# **Secure Software Supply Chain Implementation**

This project demonstrates the implementation of advanced security controls and automation for a secure software supply chain, focusing on the integrity and authenticity of code and container images.

Tools:

**GPG (GNU Privacy Guard)**: For signing Git commits.

**Cosign**: For signing and verifying container images and generating attestations.

**SLSA (Supply-chain Levels for Software Artifacts)**: A framework for ensuring software integrity, with provenance generation.

Implementation :-

Step 1 :

Enforcing GPG signed commits. Generate a GPG public key stored it in the github settings, and applied the branch protection rule.

A verified signed commit in the repo.

Step 2:

Install cosign and generated public and private key.

Stored it in github secrets.

Step 3:

Wrote a basic python/flask code , its dockerfile, requirements.txt

Step 4 :

Wrote a github actions workflow which first build and push image to ghcr.

Then sign the container image and generate Generate SLSA Provenance Attestation.

Step 5 :

The next stage of pipeline verifes the image which ensures that only verified image go for deployment.

Challenges Faced:

No such things as challenge but I tried Github Container Registry for the first time(on my own), found some new things like we cannot push a image in ghcr with a name which contians Upper Case.

More Screenshots:

