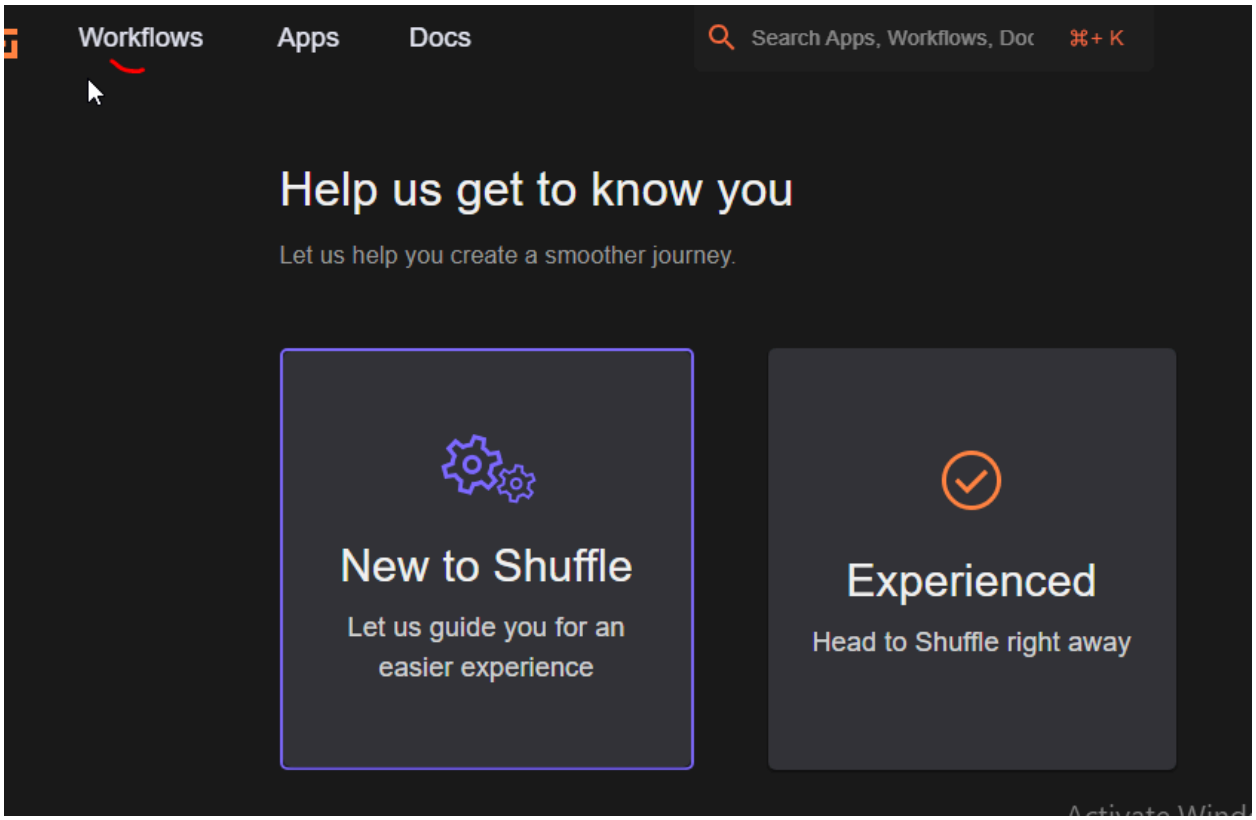
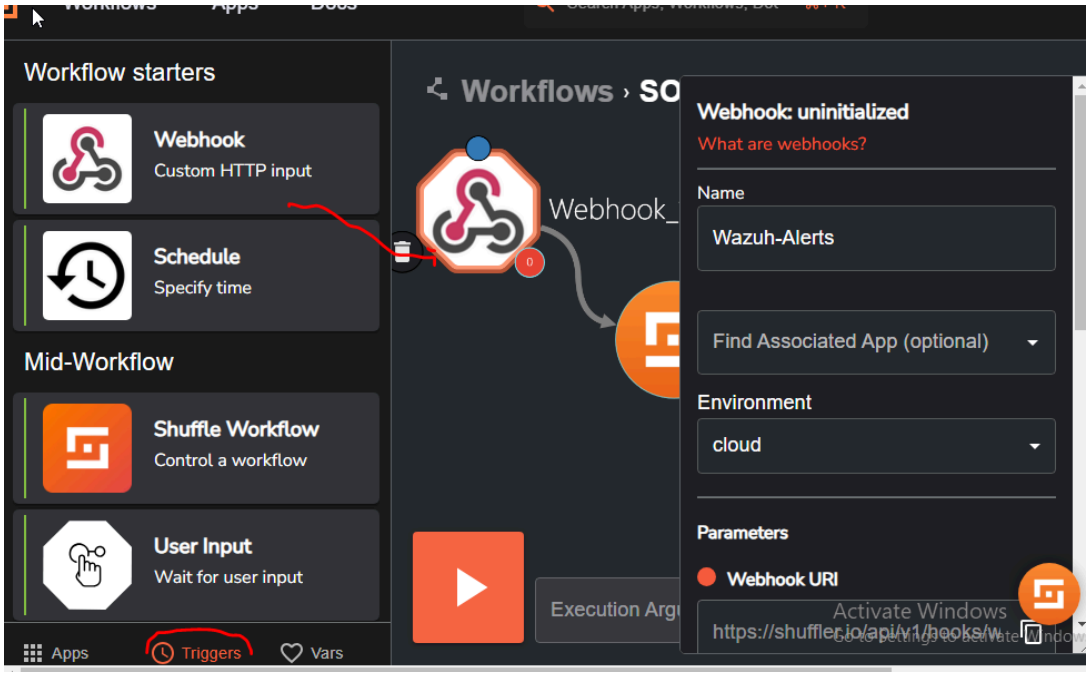
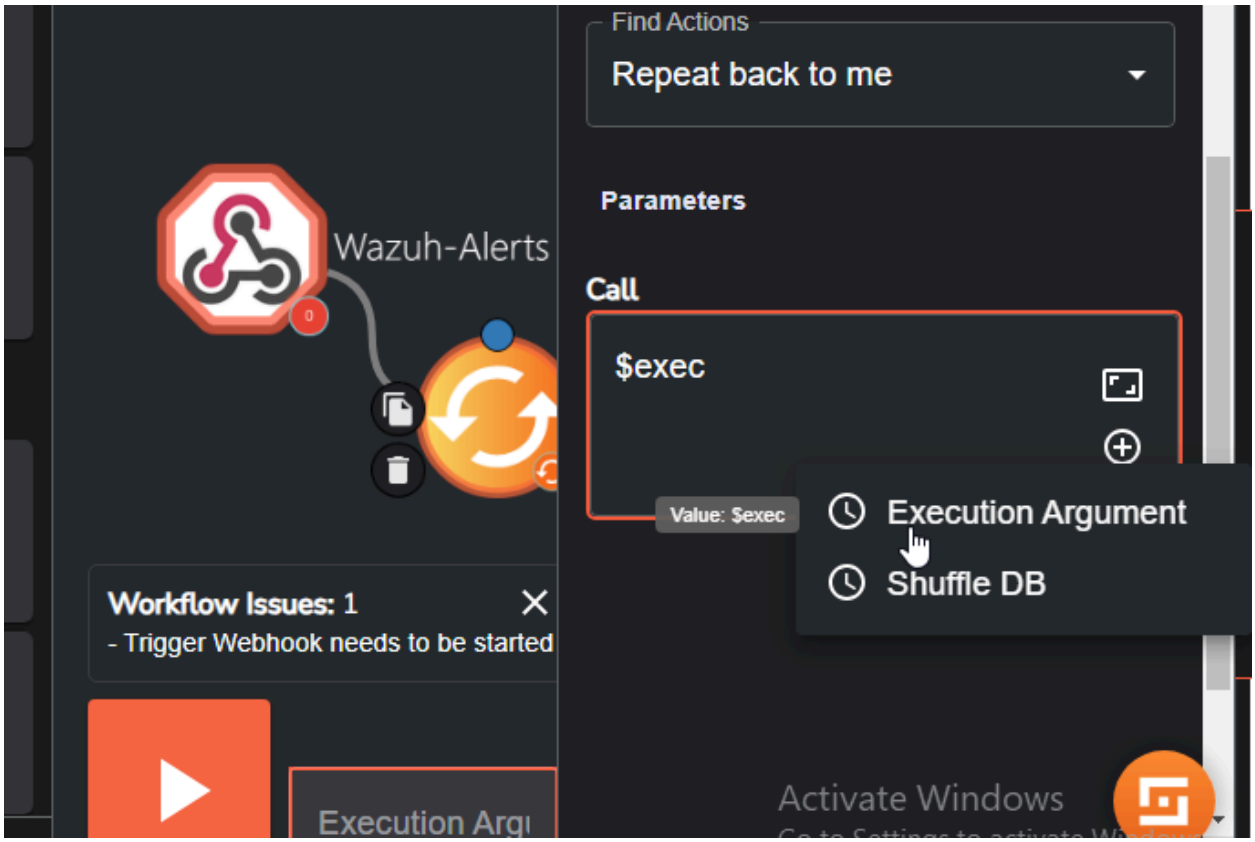
Go to shuffle.io and register for free and go to workflows



On the bottom left I selected triggers and dragged Webhook trigger onto the workflow. The on the right I renamed it to Wazuh-Alerts and copied the URI. We need this URI copied to our ossec posted on the Wazuh Manager.



Next I selected Change me, removed the “hello world” and added the $exec as the execution argument



Save and go to wazuh manager.

We need to connect Wazuh to Shuffle by adding an integration tag within our ossec.conf file.
I added an integration here after </global>
And set the rule id to match our rule in wazuh

```
  <smtp_server>smtp.example.wazuh.com</smtp_server>
  <email_from>wazuh@example.wazuh.com</email_from>
  <email_to>recipient@example.wazuh.com</email_to>
  <email_maxperhour>12</email_maxperhour>
  <email_log_source>alerts.log</email_log_source>
  <agents_disconnection_time>10m</agents_disconnection_time>
  <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
</global>

<integration>
  <name>shuffle</name>
  <hook_url>http://https://shuffler.io/api/v1/hooks/webhook_7b2b2359-431e-4fd4-9da9-ccc30d104f64 </hook_url>
  <rule_id>100002</rule_id>
  <alert_format>json</alert_format>
</integration>

<alerts>
  <log_alert_level>3</log_alert_level>
  <email_alert_level>12</email_alert_level>
</alerts>

<!-- Choose between "plain", "json", or "plain,json" for the format of internal logs -->
<logging>
  <log_format>plain</log_format>
</logging>
```

Restart wazuh manager service as we made changes to ossec.

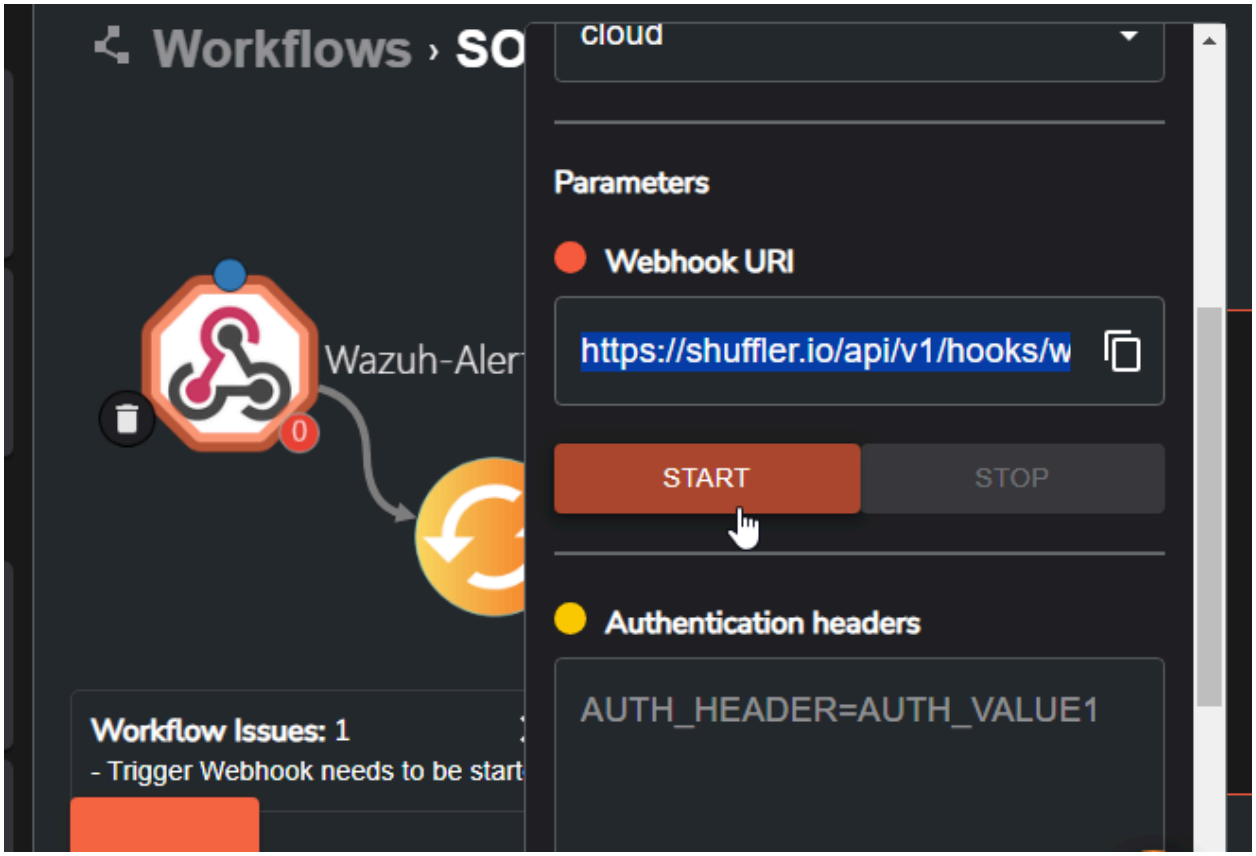
```
root@Wazuh:/var/ossec/logs/archives# root@Wazuh:/var/ossec/logs/archives# nano /var/ossec/etc/ossec.conf
root@Wazuh:/var/ossec/logs/archives# systemctl restart wazuh-manager.service
```

Next we will go regenerate our mimikatz on windows client machine

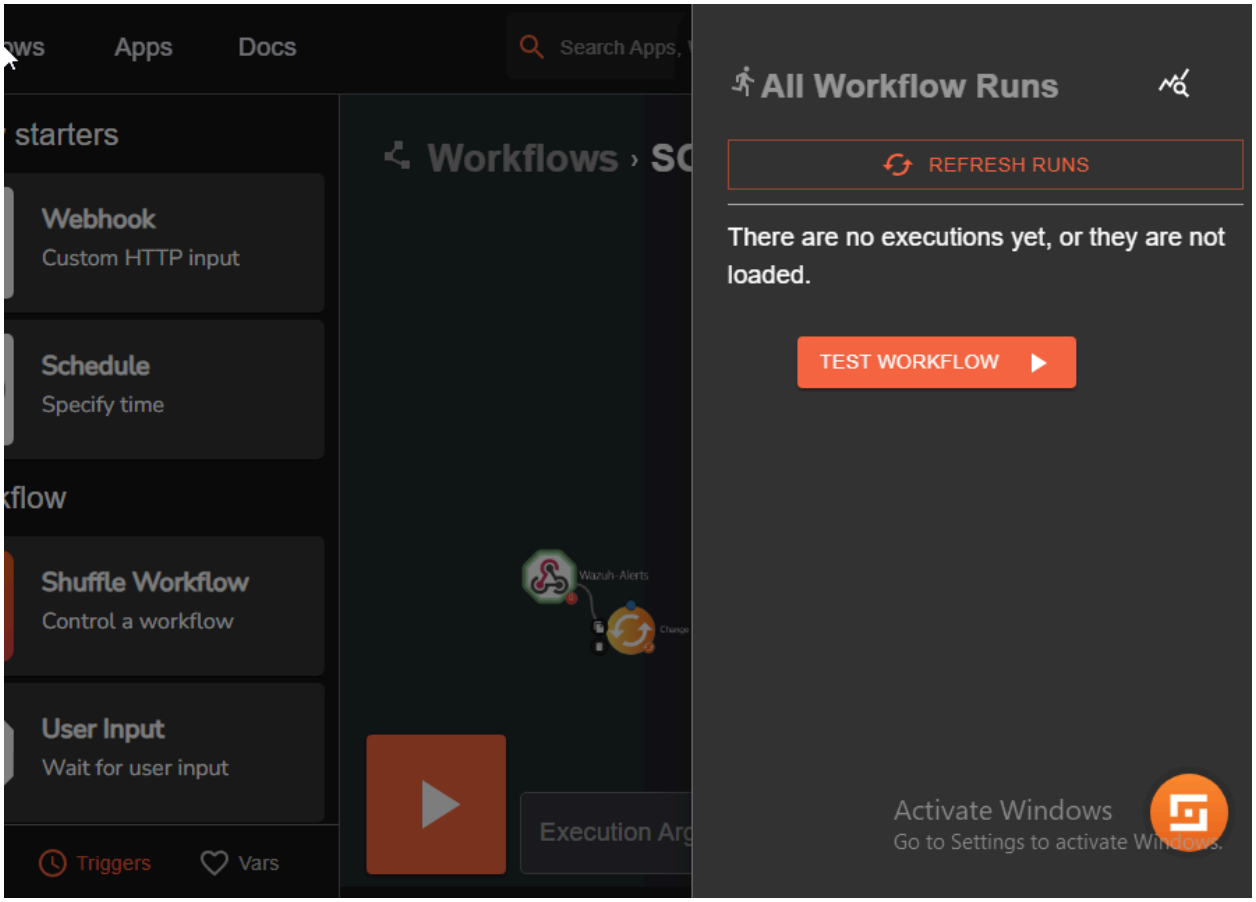
```
mimikatz # exit
Bye!
PS C:\Users\knuj9\Downloads\mimikatz_trunk\x64> .\youareawesome.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/
```

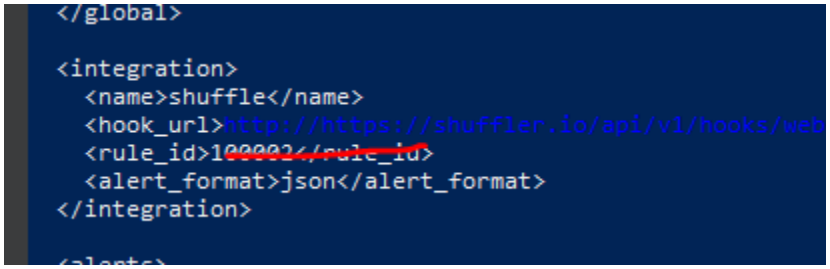
Next go over to shuffle and select your webhook and click start.



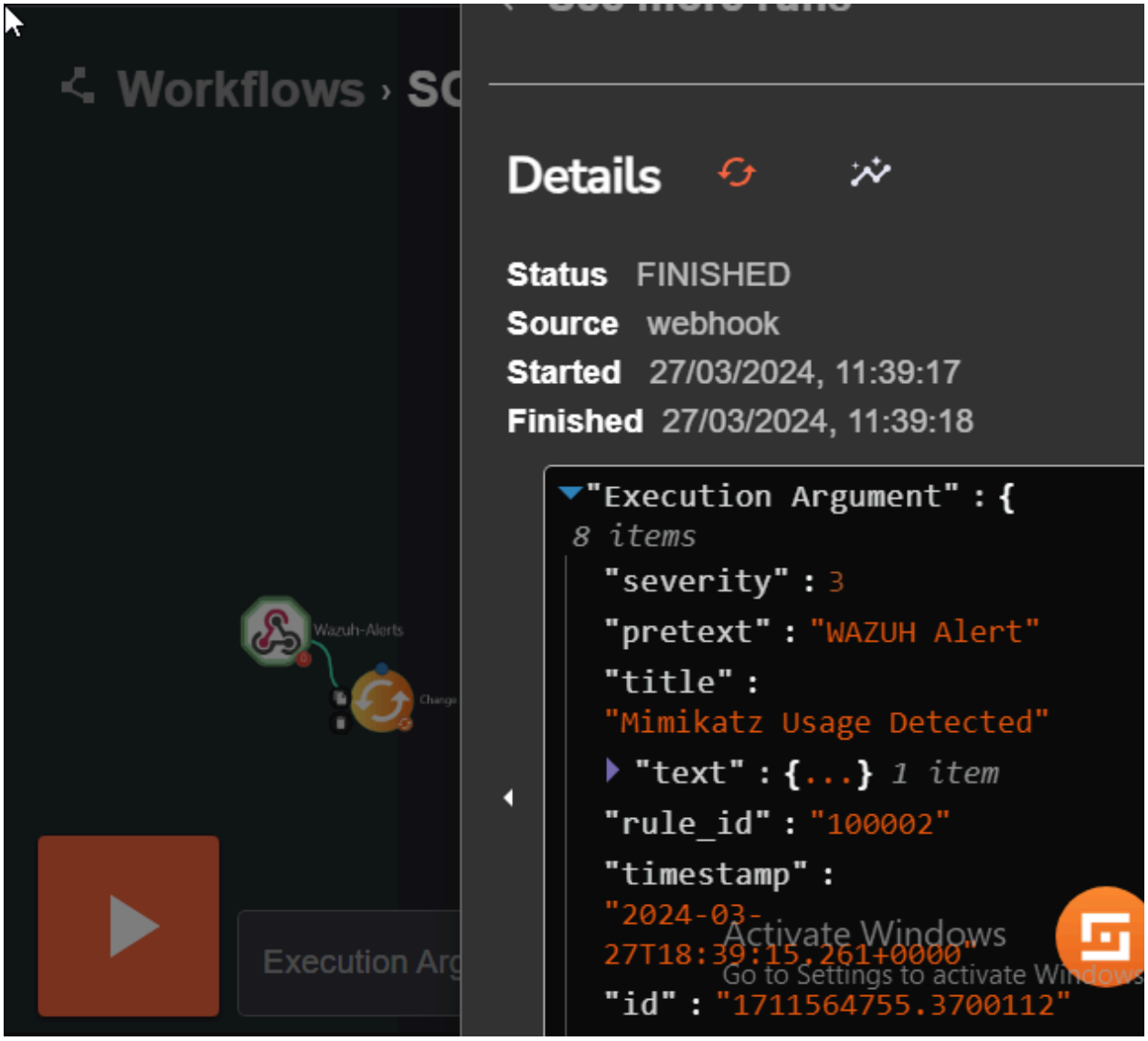
Click on the person icon on the bottom and you can see that nothing came up in our workflow
So we will need to trouble shoot



Going back to our wazuh manager ossec file I can see the link I copied has http://https://



I will remove the http part, save, restart the wazuh manager and try again.



And now our workflow has picked up the mimikatz and alerted us (: