|  |  |  |  |
| --- | --- | --- | --- |
| 功能A描述 | 添加角色 | | |
| 用例目的 | 用户向系统添加角色信息 | | |
| 前提条件 | 用户登录该系统，并且拥有添加角色的权限 | | |
| 输入/动作 | | 期望的输出/相应 | 实际情况 |
| 点击添加角色按钮，输入数据  角色名：普通员工  角色等级：5  用户权限：无特殊权限 | | 提示“操作成功” | 提示“操作成功” |

|  |  |  |  |
| --- | --- | --- | --- |
| 功能A描述 | 修改角色 | | |
| 用例目的 | 用户修改角色信息 | | |
| 前提条件 | 用户登录该系统，并且拥有修改角色的权限 | | |
| 输入/动作 | | 期望的输出/相应 | 实际情况 |
| 选择要修改的角色，点击修改按钮，输入数据  角色名：普通员工  角色等级：4  用户权限：无特殊权限、资产列表 | | 提示“操作成功” | 提示“操作成功” |

|  |  |  |  |
| --- | --- | --- | --- |
| 功能A描述 | 删除角色 | | |
| 用例目的 | 用户删除角色信息 | | |
| 前提条件 | 用户登录该系统，并且拥有删除角色的权限 | | |
| 输入/动作 | | 期望的输出/相应 | 实际情况 |
| 选择要修改的角色，点击删除按钮 | | 提示“操作成功” | 提示“操作成功” |

|  |  |  |  |
| --- | --- | --- | --- |
| 功能A描述 | 用户权限设置 | | |
| 用例目的 | 用户修改其他用户的角色权限 | | |
| 前提条件 | 用户登录该系统，并且拥有权限设置的权限 | | |
| 输入/动作 | | 期望的输出/相应 | 实际情况 |
| 选择要修改的用户，点击修改权限，输入数据  角色名称：部门经理 | | 提示“操作成功” | 提示“操作成功” |

## 安全性测试

* **概述：**确保系统Web应用下的安全性
* **目标：**核实下列情况下的性能行为
  + 用户重要的操作是否写进日志、是否可追踪
  + 视图权限是否完整
  + 数据权限是否完整
  + URL路径是否有得到有效的控制

相关表格如下：

|  |  |
| --- | --- |
| 检查项 | 测试人员的类别及其评价 |
| 用户重要的操作是否写进日志、是否可追踪 | 基本都已实现，所有用户的增加、修改、删除操作都有写入系统日志。 |
| 访问系统页面是否有进行用户登录过滤 | 基本都已实现，用户需要登录才能进入系统，如果直接访问其中任一页面或任一接口路径(除了登录接口)都会跳转到登录页面。 |
| 视图权限是否完整 | 基本都已实现，每个用户都有对应的角色，每个角色都有相应的视图权限，一些重要板块需要拥有该板块访问权限的用户才能访问（具体到某个菜单项、某个按钮）。 |
| 数据权限是否完整 | 基本都已实现，一些列表的数据会根据用户的角色进行筛选显示，如用户权限设置板块，所能修改的用户只能是比操作者的角色等级低的用户。 |
| URL路径是否有得到有效的控制 | 基本都已实现，一些重要的请求路径需要拥有对应路径的权限才能访问，如无该路径的请求权限系统会拦截下来并提示无访问权限的信息。 |