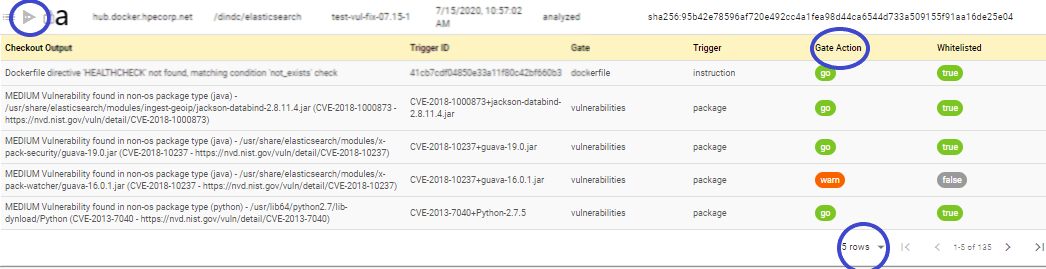
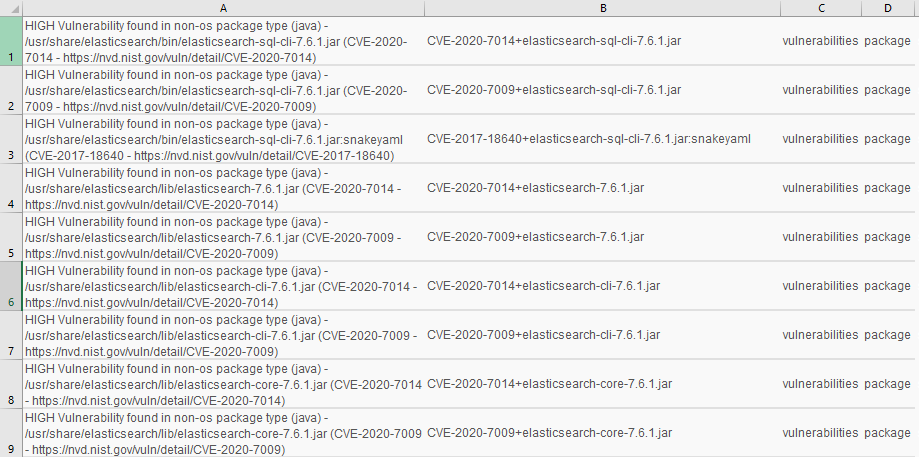
## Steps to Follow for analyzing vulnerabilities:

### Copy the Vulnerabilities to an Excel sheet and start with analysis

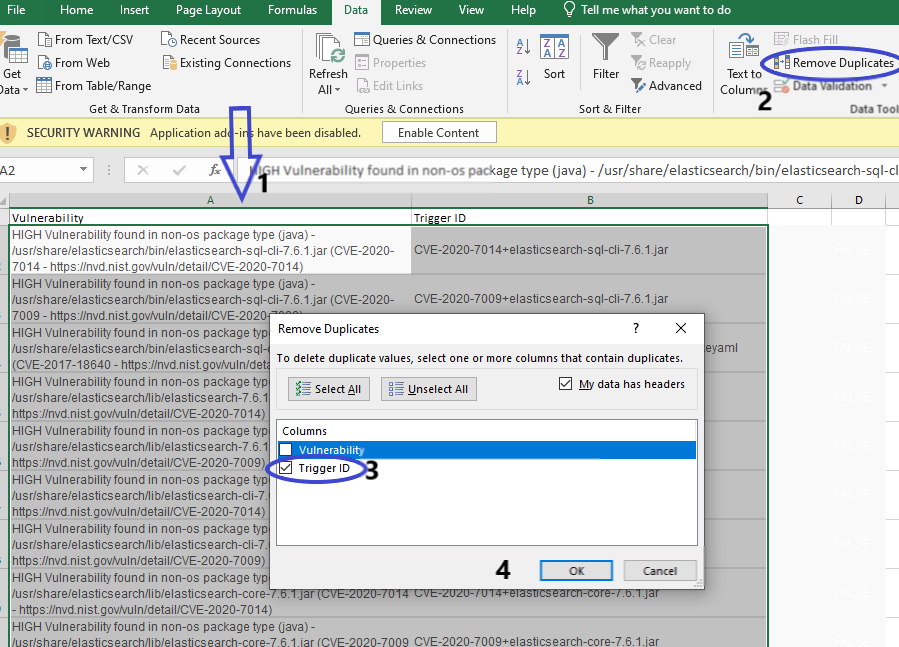
1. Open the Policy evaluation report from Anchore Dashboard and increase the number results as needed (Ex 100).
2. Sort the table by Gate Action column and copy all the vulnerabilities with Stop Gate Action to an excel sheet.

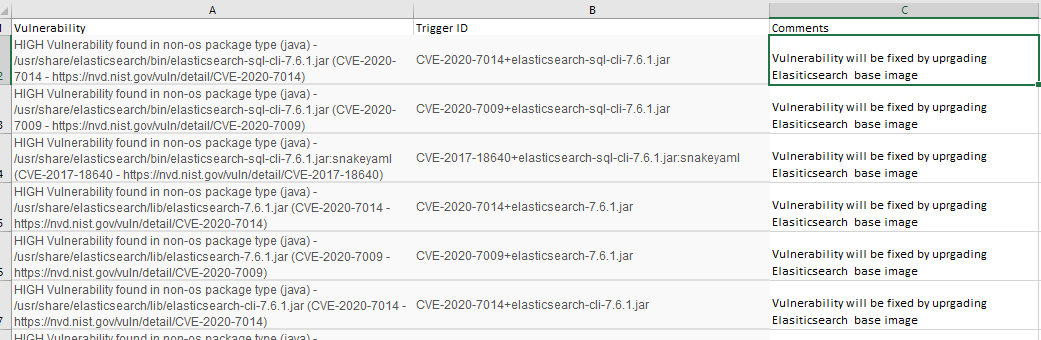


To

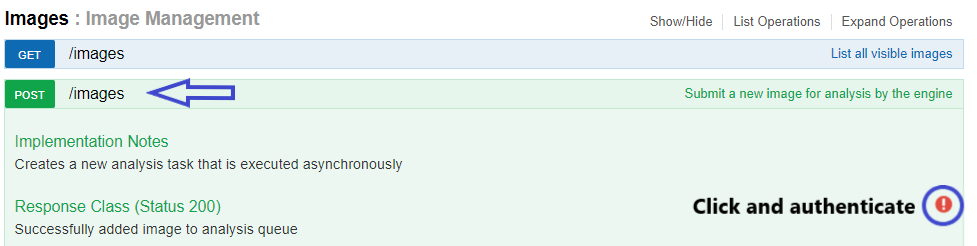


1. Remove Duplicates of Trigger ID and start fixing the vulnerability/Document the challenge in fixing for whitelisting.





1. Apply the fix if available to Docker image, build the new image and push to a DTR repo.
   1. In case of an Application Package try upgrading to a version that the vulnerability has a fix
   2. In case of an OS Package try upgrading the package by yum update
   3. Or any other fix specific to the vulnerability
2. Scan the newly built image and repeat (1) and (2) until the report has zero vulnerabilities.
   1. Login to [Anchore API Swagger UI](https://anchore.dc01.its.hpecorp.net/v1/ui/#/) with the credentials shared internally and authenticate under Image post request



* 1. Submit the image scan request for the newly built image by providing image tag in below format and click “Try it out!”. If you see a 200 response then the image is submitted for analyzing. Repeat step (1) i.e., please check the dashboard and search for the submitted image for viewing the updated vulnerabilities list.

