# Brute Force Attacker vs Rate Limiter/Account Lockout Attack:

A simple Python brute force script will be developed which tries multiple passwords automatically against a dummy login form on a test Flask web app hosted locally. The attack will demonstrate how repeated login attempts can be automated.

## Defense:

A rate limiter and account lockout system will be implemented in the same Flask login form. After a certain number of failed attempts (e.g., 5), either rate limiting will block more attempts for some time, or the account will be locked out and an alert generated (log/console message).

## Lab Target:

Both testing and defense will be done on a simple Flask-based login system running on an isolated VM/local environment. No real user data or external targets involved.

## Objective:

This assignment aims to practically show how brute-force login attacks are done and demonstrate web-level defenses using basic scripting and logic.