**Practical Exercise 36 - Preventing Script Injection via Custom Actions**

**Exercise Description**

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

Here are the instructions for the exercise:

1. Create a JavaScript custom action following similar steps as explained in **Section 16: Developing Custom Actions from Scratch**. The custom action should:
   1. Be named Safe Title Check.
   2. Have a description of Safely checks the title of a PR.
   3. Receive a single input named pr-title, with a description of The PR title, and required.
   4. Retrieve this input and:
      1. Print PR is a feature if the pr-title starts with the substring feat.
      2. Print PR is not a feature otherwise.
2. Extend the workflow 20-workflow-security.yaml to include a new job named js-safer-pr:
   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 use the newly created JavaScript custom action to check whether the PR is a feature or not.
3. 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. Were the malicious commands executed?