## v1.1 Spirnt2合规测试记录

## R1.1 Sprint2 Compliance Test Record

## Test case EG-TST-SEC-CP-1-1

#### 测试说明：

所有用于跨网络传输的机器对机器和人对机器接口都必须具有访问认证机制，并且认证过程必须在服务器上执行。 **注意**：跨网络接口必须支持身份验证，以防止欺骗

[【AppStore】支持应用主动拉取功能](https://gitee.com/OSDT/dashboard?issue_id=I2E10V)

测试方法：尝试删除appstoreSessionID，查看能否访问成功

可以看到，显示302跳转，无法正常访问，ok

**测试结论**：**PASS**

[【developer】支持部署文件可视化配置（sprint1, sprint2）](https://gitee.com/OSDT/dashboard?issue_id=I2EDT4)

测试方法：尝试删除developerSessionID，查看能否访问成功。

可以看到访问失败，3.2跳转。Ok

**测试结论**：**PASS**

## Test case EG-TST-SEC-CP-1-2

#### 测试说明：

对于每个需要授权的访问请求，服务器必须验证用户是否有权执行此操作。

[【AppStore】支持应用主动拉取功能](https://gitee.com/OSDT/dashboard?issue_id=I2E10V)

测试方法：尝试纵向越权，使用普通用户访问应用拉取接口。

可以看到访问失败，ok

**测试结论**：**PASS**

[【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)

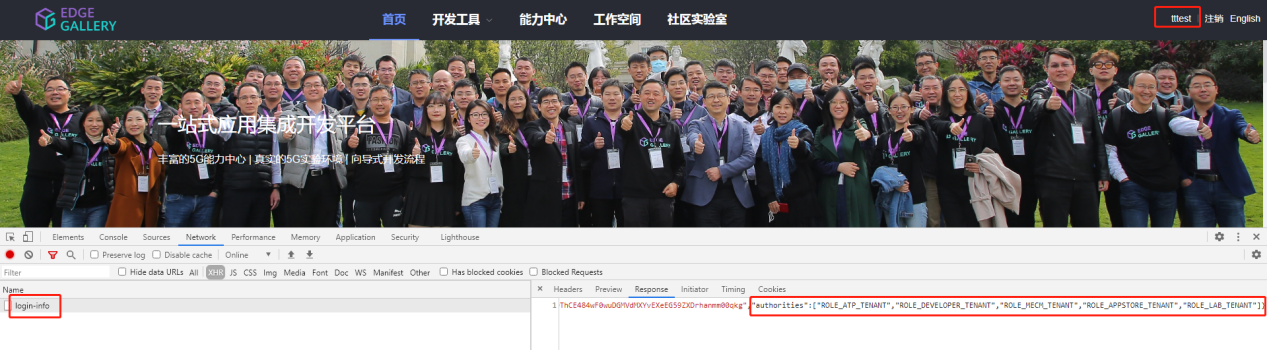
[【developer】支持能力中心管理](https://gitee.com/OSDT/dashboard?issue_id=I2EDOC)

[【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**

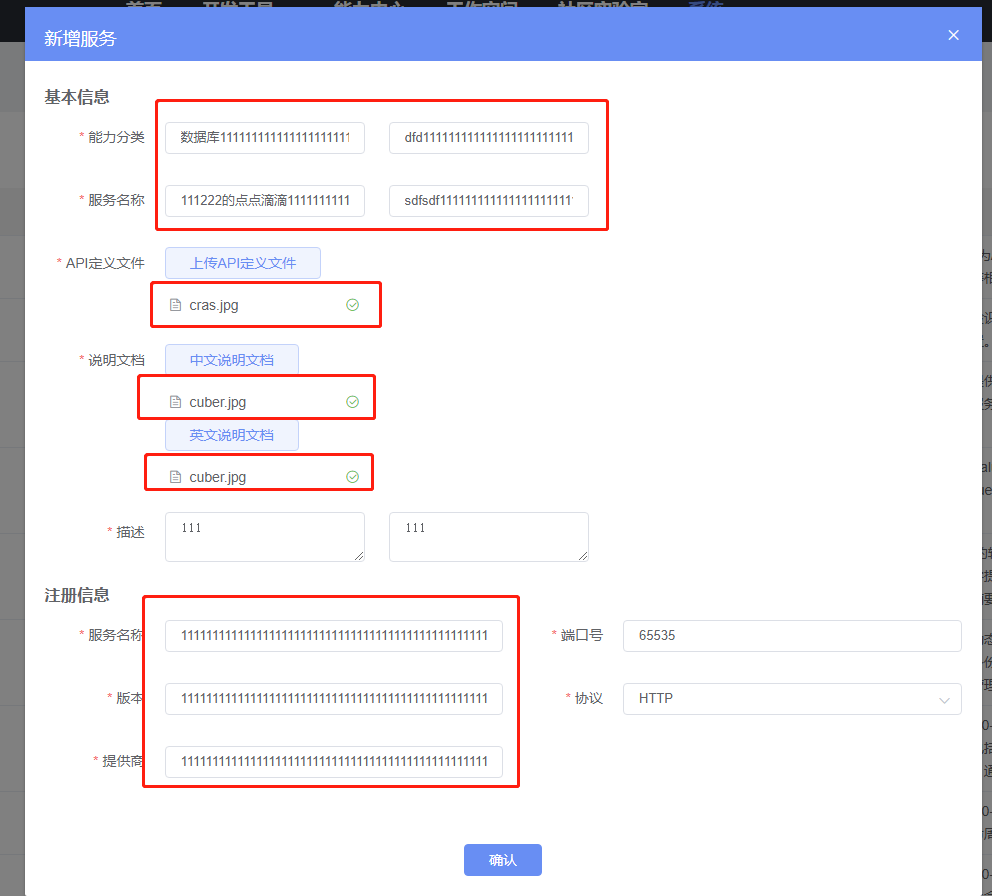
**不通过原因："沙箱管理"和"能力中心管理"存在垂直越权漏洞。**

## Test case EG-TST-SEC-CP-1-3

#### 测试说明：

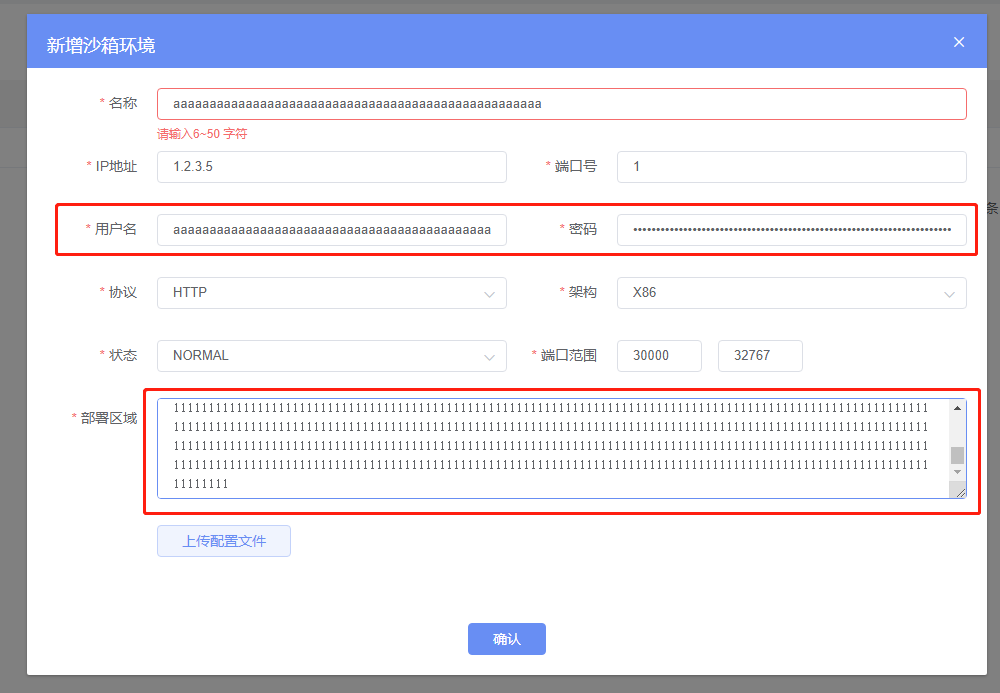
服务器必须验证所有不受信任的数据源的大小，类型，长度和特殊字符，并拒绝所有未通过验证的数据

## [【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)

这两项功能均包含“新增”功能。新增时测试应用是否限制数据大小、格式等。



可以看到前端均未限制用户输入长度、格式等。

**测试结论**：**Not PASS**

**不通过原因："沙箱管理"和"能力中心管理"新增页面未限制用户输入数据长度/格式等。**

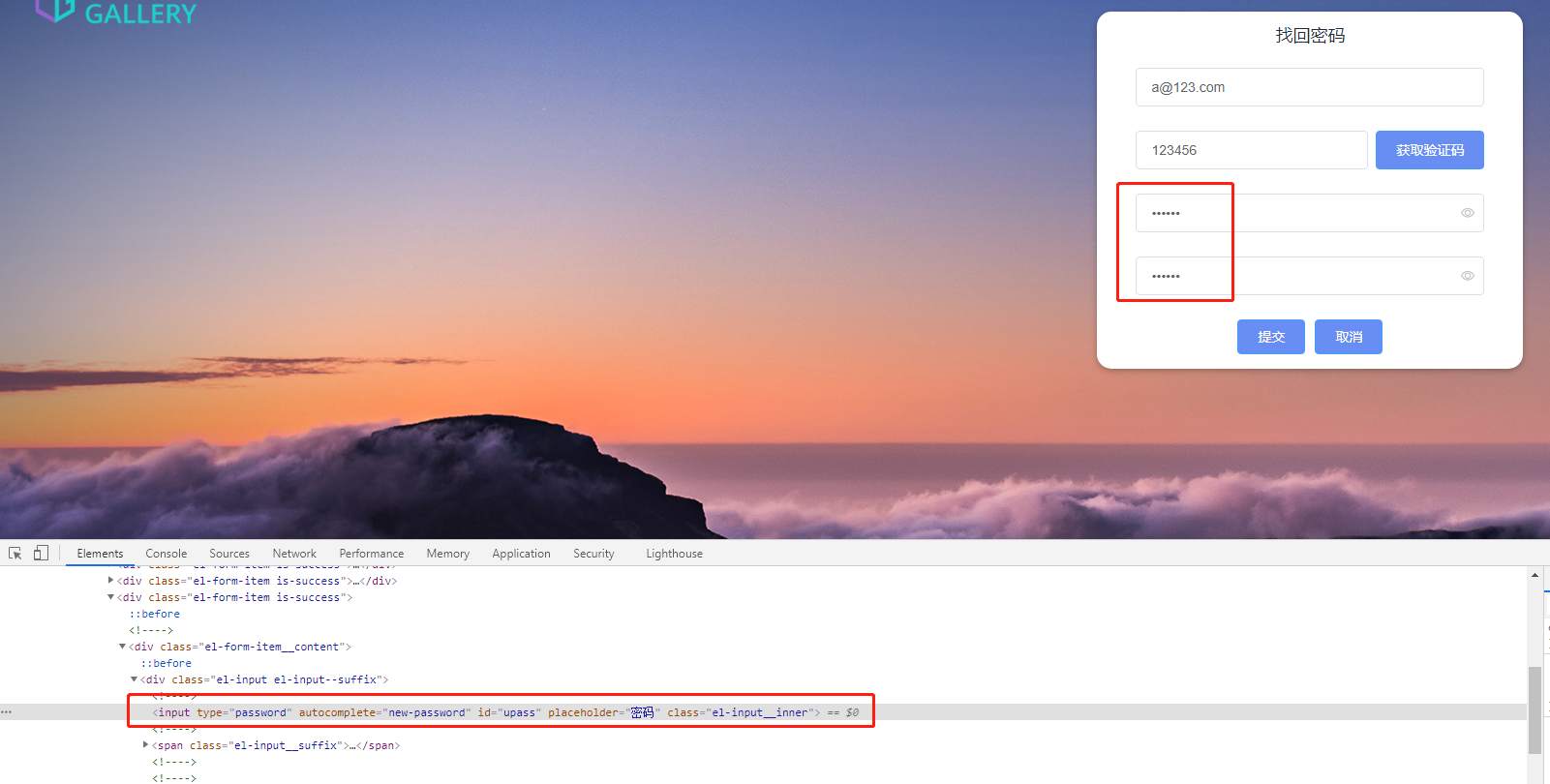
## Test case EG-TST-SEC-CP-1-8

#### 测试说明：

忘记的密码功能和其他恢复路径不应泄露当前密码，新密码也不应以明文形式发送给用户。

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

测试步骤： 1.登录系统并使用“忘记密码”功能重置密码。 2.检查当前密码未显示，并且新密码已加密。



可以看到，type=password autocomplete=new password ok.

**测试结论**：**PASS**

## Test case EG-TST-SEC-CP-1-10

#### 测试说明：

确认已采取措施阻止使用常用的密码和弱密码短语。

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

测试方法：尝试使用简单密码，查看能否使用成功。



**测试结论**：**PASS**

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



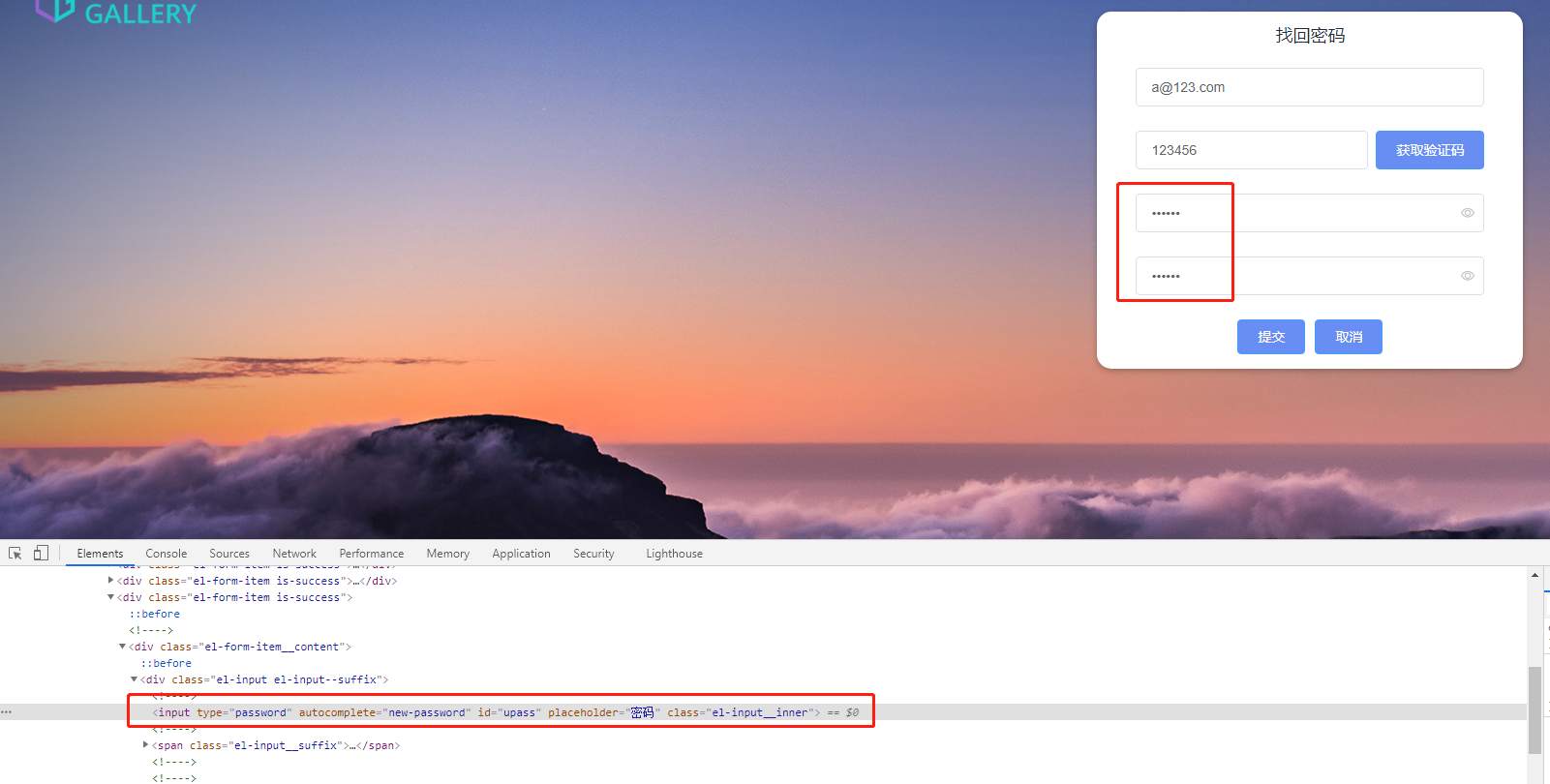
**测试结论**：**PASS**

## Test case EG-TST-SEC-CP-1-14

#### 测试说明：

在口令框中输入的口令不能明文显示和拷贝/剪切，密码框也不允许使用自动填充功能。tag: version v1.1

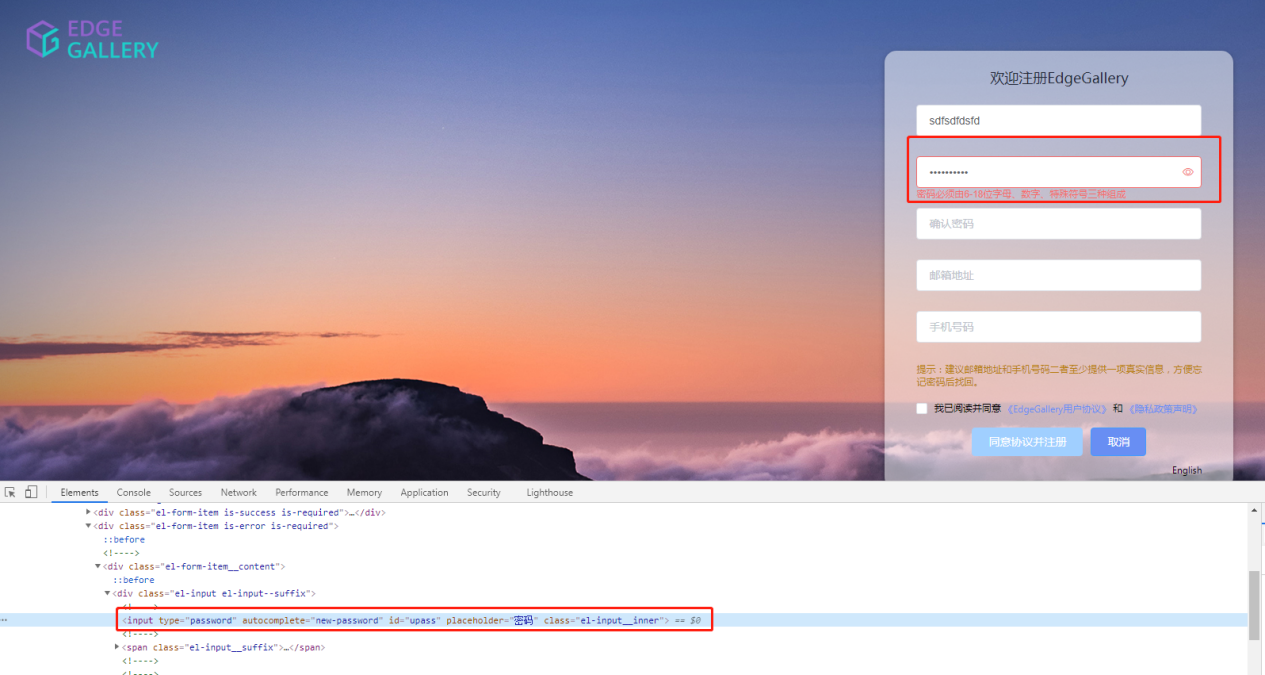
[【UserMgmt】支持用户忘记密码后通过邮箱找回](https://gitee.com/OSDT/dashboard?issue_id=I2E9LG)



可以看到，type=password autocomplete=new password ok.

**测试结论**：**PASS**

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



可以看到，type=password autocomplete=new password ok.

**测试结论**：**PASS**

## Test case EG-TST-SEC-CP-1-1

#### 测试说明：

不再使用的账号必须删除或停用。删除账号时，必须同时删除相应的凭据（如密码、秘钥等），以防止这些被认为是后门。tag: version v1.1

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

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

测试方法：查看admin用户管理页面，查看是否存在可疑用户。

可以看到，处理guest和admin是内置用户，其他都为用户创建用户，并且启用/停用功能有效。Ok

**测试结论**：**PASS**