**Practical Exercise 35 - Preventing Script Injection via Intermediate Variables**

**Exercise Description**

**In this practical exercise, our goal is to get familiar with preventing script injection attacks in GitHub Actions.**

Here are the instructions for the exercise:

1. Create a file named 20-workflow-security.yaml under the .github/workflows folder at the root of your repository.
2. Name the workflow 20 - Workflow Security.
3. Add the following triggers to your workflow:
   1. pull\_request
4. Add a single job named unsafe-pr to the workflow.
   1. It should run on ubuntu-latest.
   2. It should contain two steps:
      1. The first step should checkout the code using the appropriate third-party action.
      2. The second step, named Check PR title, should run the following shell script (it checks whether the PR title starts with the substring feat and prints a message accordingly):
         1. title=${{ github.event.pull\_request.title }}
         2. if [[ $title =~ ^feat ]]; then
         3. echo "PR is a feature"
         4. exit 0
         5. else
         6. echo "PR is not a feature"
         7. exit 1
         8. fi
5. Commit the changes and push the code. Create a PR by changing any file in the repository, committing the changes to a new branch, and proposing the changes via a PR. Provide the following title to the "abc"; ls -R; . Take a few moments to inspect the result of the triggered workflow run. Which commands did it execute?
6. Add a second job named  safer-pr to the workflow.
   1. It should run on ubuntu-latest.
   2. It should contain two steps:
      1. The first step should checkout the code using the appropriate third-party action.
      2. The second step, named Check PR title, should execute the same script as above. However, instead of setting the title variable in the shell command, it should set an env variable named TITLE and with value set to the PR title, and then reference this variable from within the shell script.
7. Commit the changes and push the code. Create a PR yet another time by changing any file in the repository, committing the changes to a new branch, and proposing the changes via a PR. Provide the following title to the "abc"; ls -R; . Take a few moments to inspect the result of the triggered workflow run. Were the malicious commands executed?