# CTF Quest

## Challenge Name: Docker Layer Leak

*by OM3N*

## Challenge Overview

An internal build artifact named image.tar was provided. The description suggested sensitive data was removed but might still exist inside the file.

## Step 1 – Extract Archive

The archive was extracted using tar -xf image.tar to reveal Docker image layers.

## Step 2 – Inspect Layers

Each directory contained a layer.tar file representing filesystem changes in Docker.

## Step 3 – Search for Flag

A recursive search was performed to find any flag-related files.

## Step 4 – Whiteout Discovery

A file named .wh.flag.txt was discovered, indicating deletion of flag.txt in a newer layer.

## Step 5 – Recover Flag

The original flag.txt was located in an earlier layer and contained the hidden data.

## Final Flag

SECE{layers_never_forget}

## Conclusion

Docker images retain data in previous layers. Deleted files may still be recovered from older layers.