**LABORATORIUM: Programowanie Aplikacji w Chmurze Obliczeniowej**

**Zadanie 2**

Podstawą do wykonania zadania jest przykład analizowany w trakcie laboratorium nr 9. Przykład ten zawiera łańcuch CI dla usługi Github Actions pozwalający na zbudowanie obrazu Docker dla dwóch architektur sprzętowych wraz z metodą tagowania tego obrazu oraz z wykorzystaniem cache w procesie jego budowania.

Ten przykład należy uzupełnić o testowanie obrazu pod kątem podatności na zagrożenia w oparciu o usługę Docker Scout. Sposób uzupełnienia łańcucha opiera się o informację zawarte w materiałach wykładowych i laboratoryjnych jak i dokumentacji środowiska Docker:

https://github.com/docker/scout-action
https://docs.docker.com/scout/integrations/ci/gha/

**W rozwiązaniu należy:**

- wykorzystać aplikację z zadania nr 1,
- wykorzystać łańcuch CI z lab. 9,
- do łańcucha dodać test CVE obrazu, który zapewni, że obraz zostanie przesłany do swojego **publicznego** repozytorium obrazów na Github (ghcr.io) **tylko wtedy** gdy nie będzie zawierał zagrożeń sklasyfikowanych jako krytyczne lub wysokie.

**Sprawozdanie:**

Sprawozdanie należy wykonać jako repozytorium na Github wraz z plikiem README.md, w którym krótko będzie opisane jak skonfigurowano wymagany test. Opracowany łańcuch CI powinien być przynajmniej raz uruchomiony tak by potwierdzić poprawność jego działania.