PoC : Integration of container vulnerability tool with rails

Integration with rails/heroku application

We can install trivy using apk command, docker run or binary : ref

1. Apk-command:

This will require access to the server which will be redundant and unnecessary setup every time the server goes down.

2. Docker run

This requires a docker daemon running in the server
1. Heroku has a container image deployment strategy but it was difficult to implement and was not working. Reference
2. Start own server
    Con : We will have to maintain a separate server
    Pro: will not make the application heavy and more of a microservice approach

3. Binary:

Download as binary and add it to rails directory and can be directly used

Pro: No need to maintain a separate server
Con: the binary is 190 MB and hence makes deployment heavy(monilithic approach)

4. **Buildpack to install trivy on the go i.e during deployment - finalised**

a. Public repo : https://github.com/tamu-edu-students/buildpack-trivy/blob/main/bin/compile
   This is a buildpack which will install trivy and add it to path
b. Import buildpacks
   I. heroku buildpacks:set heroku/ruby --index 1 -a <app-name>
   Ii. heroku buildpacks:add https://github.com/tamu-edu-students/buildpack-trivy --index 2 -a <app-name>
   Note : order is very important

Buildpacks

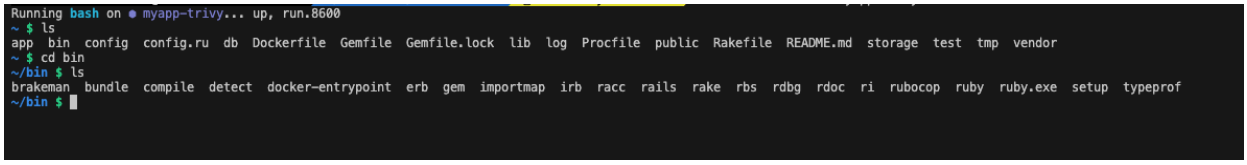
1. Buildpacks are used to install additional dependencies and prepare dyno for application to be deployed
2. The scripts are to be assigned to open source git repository and added to heroku app before pushing the application - **this is a one time task**

How to verify if the dependencies are installed ?

The files created during the non-build process in heroku are ephemeral and that is the reason all dependencies must be assessed during build process and not in Procfile.

To verify the installation:
1. Check the logs of installations when application is pushed to heroku (this is when heroku detected buildbacks and runs the scripts)
2. Run `heroku run bash -a <app-name>`
3 This will give remote access to dyno and /app/bin is where binary should be installed

Before:



Debugging:

```
remote:        For more information see:
remote:          https://devcenter.heroku.com/articles/ruby-versions
remote:
remote:
remote: -----> installing trivy app detected
remote: ------------------------- Downloading Trivy version 0.39.0 ------------------------------------------------------------------
remote:   % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
remote:                                  Dload  Upload   Total   Spent    Left  Speed
remote:   0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
remote: 100 48.2M  100 48.2M    0     0  33.6M      0  0:00:01  0:00:01 --:--:-- 39.6M
remote: -----> Discovering process types
remote:        Procfile declares types     -> web
remote:        Default types for buildpack -> console, rake
remote:
remote: -----> Compressing...
remote:        Done: 92.6M
remote: -----> Launching...
remote:        Released v9
remote:        https://myapp-trivy-5b7503bf213d.herokuapp.com/ deployed to Heroku
remote:
remote: This app is using the Heroku-22 stack, however a newer stack is available.
remote: To upgrade to Heroku-24, see:
remote: https://devcenter.heroku.com/articles/upgrading-to-the-latest-stack
remote:
remote:  !
remote:  ! ## Warning - The same version of this code has already been built: c7f8528dbecc7d23b24aef5d4647636236f8932e
remote:  !
remote:  ! We have detected that you have triggered a build from source code with version c7f8528dbecc7d23b24aef5d4647636236f8932e
remote:  ! at least twice. One common cause of this behavior is attempting to deploy code from a different branch.
```

```
 $ ls
pp  bin  config  config.ru  db  Dockerfile  Gemfile  Gemfile.lock  lib  log  Procfile  public  Rakefile  README.md  storage  test  tmp  vendor
 $ cd bin
/bin $ ls
rakeman  bundle  compile  contrib  detect  docker-entrypoint  erb  gem  importmap  irb  LICENSE  racc  rails  rake  rbs  rdbg  rdoc  README.md  ri  rubocop  ruby  ruby.exe  setup  trivy  typeprof
/bin $
```