若依 sql注入

若依4.6.0 (版本<4.6.2)

查询时候对参数拼接导致sql注入

复现的主要问题在于burpsuite抓包设置代理和证书这里总是出现问题

出现漏洞点是在系统管理的角色管理的查询

图形用户界面, 文本, 应用程序, 电子邮件, 网站

描述已自动生成

使用burpsuite对该接口抓包

图形用户界面, 文本, 应用程序, 电子邮件

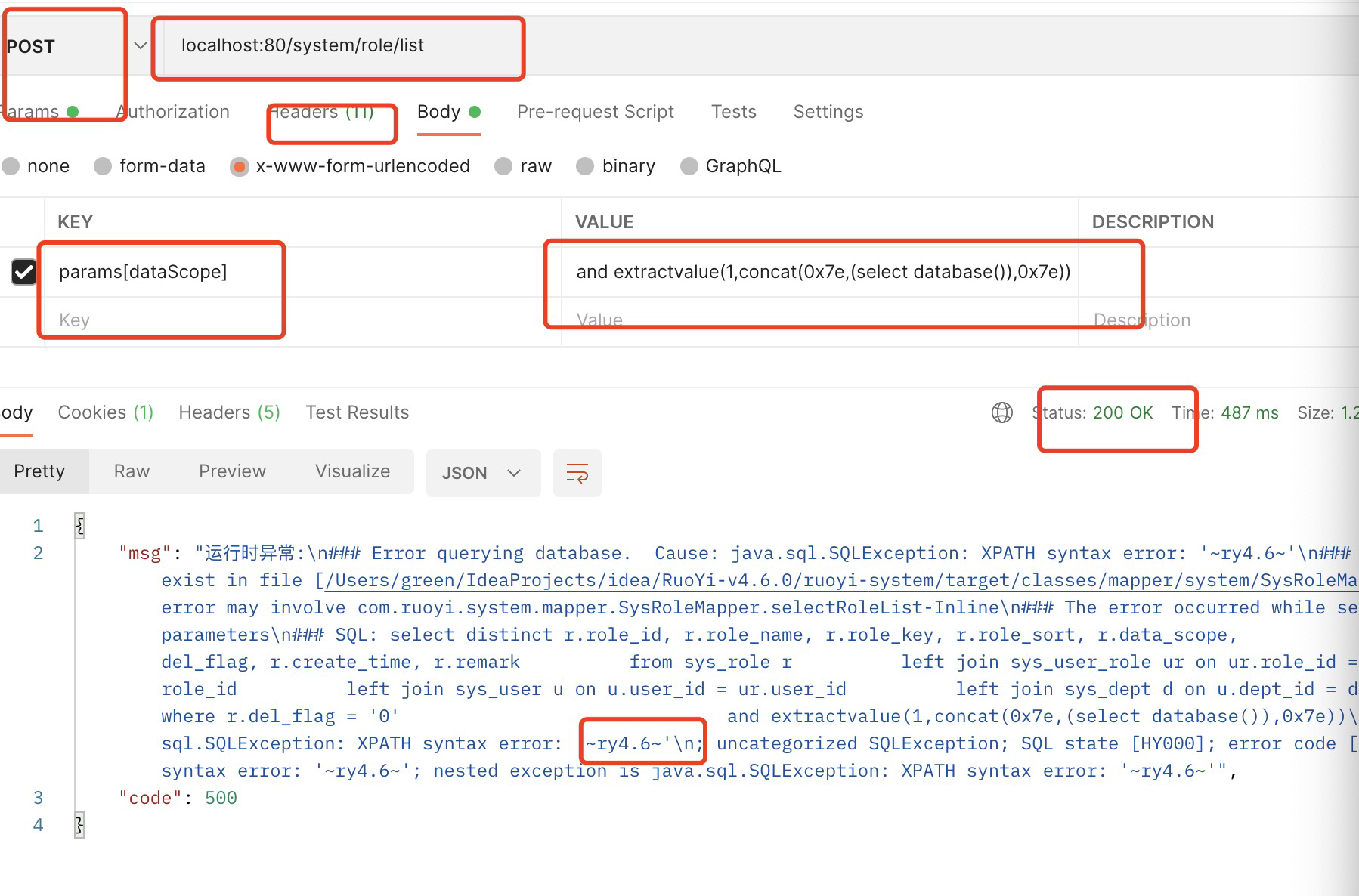
描述已自动生成

因为那个burpsuite重发比较慢就直接使用postman发请求

Payload如下

pageSize=10&pageNum=1&orderByColumn=roleSort&isAsc=asc&roleName=&roleKey=&status=&params%5BbeginTime%5D=&params%5BendTime%5D=&params[dataScope]=and extractvalue(1,concat(0x7e,(select database()),0x7e))

实际是加了params[dataScope]=and extractvalue(1,concat(0x7e,(select database()),0x7e))



Cookie要加到header里 要不然进不去接口里

使用post请求 在body里添加参数

发请求之后就能在返回体里看见数据库的名字 数据库名就被注入出来了

解析下源码

查询的代码直接把输入的参数给查出来 没有做过滤处理

Mapper里

***<***if test="dataScope != null and dataScope != ''"***>*** AND r.data\_scope = #{dataScope}  
***</***if***>***