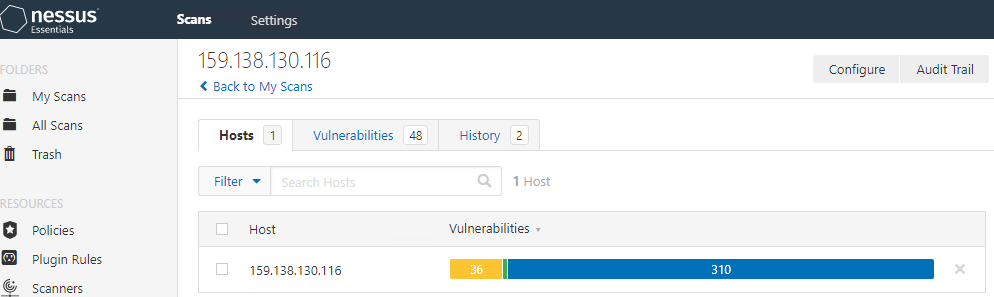
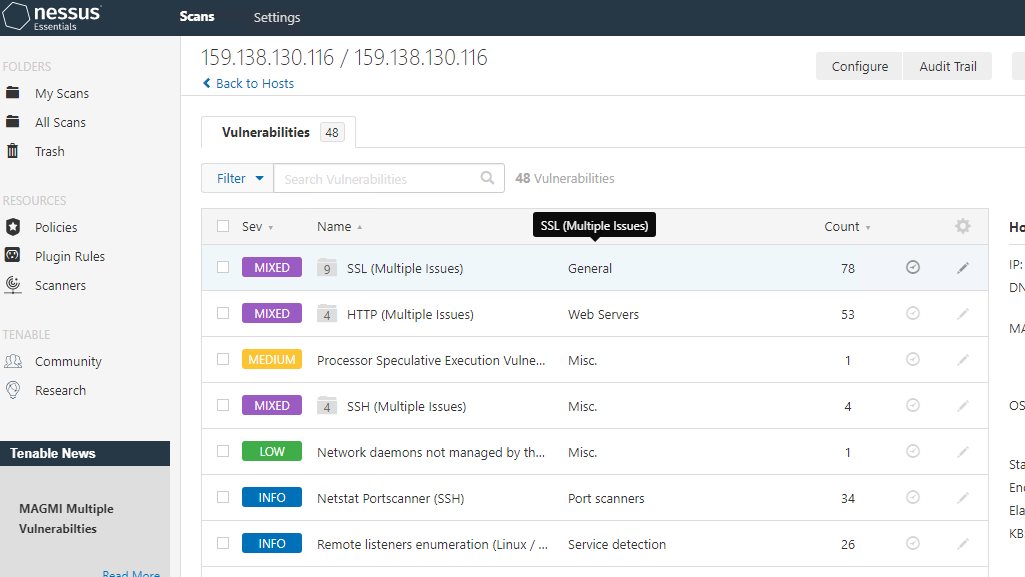
# EdgeGallery R0.9 安全合规测试结果

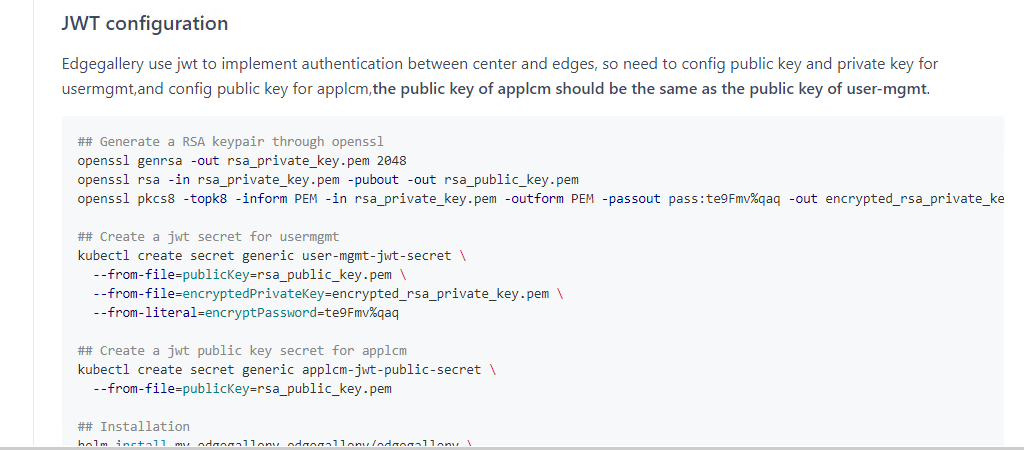
## Test case EG-TST-SEC-CP-4-1

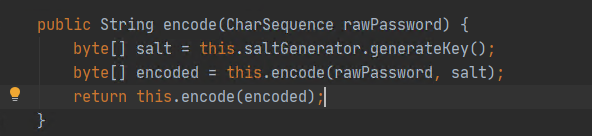
Nussus没有扫描出请勿使用专有和非标准的加密算法

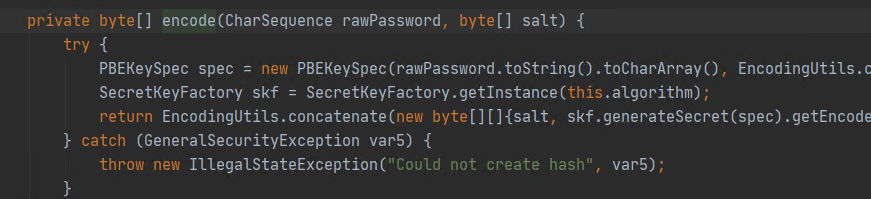




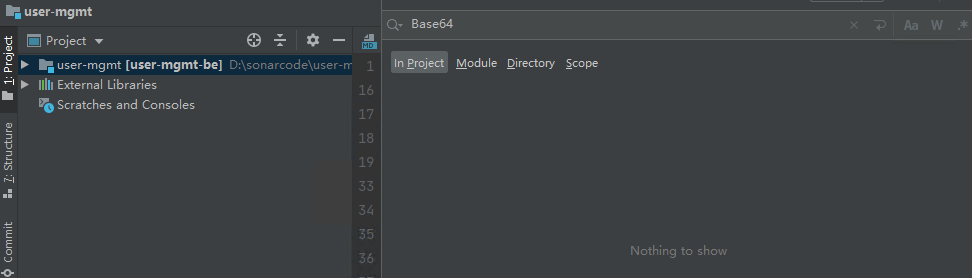
使用jwt,springsecurity进行加密解密，SHA-256 +随机盐+密钥对密码进行加密







没有使用Base64进行加密数据。

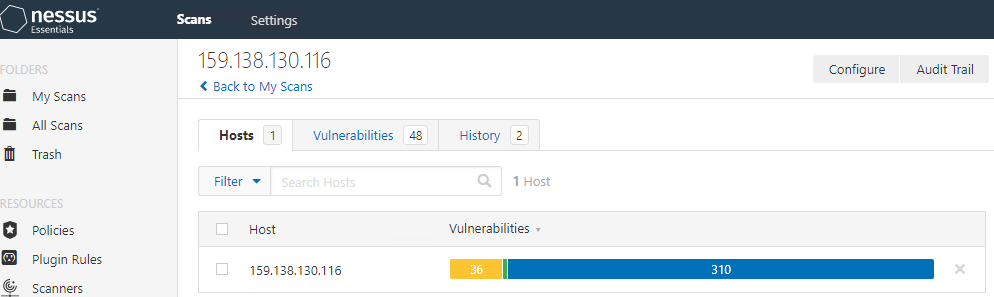


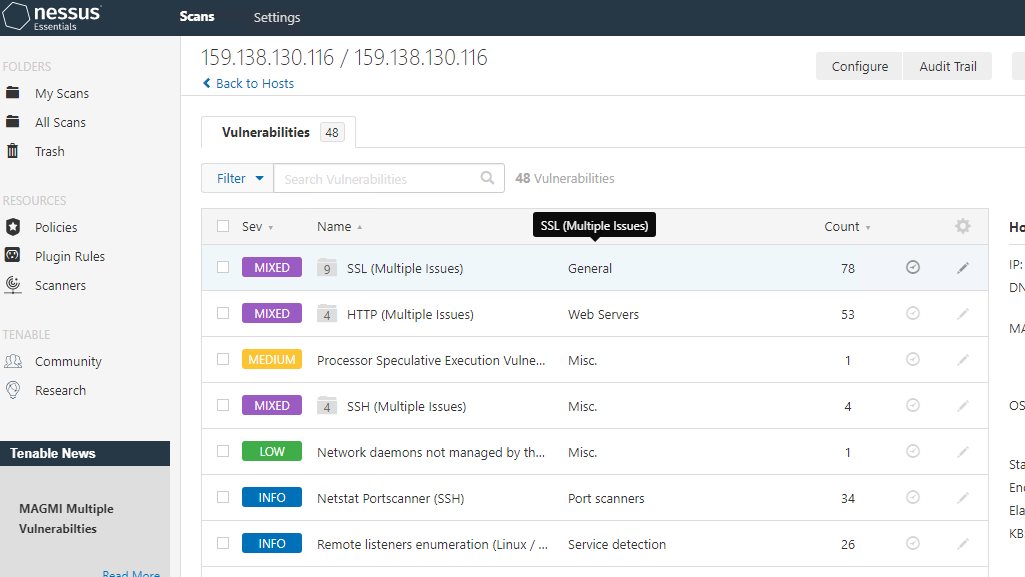
**结论：通过**

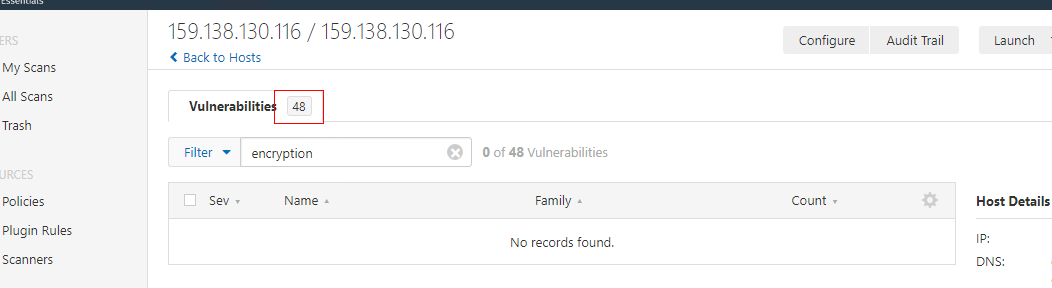
## Test case EG-TST-SEC-CP-4-2

扫描159.138.130.136

Nussus没有扫描出不安全的加密算法

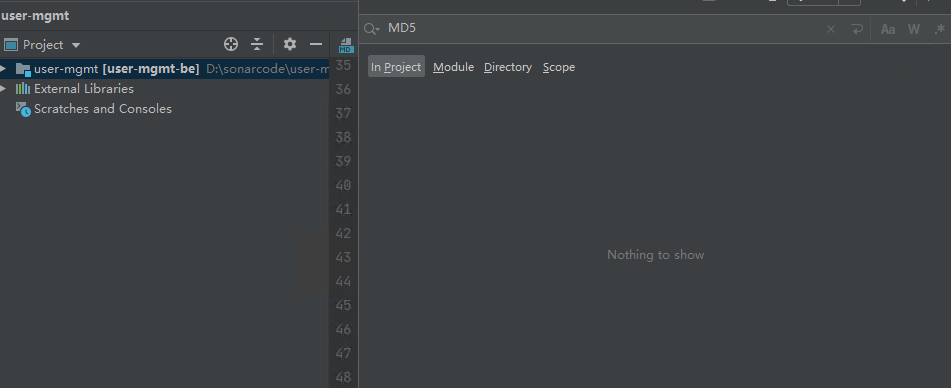


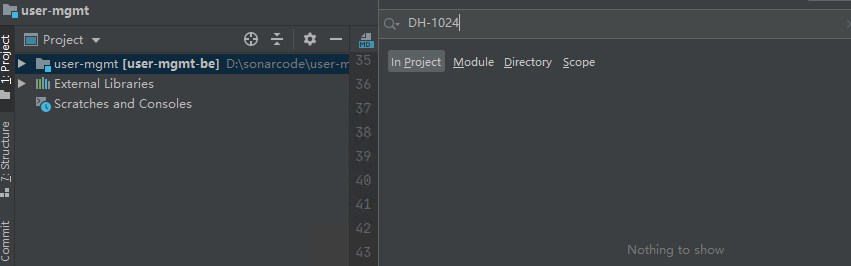


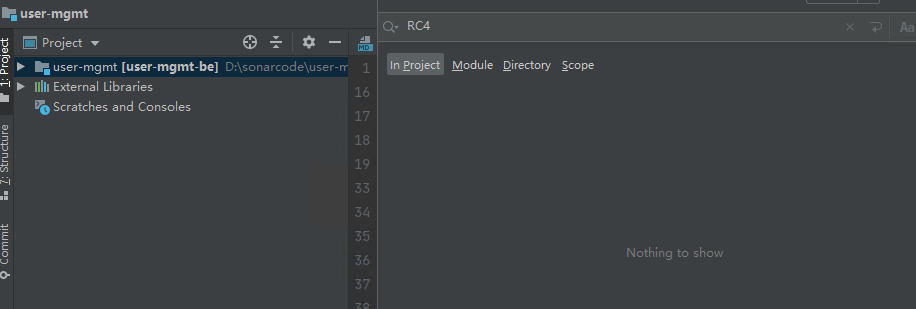


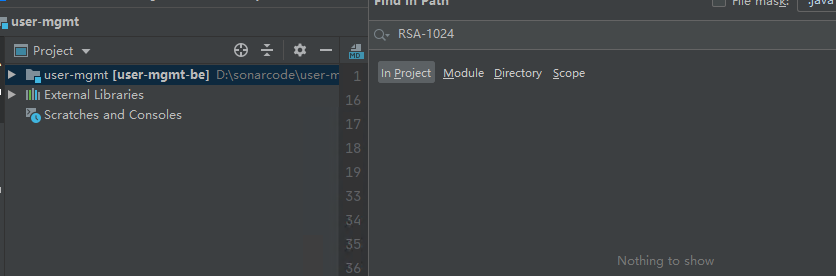
### User-mgmt

没有找到DES, RC4，RSA-1024,MD 1，MD2,MD5,DH-1024等不安全算法。

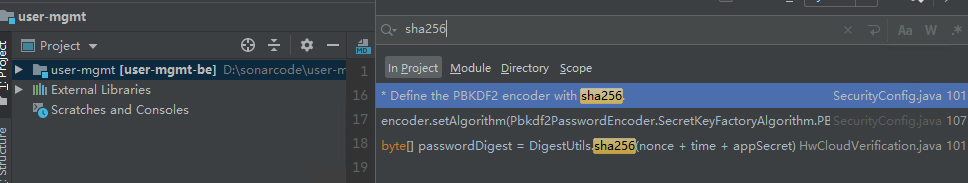


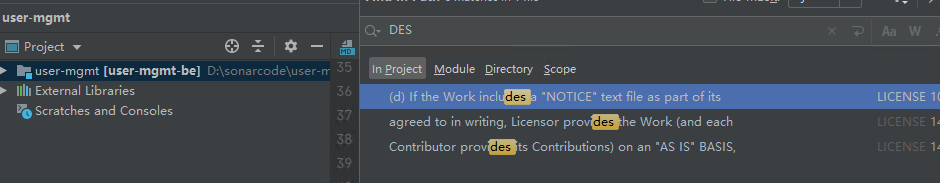






使用sha256安全算法。



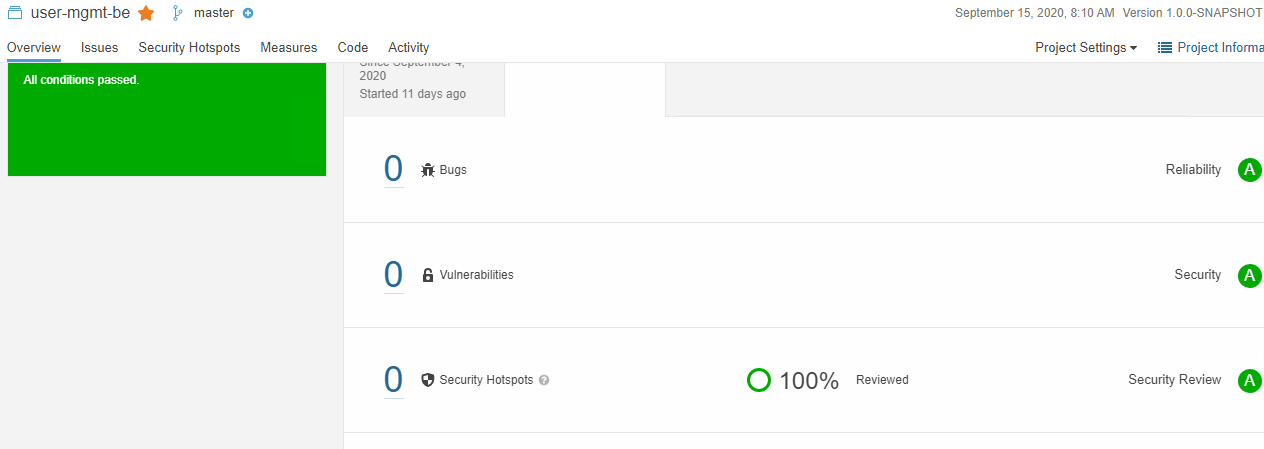


**结论：通过**

## Test case EG-TST-SEC-CP-4-3

### User-mgmt

Sonarqube没有扫出不硬编码

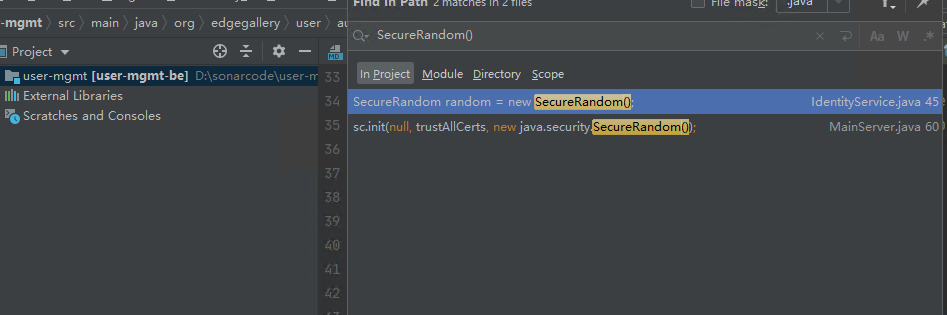


**结论：通过**

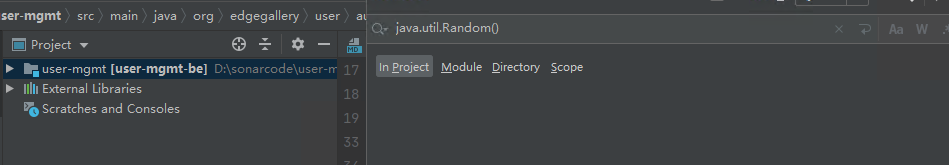
## Test case EG-TST-SEC-CP-4-4

### User-mgmt

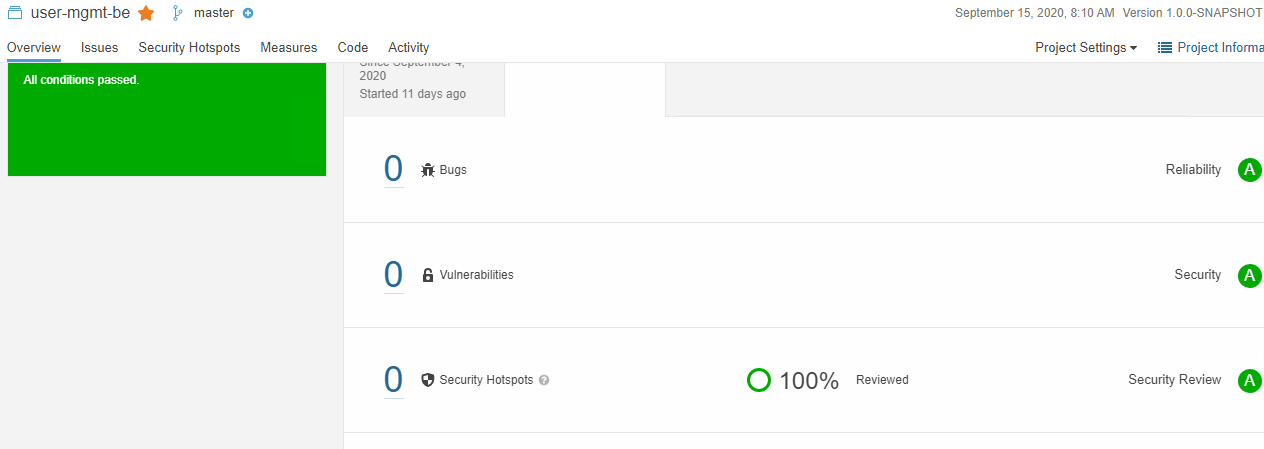
使用安全的随机数方法。



未使用不安全随机数的引用



Sonarqube没有扫出不安全随机数方法



**结论：通过**

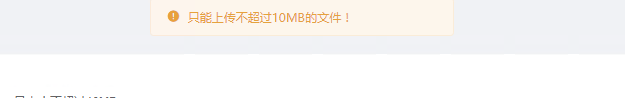
**未找到java.util.Random引用，是通过java.security.SecureRandom()生成随机数**

## Test case EG-TST-SEC-CP-5-3

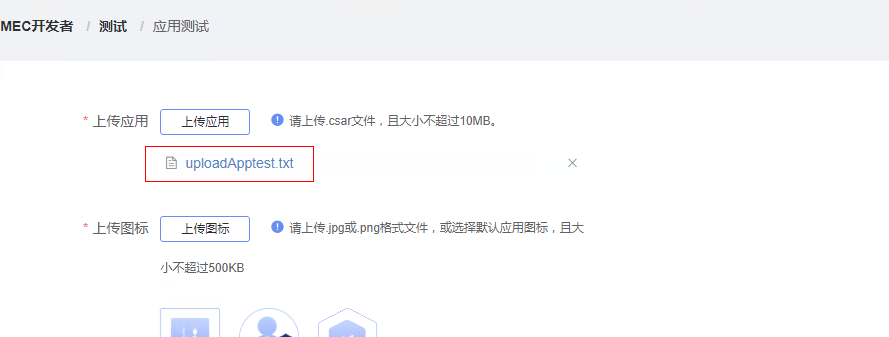
摸底测试时正常的，由于环境原因布置的代码不是最新，加上代码冻结，所以问题遗留

### Developer

上传文件做了大小限制

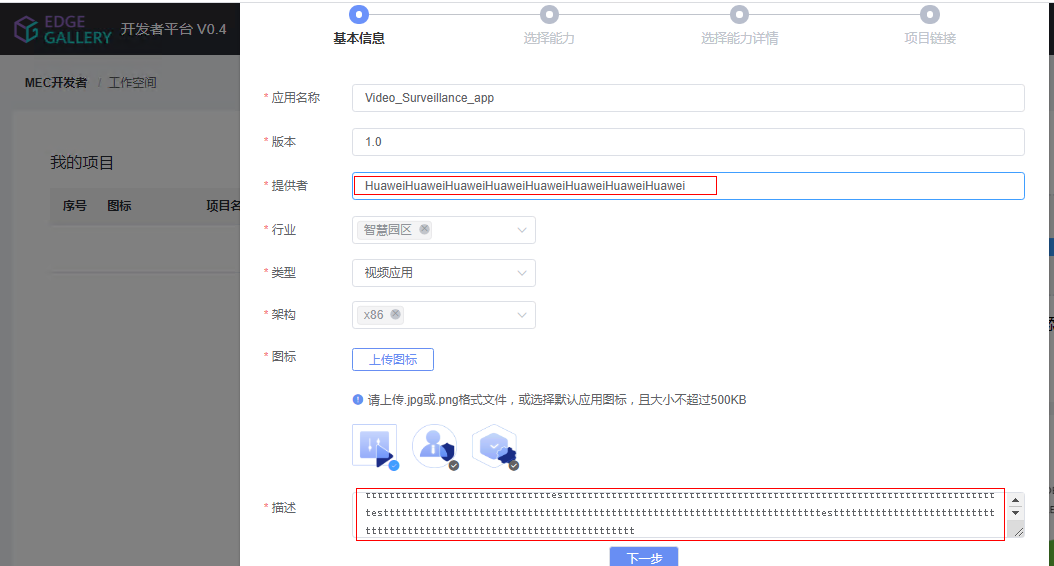


上传应用文件前台类型没有做限制





输入字符大小没有做限制。输入异常大的字符，也会项目创建成功





Cisa包正常



### AppStore

上传文件有大小限制：



上传文件类型做了限制



上传正常的可以成功



### 注：做了文件类型和大小的限制， 但是验证cisa包功能没有，计划到下个版本，所以炸弹攻击测试不涉及。

### 测试结果：不通过

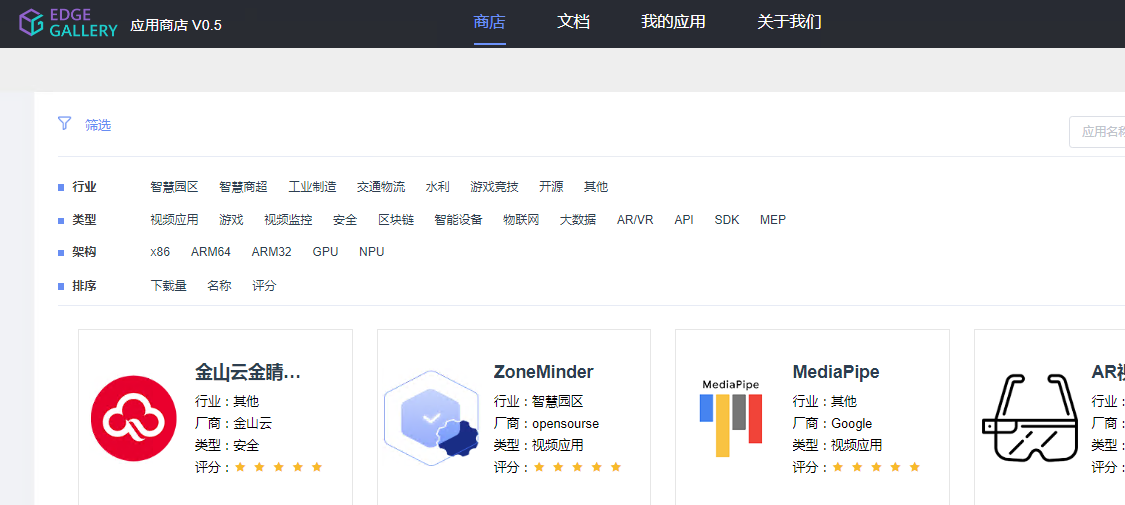
注：developer输入输入大小没有做限制， 前台创建项目上传cisa包类型没有限制。

## Test case EG-TST-SEC-CP-6-4

当前失效时间是一小时。

### Appstore

失效时间是1小时，一小时过后，刷新页面重定向到登录页面。





不刷新，直接操作界面，会出现回去数据失败。也不会跳转到登录页面



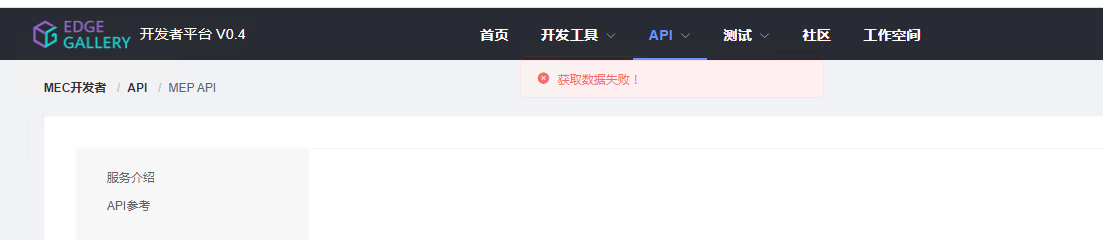
### Developer

失效时间是1小时，一小时过后，刷新页面重定向到登录页面。





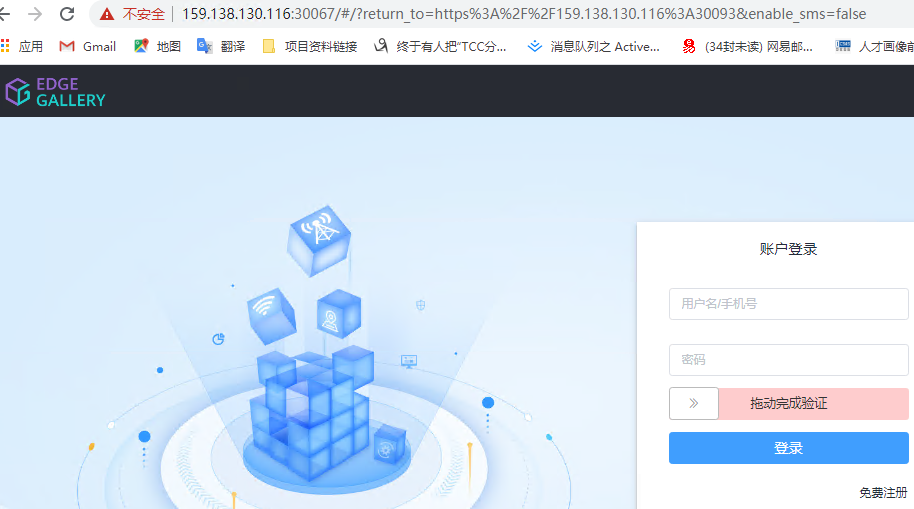
不刷新，直接操作界面，会出现回去数据失败。也不会跳转到登录页面



### Mecm

失效时间是1小时，一小时过后，刷新页面重定向到登录页面。





不刷新，直接操作界面，会出现回去数据失败，也不会跳转到登录页面



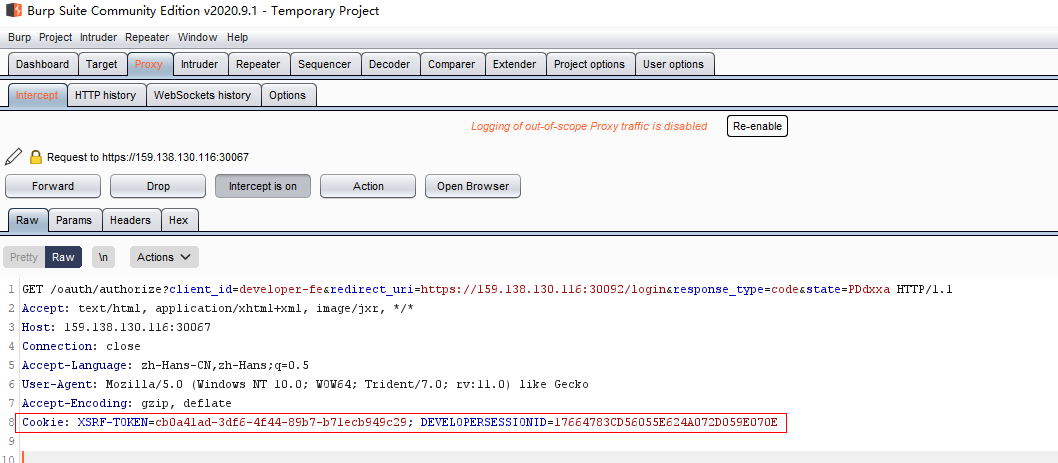
### 测试结果：通过

注：如果在以前基础上继续操作，需要手动刷新才会跳转到登录界面，不会自动跳转。（issue）

## Test case EG-TST-SEC-CP-6-3

### Appstore

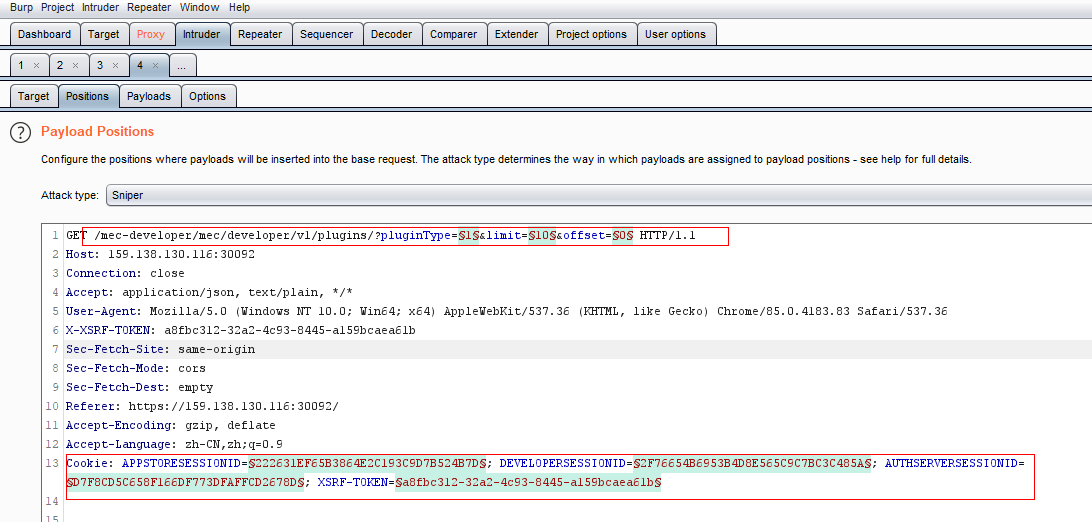
### ADeveloper

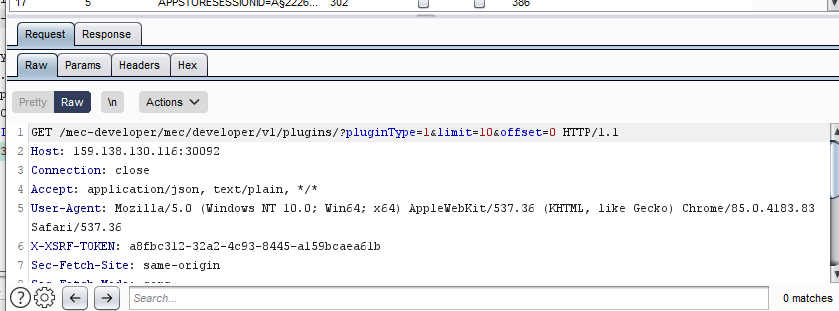


获取插件的接口，

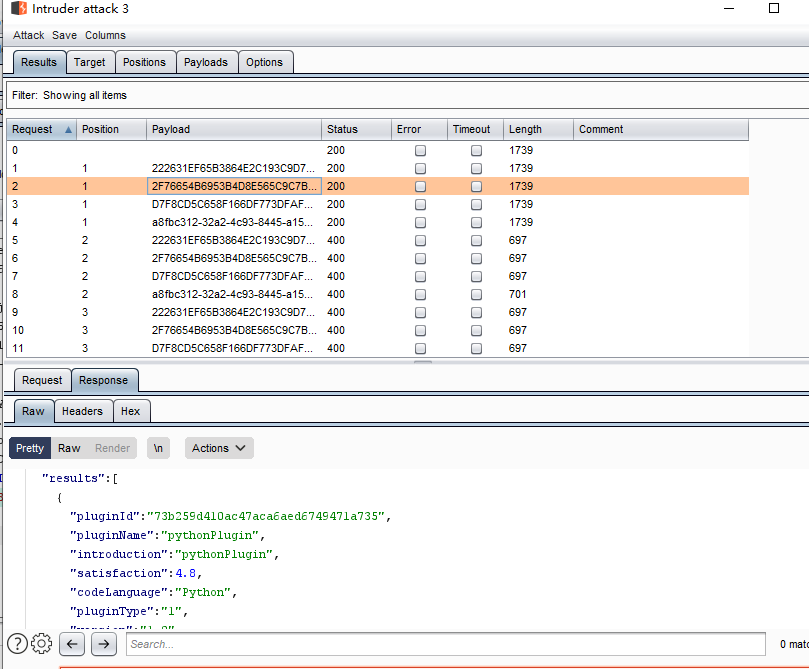


第一次Intruder

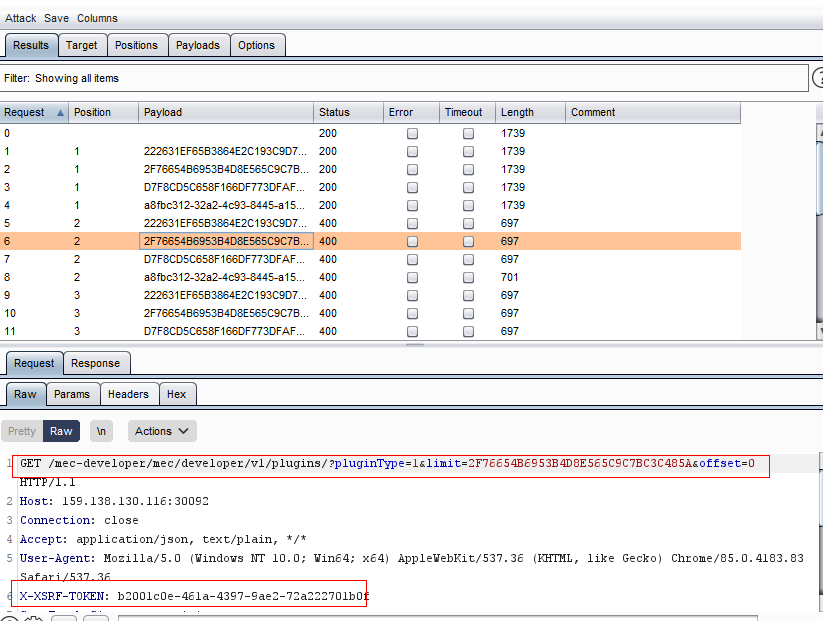




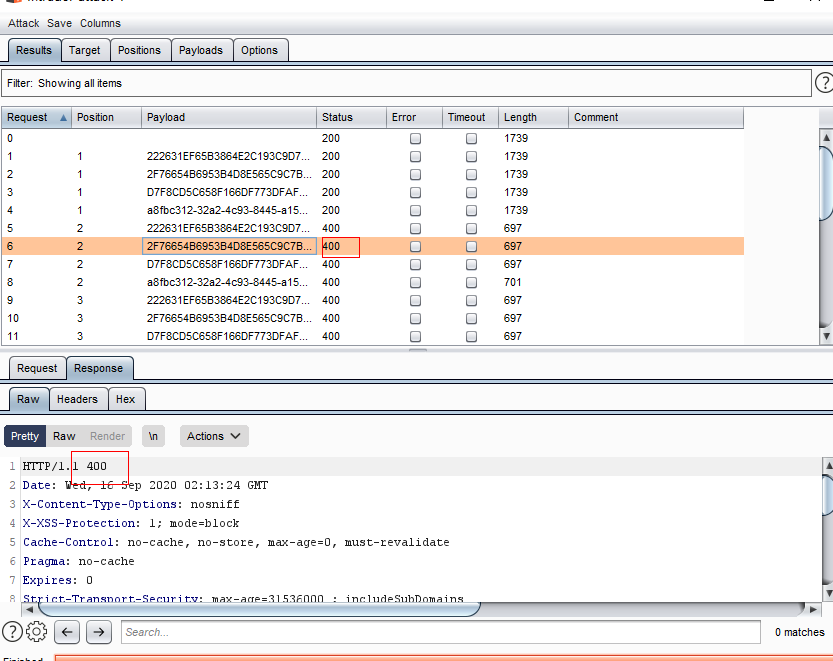
第一次instruder的响应。



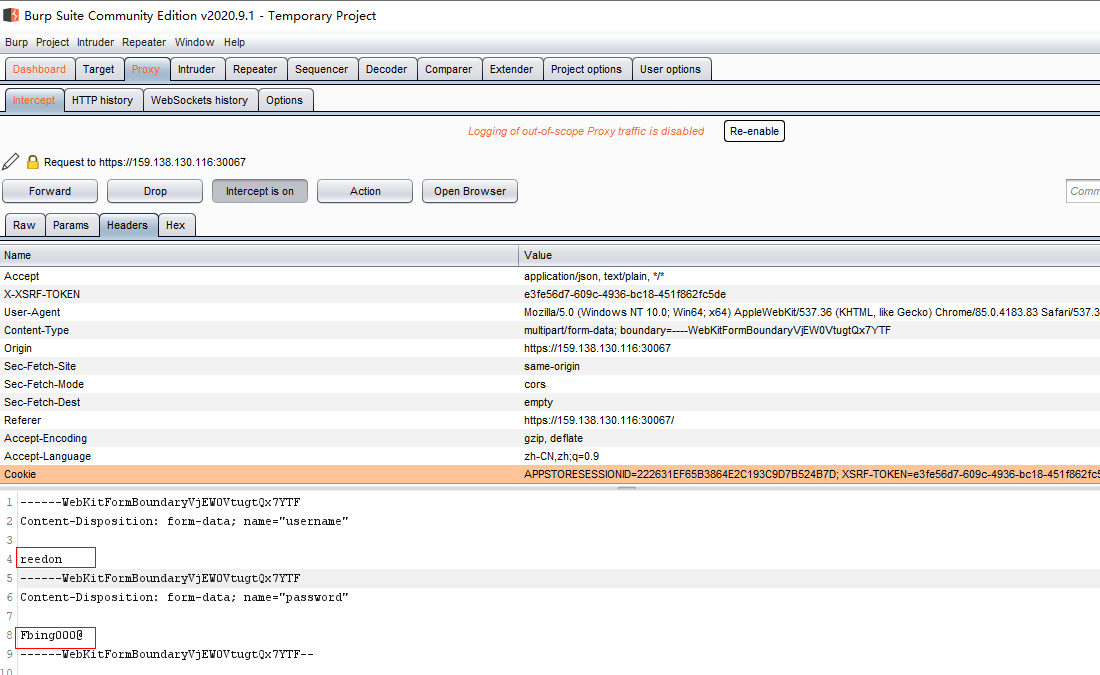
退出登录后，中心登录，第二次使用第一次登录的token，intruder,获取插件接口



第二次请求返回接口，400失败，参数错误



可以拦截到密码：

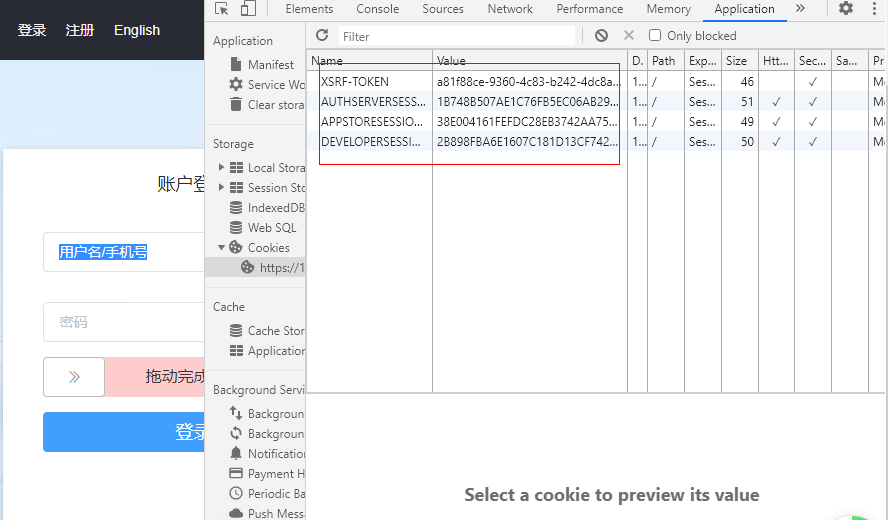


## Test case EG-TST-SEC-CP-6-4

### Appstore

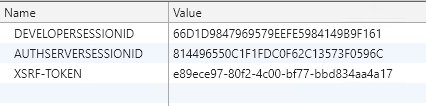
重新登录token不一致，DevelopSessionID一致。

退出登录seesionID和token未清除：

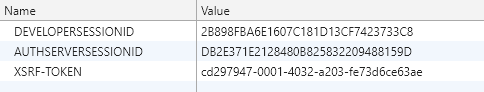


### Developer

退出登录seesionID和token未清除：



第二次登录：



### MECM(环境未好)

前台与后台均使用UTF-8编码

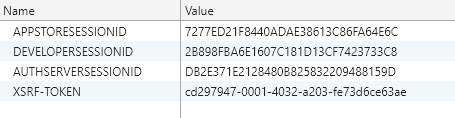
### 测试结果：通过

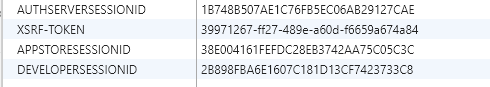
## Test case EG-TST-SEC-CP-6-5

### Appstore

重新登录token不一致，DevelopSessionID一致。

第一次登录：

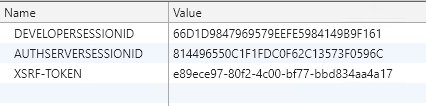




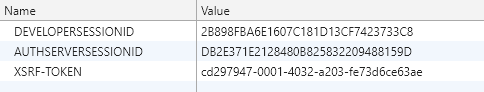
### Developer

重新登录seesionID和token不一致

第一次登录：



第二次登录：



### MECM(环境未好)

前台与后台均使用UTF-8编码

### 测试结果：通过