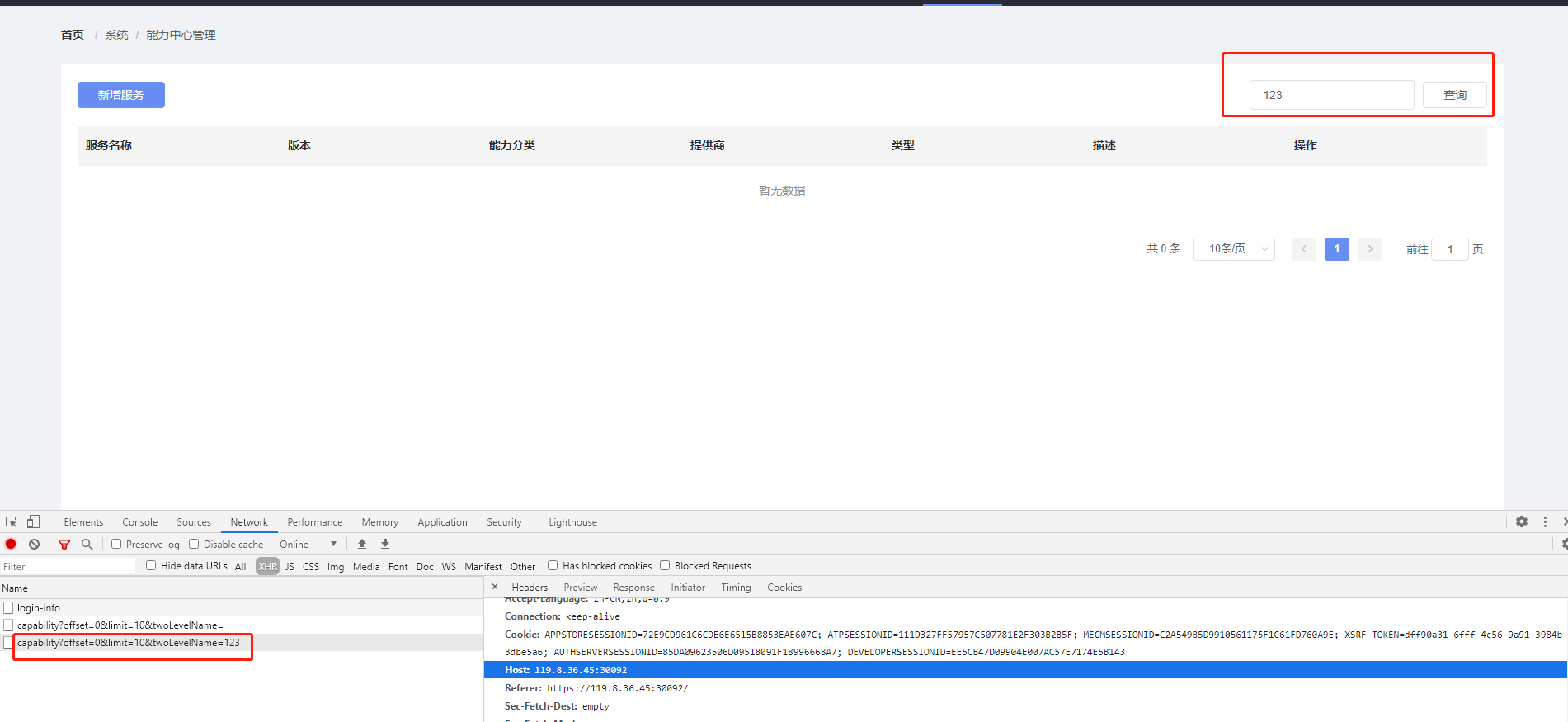
[【developer】支持能力中心管理](https://gitee.com/OSDT/dashboard?issue_id=I2EDOC)

[【developer】支持配置沙箱环境](https://gitee.com/OSDT/dashboard?issue_id=I2EDO1)

测试用例：SQL注入

测试方法：由于该页面有后台查询功能，所以使用sqlmap尝试进行SQL注入

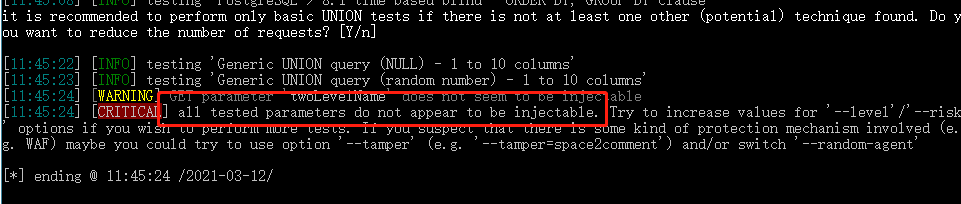
测试过程：



Sqlmap命令：

python sqlmap.py -u "https://x.x.x.x:x/mec-developer/mec/developer/v1/system/capability?offset=0&limit=10&twoLevelName=123" -p twoLevelName --cookie "DEVELOPERSESSIONID=EE5CB47D09904E007AC57E7174E5B143" --risk 3 --level 3 --dbms=xxx

扫描结果：



**测试结论**：**PASS**

[【UserMgmt】支持用户忘记密码后通过邮箱找回](https://gitee.com/OSDT/dashboard?issue_id=I2E9LG)

测试用例：邮件轰炸（暂无测试用例）

测试方法：尝试通过忘记密码的邮件发送功能，无限制发送邮件

测试过程：

①在找回密码页面，填写邮箱（已注册/未注册均可），点击“获取验证码”，使用Burp抓包，传入“Repeater”模块。

②重复点击“Send”按钮，可以看到每次都返回201状态，“true”。  
③可以看到邮箱中收到了大量垃圾邮件。

攻击者可以使用工具（如Burp Intruder）或编写攻击脚本，循环发送该请求，可能造成以下危害：  
①无限制的邮件发送，造成高额费用；（可以在发送时不断更换目标邮箱）  
②可能对邮件服务器造成较高负荷，甚至DOS。  
③目标邮箱被大量垃圾邮件占满。

修补建议：  
①点击“获取验证码”后，后端服务器记录访问者的IP和请求时间，如果在设定时间段内（如固定10分钟，或以5/15/30/45/60分钟方式递增）再次收到该IP的请求则拒绝发送邮件（可以在前端提示“您刚刚申请了密码找回，请过x分钟再次尝试”）。这样就限制了每个IP申请发送邮件的频率。  
②在此基础上，应限制每个IP每天申请发送邮件的次数上限。（考虑到NAT，每个公网IP下可能有多个用户，可以适当提高每个IP的申请上限，如每天20-30次）  
③（此条防邮件轰炸有效，但弊端也很大，需讨论）发送邮件前检查该邮箱是否为已注册邮箱，仅对已注册邮箱发送。（这条措施可能带来安全隐患：攻击者可以通过循环跑字典的方式确定已注册的邮箱，进而通过暴力破解/撞库等方式破解邮箱密码）

**测试结论**：**Not PASS**

**不通过原因：找回密码功能存在邮件轰炸漏洞。**

[【UserMgmt】支持用户通过邮箱注册](https://gitee.com/OSDT/dashboard?issue_id=I2E9LE)

测试用例：任意用户注册（暂无测试用例）

测试方法：尝试无限注册用户

测试过程：

①点击“免费注册”，填写用户名、密码信息，使用Burp抓包，并传至Burp Repeater模块。

②每次修改用户名，然后点击“Send”，可以无限制注册用户。

攻击者可以使用工具（如Burp Intruder）或编写攻击脚本，循环发送注册请求（每次修改用户名即可），造成以下后果：  
①服务器/数据库存储空间被占满；  
②数据量非常庞大时每次查询开销增加，甚至造成DOS。

修补建议：  
①限制每个IP注册用户的频率：如最快5分钟/次。  
②限制每个IP每天注册用户数量上限：如每天30个。  
③（更完美的方法，可讨论）注册时邮箱和手机号2选1必填，邮箱注册时发送邮件验证码，手机注册时发送短信验证码。不论邮件验证码还是短信验证码，均限制发送频率和单日发送数量上限。

**测试结论**：**Not PASS**

**不通过原因：找回密码功能存在任意用户注册漏洞。**

[【Developer】Developer应用支持分权控制，区分不同角色进行差异化功能展现](https://gitee.com/OSDT/dashboard?issue_id=I2E6S7)

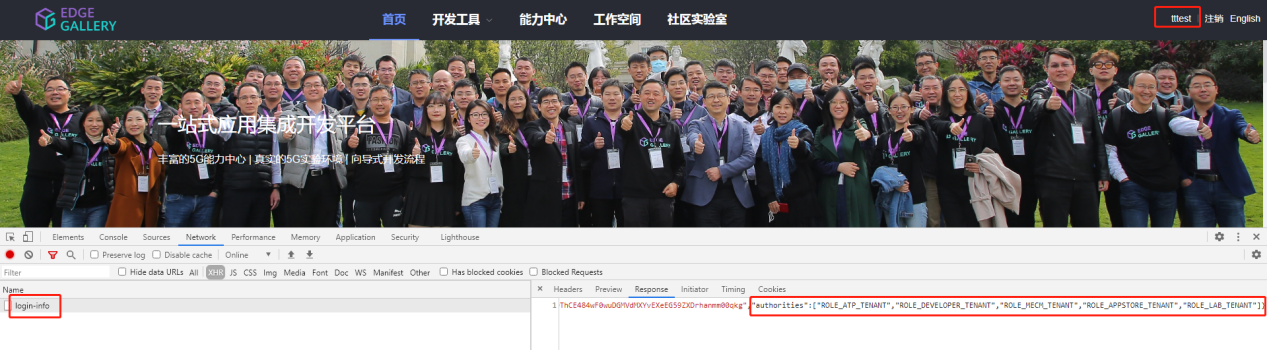
[【developer】支持能力中心管理](https://gitee.com/OSDT/dashboard?issue_id=I2EDOC)

[【developer】支持配置沙箱环境](https://gitee.com/OSDT/dashboard?issue_id=I2EDO1)

[【developer】系统管理面界面开发](https://gitee.com/OSDT/dashboard?issue_id=I2EDNR)

测试方法：尝试使用低权角色访问高权接口/功能。

①登录租户，如图



②通过url访问沙箱管理页面，访问成功。尝试新建沙箱，成功。

③通过url访问能力中心管理页面，访问成功。尝试删除“服务治理”能力，成功。

**测试结论**：**Not PASS**

**不通过原因："沙箱管理"和"能力中心管理"存在垂直越权漏洞。**