**EdgeGallery R1.0渗透测试报告**

**Sprint 1：**

**Story：**[need to add the role of GUEST for all of GET APIs in Developer](https://gitee.com/OSDT/dashboard?issue_id=I24IMF)

**测试用例：EG-TST-SEC-007** 越权

**测试说明**：

为所有的GET型API添加了Guest用户：目前项目仅有2类权限用户：GUEST用户和普通用户，测试内容为判断GUEST用户能否访问普通用户数据。

**测试过程**：

**Developer**：

①新建项目：

尝试新建项目，点击“下一步”按钮时提示“GUEST用户无权操作，请先登录！”，然后“下一步”按钮变为不可点击；通过。

②迁移项目：

尝试迁移项目，点击“下一步”按钮时提示“GUEST用户无权操作，请先登录！”，然后“下一步”按钮变为不可点击；通过。

③上传插件：

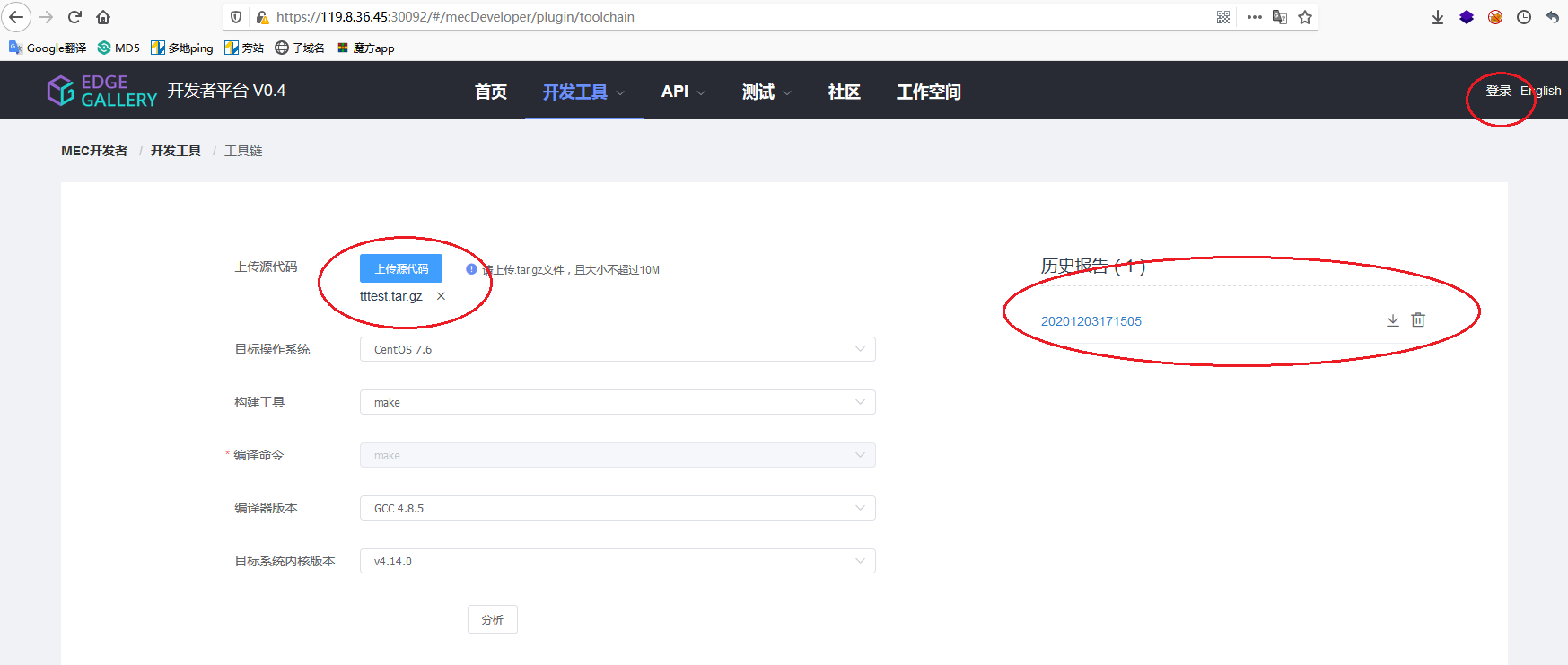
尝试上传插件，点击“立即上传”按钮时提示“GUEST用户无权操作，请先登录！”；通过。

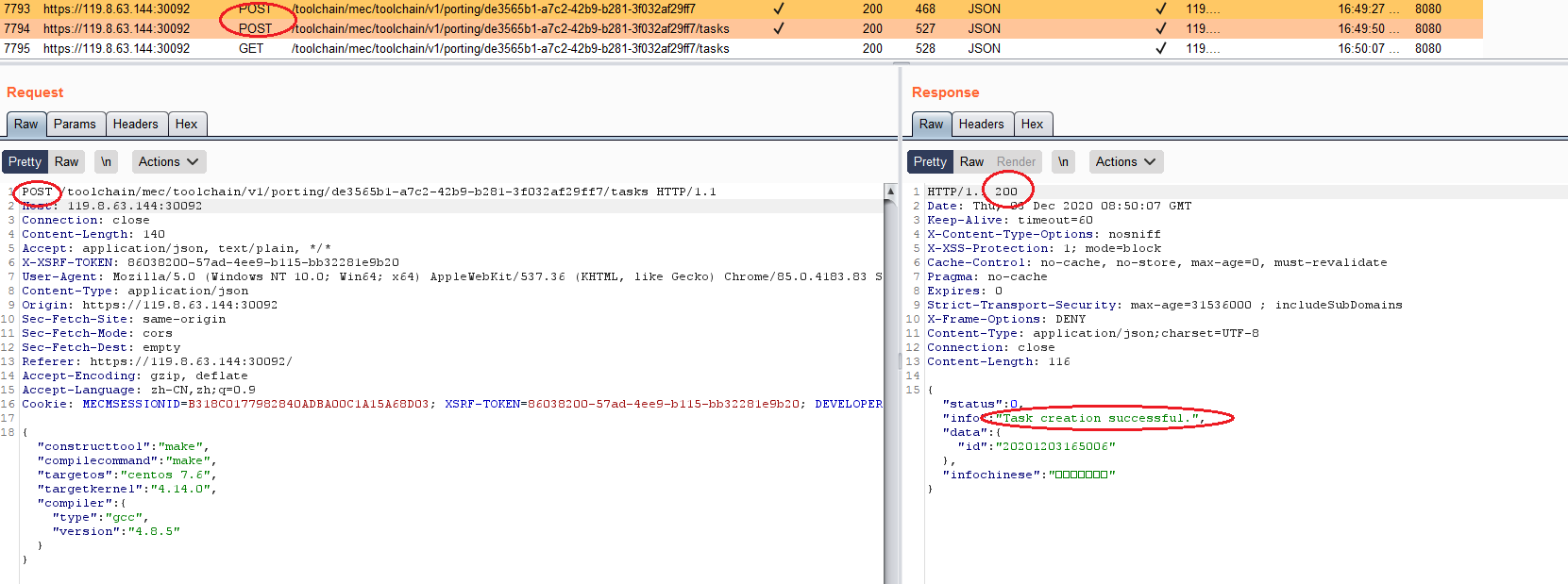
④下载插件：

尝试下载已上传的插件，点击“详情”，可以看到详情；点击“下载”，可以正常下载；下载完毕后进行评分，提示“GUEST用户无权操作，请先登录！”；通过。

④工具链：

尝试上传xxx.tar.gz，点击“分析”按钮后，生成历史报告，并可下载；不通过。





⑤测试应用：

尝试上传.csar文件，点击“立即上传”按钮时提示“GUEST用户无权操作，请先登录！”；通过。

**测试结论**：**Not PASS**

**不通过原因：GUEST用户可以通过“工具链”功能中POST接口上传文件。**

**Story：**[need to add the role of GUEST for all of GET APIs in AppStore](https://gitee.com/OSDT/dashboard?issue_id=I24IKL)

**测试用例：EG-TST-SEC-007** 越权

**测试说明**：

为所有的GET型API添加了Guest用户：目前项目仅有2类权限用户：GUEST用户和普通用户，测试内容为判断GUEST用户能否访问普通用户数据。

**测试过程**：

**AppStore**：

①App评论区：

尝试提交评论：提示“GUEST用户无权操作！请登录”；

②上传文件：

尝试上传csar文件，“检测”按钮禁止点击；点击“确认”按钮后，提示“GUEST用户无权操作！请登录”；

**测试结论**：**PASS**

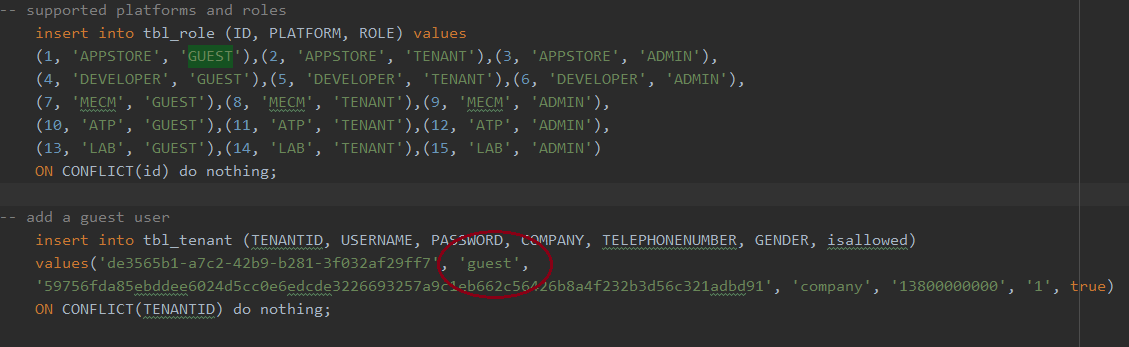
Story：[用户管理模块中需要支持用户的角色定义](https://gitee.com/OSDT/dashboard?issue_id=I23FRE)

**测试用例：EG-TST-SEC-007** 越权

**测试说明**：

为所有的GET型API添加了Guest用户：目前项目仅有2类权限用户：GUEST用户和普通用户，测试内容为判断GUEST用户能否访问普通用户数据。

**测试过程**：



可以看到，已添加guest用户。

**测试结论**：**PASS**

Story：[用户管理支持guest访客用户，在界面上只有只读权限](https://gitee.com/OSDT/dashboard?issue_id=I23FRC)

测试说明：

此条story已分解为3条story：

[need to add the role of GUEST for all of GET APIs in Developer](https://gitee.com/OSDT/dashboard?issue_id=I24IMF)

[need to add the role of GUEST for all of GET APIs in AppStore](https://gitee.com/OSDT/dashboard?issue_id=I24IKL)

[need to add the role of GUEST for all of GET APIs in MECM](https://gitee.com/OSDT/dashboard?issue_id=I24IKE)

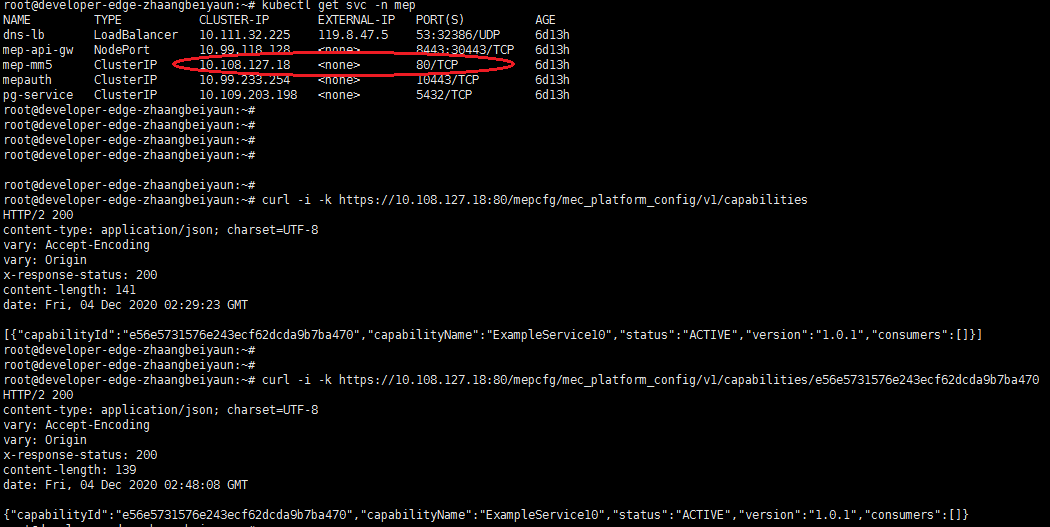
其中前2则story已测试。Mecm正在开发中（计划sprint3完成），待开发完毕进行测试。

Story：[【MEP】MEP Support to query the capabilities.](https://gitee.com/OSDT/dashboard?issue_id=I1W7UU)

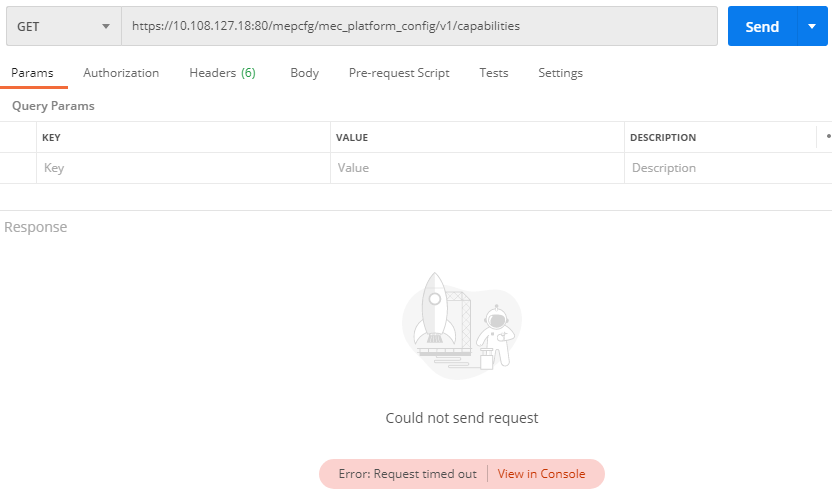
**测试用例：EG-TST-SEC-005 SQL注入**

**测试过程：**

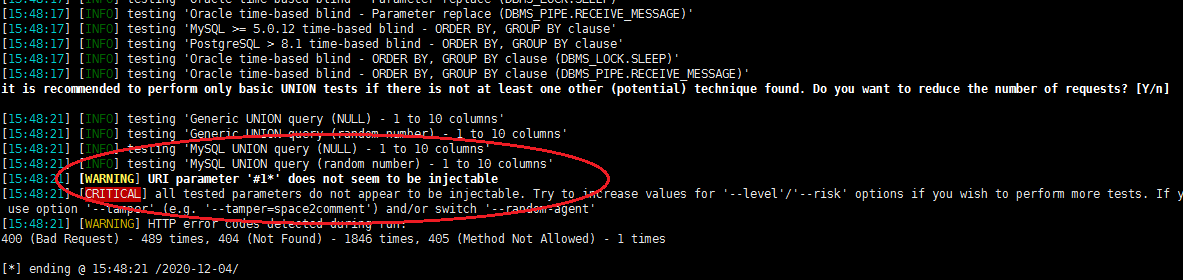
Mep的查询功能信息由Mecm使用，以在其门户上显示。Mecm通过mm5接口将功能查询发送到mep。经过确认，mep的查询接口为内部接口，不能由用户直接调用或访问，所以外部攻击者也无法访问该接口，不会受到外部攻击的威胁。同时使用sqlmap进行辅助测试，未发现可利用的注入点。



通过外部无法访问mep查询接口。



使用sqlmap尝试对该接口进行注入，未发现注入点。



**测试结论**：**PASS**

**Sprint 2：**

**Story：**[【MECM 】MECM Support to query the capabilities](https://gitee.com/OSDT/dashboard?issue_id=I1Z3CN)

**测试用例：EG-TST-SEC-007** 越权 **EG-TST-SEC-005 SQL注入**

**测试说明**：

对查询时是否进行了权限鉴别进行判断，防止非授权查询；对查询参数进行SQL注入测试。

**测试过程**：

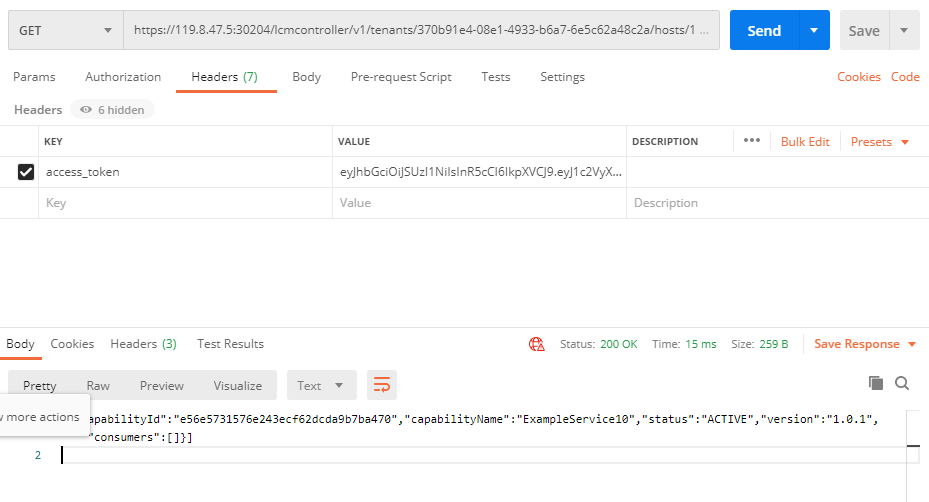
1.越权测试

1.1调用/lcmcontroller/v1/tenants/{tenantId}/hosts/{hostIp}/mep\_capabilities

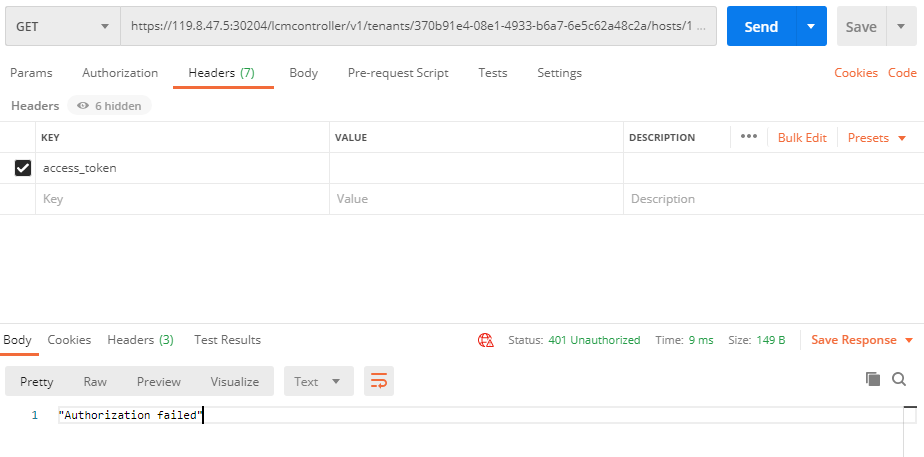
查询接口

<https://119.8.47.5:30204/lcmcontroller/v1/tenants/370b91e4-08e1-4933-b6a7-6e5c62a48c2a/hosts/119.8.47.5/mep_capabilities/>

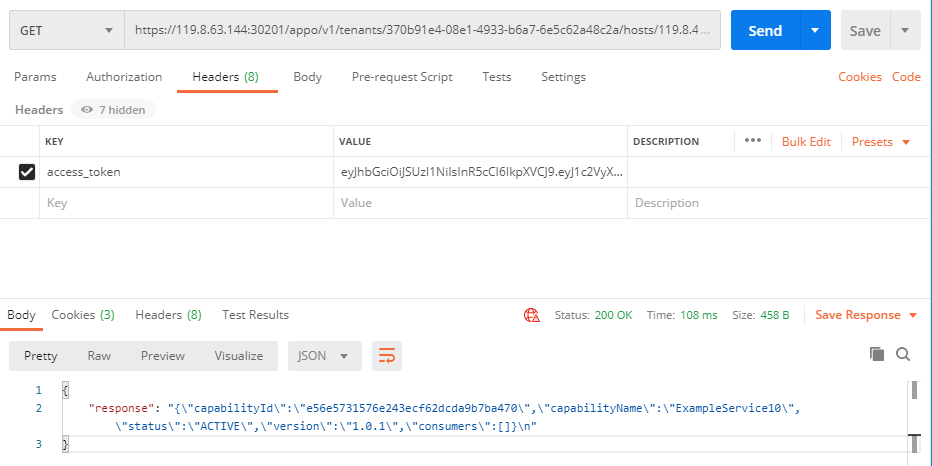
返回正常



删除身份验证信息access\_token，再次发送，返回401错误，显示"Authorization failed"。

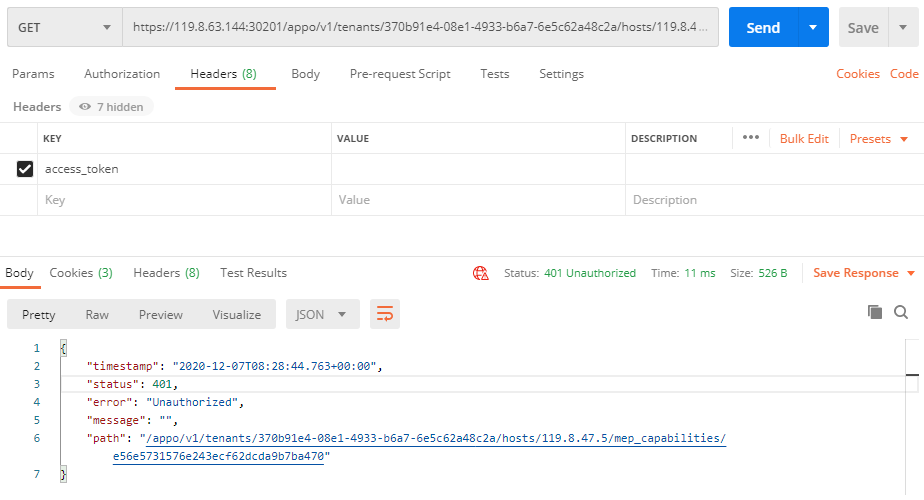


1.2调用/appo/v1/tenants/{tenant\_id}/hosts/{host\_ip}/mep\_capabilities查询接口



删除身份验证信息access\_token，再次发送，返回401错误，显示"error": "Unauthorized"

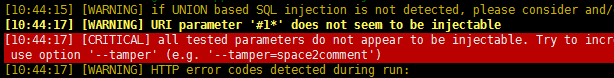
。



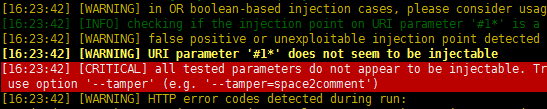
1. SQL注入测试

使用sqlmap进行SQL注入测试，未发现可利用的注入点。

2.1针对/lcmcontroller/v1/tenants/{tenantId}/hosts/{hostIp}/mep\_capabilities接口：

****

**2.2 针对**/appo/v1/tenants/{tenant\_id}/hosts/{host\_ip}/mep\_capabilities接口：



**测试结论**：**PASS**

**Story：**[【MECM】MECM Support Batch Distribution and Batch Deployment](https://gitee.com/OSDT/dashboard?issue_id=I249AF)

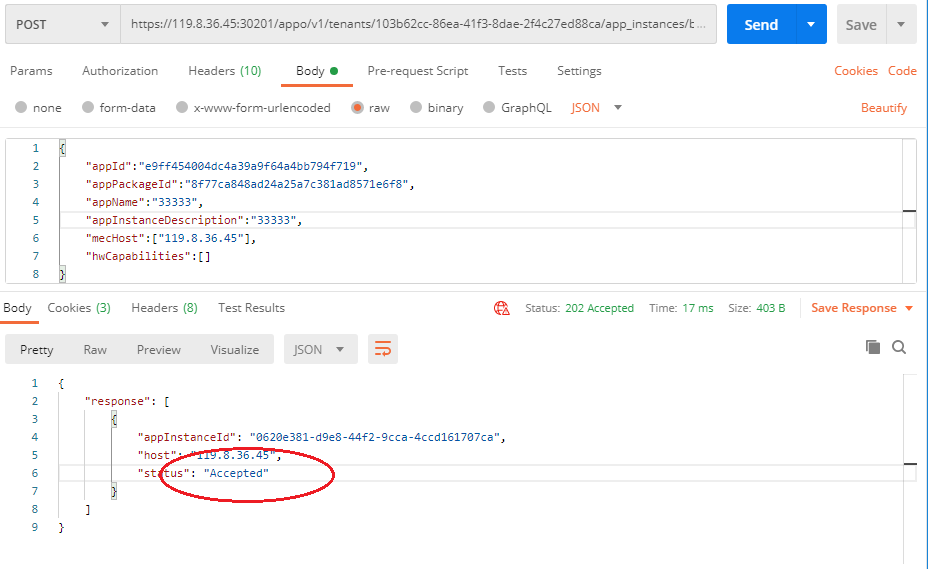
**测试用例：EG-TST-SEC-007** 越权

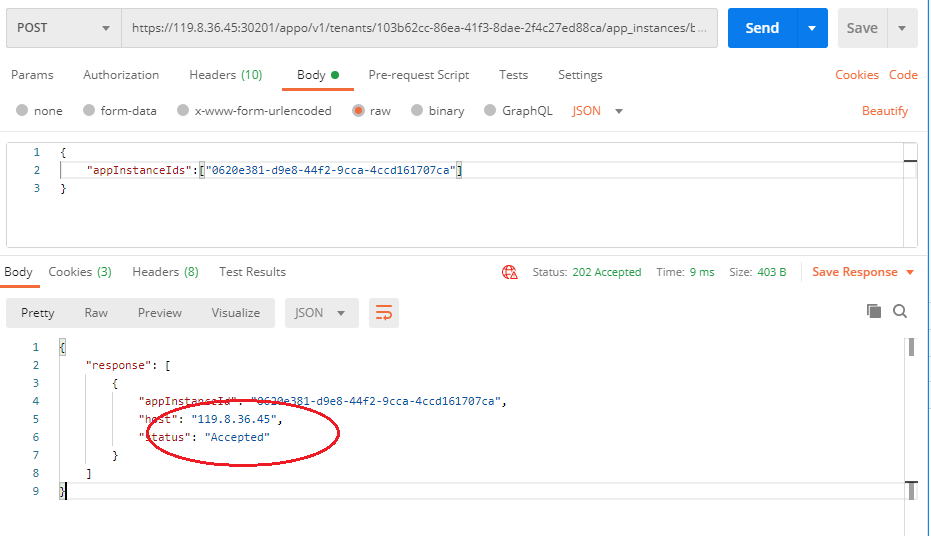
**测试说明**：

对查询时是否进行了权限鉴别进行判断，防止非授权调用接口；

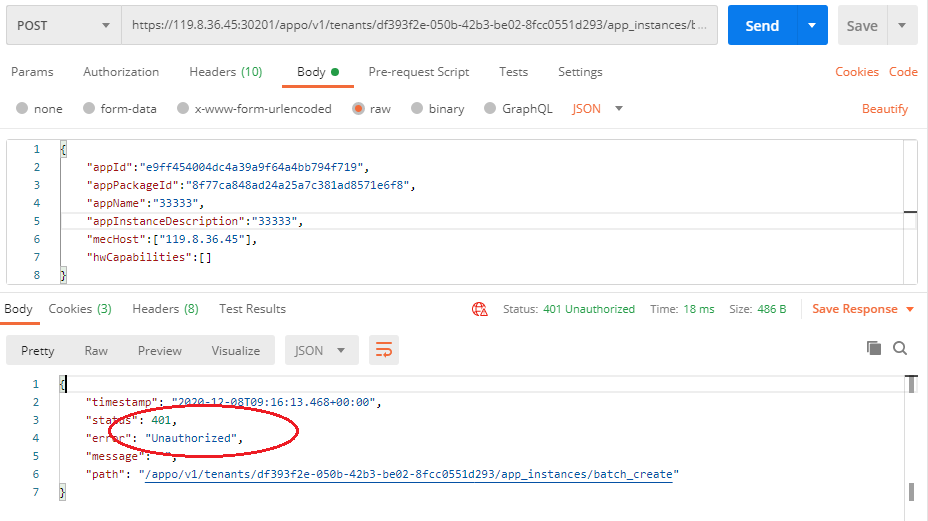
**测试过程**：

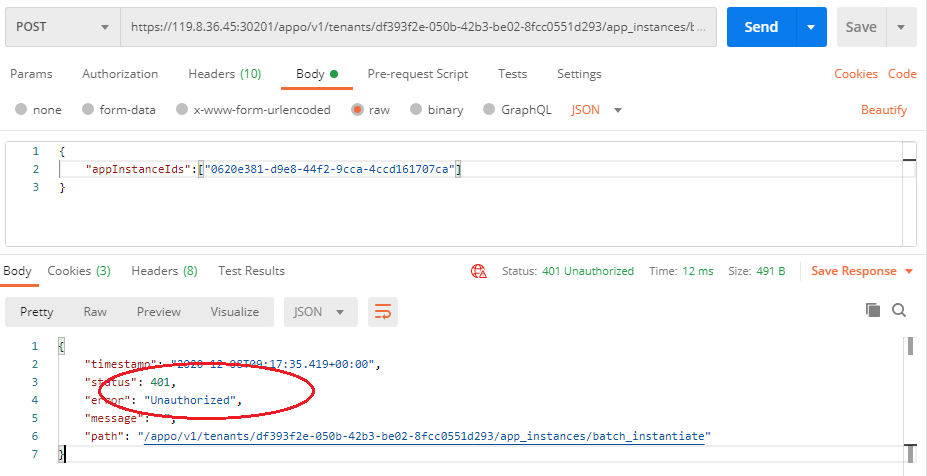
①正常的批量分发部署过程，OK





②尝试修改UserID，观察能否以其他用户身份进行批量分发部署操作。





均提示401错误，权限鉴别失败。

**测试结论**：**PASS**

**Story：**[【MECM】提供ak/sk分配功能](https://gitee.com/OSDT/dashboard?issue_id=I1R5LY)

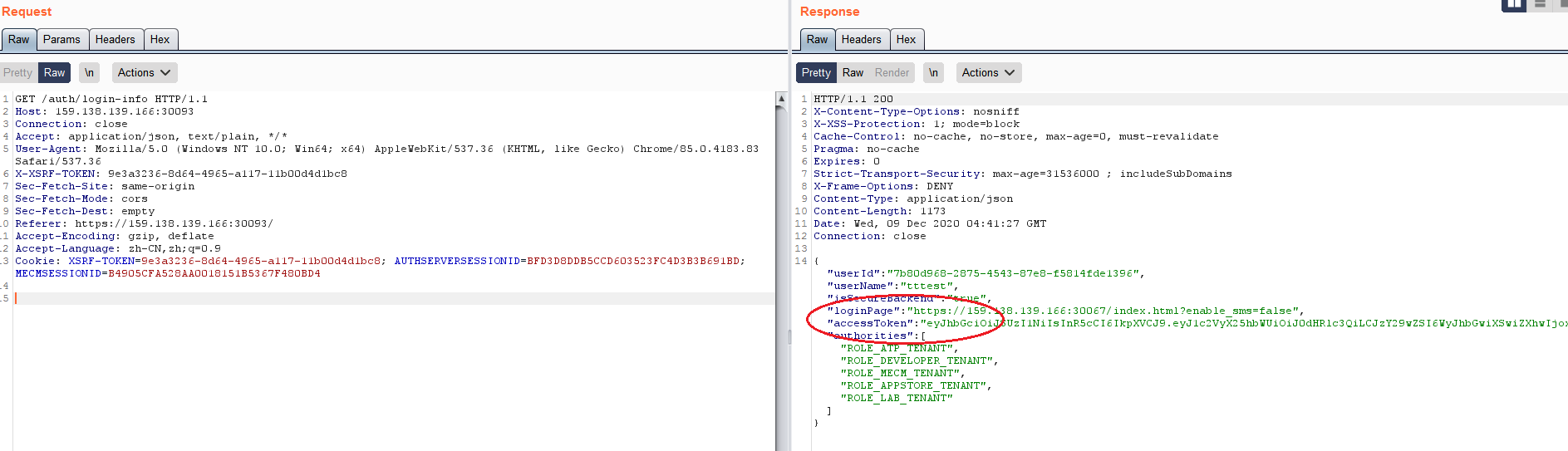
**测试用例：EG-TST-SEC-007** 越权

**测试说明**：

对接口调用时是否进行了权限鉴别进行判断，防止非授权调用接口；

**测试过程**：

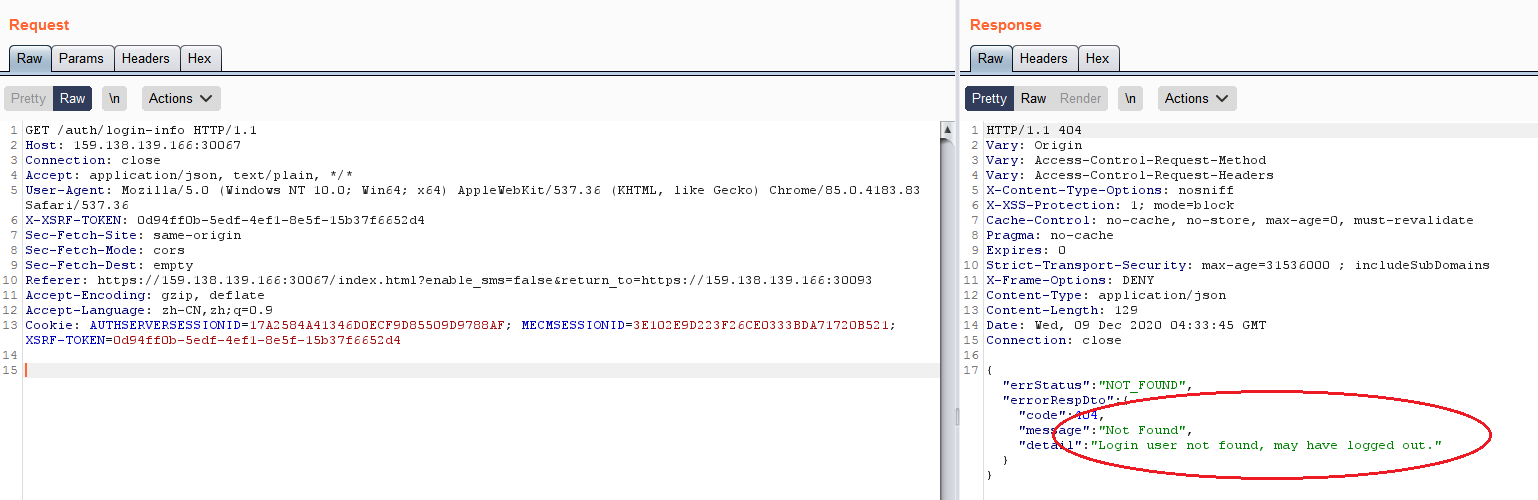
①正常的获取access\_token过程，OK

****

②修改MECMSESSIONID为另一个用户的MECMSESSIONID，观察能否成功获取access\_token。结果无法获取access\_token。



③观察正常获取access\_token时所用的MECMSESSIONID失效后，还能否成功获取access\_token。结果无法获取access\_token。



**测试结论**：**PASS**