1. Our model is vulnerable to what types of attacks? Can we say adversarial attacks?