Epic：  
【ATP】ATP测试用例扩充

【ATP】测试用例模型增强

Story:

【ATP】ATP应用支持分权控制，区分不同角色进行差异化功能展现

|  |  |
| --- | --- |
| **Content** | **Related Information** |
| **Security design rule ID** | 1.1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，以防止欺骗访问  All machine-to-machine and man-to-machine interfaces for cross-network transmission must have an access authentication mechanism, and the authentication process must be performed on a server.  1.2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  For each access request that requires authorization, the server must verify whether the user is authorized to perform this operation.  1.3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。 注意：为了防止攻击者通过代理来拦截和篡改请求以绕过客户端的有效性检查，必须在服务器上执行数据验证。  The server must validate the size, type, length, and special characters of all untrusted data sources and reject any data that fails the validation.  1.12基于角色的访问控制  Role based Access control.  5.3所有输入必须限制在适当的大小限制内。  All input must be limited to an appropriate size limit.  7.2必须接受XML或JSON模式，并在接受输入之前对其进行验证   XML or JSON schema must be in place and verified before accepting input.  8.1所有公共功能接口，RESTful接口，本地功能接口，命令行接口以及用于身份验证的默认用户名和密码都必须在产品或应用程序文档中进行描述。  All public function interfaces, RESTful interfaces, local function interfaces, command line interfaces, and default usernames and passwords used for identity authentication must be described in the product or application document.  9.1请勿记录未经消毒的用户输入。  Do not log unsanitized user input. Notice: Unsanitized logging can allow an attacker to forge log entries or inject malicious content into logs.  9.2足够的日志记录  Sufficient Logging.  9.4避免记录过多的数据  Avoid Logging of Excessive Data |
| **Implementation details** | * 1. 对token进行了解析验证   Validate the token in request header   * 1. 每个restful接口都有角色校验，符合的角色才能访问接口   Each restful interface has access validation based on role   * 1. 接口校验用户输入的参数的长度   Interface validates the length of input parameters  1.12 接口做了角色访问控制  Access to interface must satisfy the role  5.3 对接口入参做了长度校验  Validate the length of input parameter.  7.2 所有的接口结构体都是json的形式  All pattern of request or response body is json  8.1 接口在产品文档中进行描述  Describe the restful interface in document.  9.1 日志未记录用户输入的字段  Do not logging user input data.  9.2 在异常情况分支中，记录了足够的日志，能够支撑定位。  logging enough log in exception branch.  9.4 对于流程的日志，没有记录，只在异常分支中记录了日志。  Only logging in exception branch, do not logging to much redundant logs. |
| **Related APIs** | edgegallery/atp/v1/tasks/batch\_delete POST  edgegallery/atp/v1/tasks/action/analysize GET  edgegallery/atp/v1/testcases/{id}/action/download GET  edgegallery/atp/v1/testscenarios POST  edgegallery/atp/v1/testscenarios/{id} PUT  edgegallery/atp/v1/testscenarios/{id} DELETE  edgegallery/atp/v1/testscenarios/{id} GET  edgegallery/atp/v1/testscenarios?locale=“ch”&&name = “” GET  edgegallery/atp/v1/testsuites POST  edgegallery/atp/v1/testsuites/{id} PUT  edgegallery/atp/v1/testsuites/{id} DELETE  edgegallery/atp/v1/testsuites/{id} GET  edgegallery/atp/v1/testsuites?locale=“ch”&name = “”&scenarioIdList =“” GET |
| **Example API payload** | 2.5K |
| **Related files** | NA |
| **Related GUI URLs** | NA |
| **GUI testing steps** | 在应用商城我的应用中，点击测试，验证测试场景选择页面和测试进展页面  In my application of appstore, clicking test and validating test scenario choice page and test task process page  在ATP管理面中，点击测试场景管理，验证测试场景列表、新增、删除、修改操作  In ATP management portal, clicking test scenario management, and validating test scenario CRUD operation  在ATP管理面中，点击测试套管理，验证测试套列表、新增、删除、修改操作  In ATP management portal, clicking test suite management, and validating test suite CRUD operation  在ATP管理面，点击任务管理，验证测试任务列表批量删除操作  In ATP management portal, clicking test task management, and validating batch delete test task operation |
| **GUI input example** | NA |
| **Additional Info** | NA |