Workflow Security

Workflow security involves safeguarding CI/CD processes and data through access control, secrets management, code review, vulnerability scanning, and proactive monitoring to mitigate risks and ensure integrity.

- **unsafe-pr:** This job directly reads the PR title from the event payload and checks if it starts with `"feat"` using a bash script.
- **safer-pr:** This job sets the PR title as an environment variable and then checks if it starts with `"feat"` using a bash script. This approach is slightly safer as it avoids directly referencing the event payload in the script.
- **js-safer-pr:** This job uses a custom action located at `./.github/actions/security-safe-input` to perform the check. It also checks if the PR title starts with "feat".

Testing Workflow Security

1. Create Workflow File:

- Create a new file named `25-01-Workflow-Security.yml` in the `.github/workflows` directory of your repository.

2. Define Workflow:

- Copy and paste the following YAML content into the `25-01-Workflow-Security.yml` file:

```
name: 25-01-Workflow Security

on:
  pull_request:
    types: [opened, synchronize]

jobs:
  unsafe-pr:
    runs-on: ubuntu-latest
    steps:
      - name: Checkout code
        uses: actions/checkout@v4
      - name: Check PR title
        run: |
          title=${{ github.event.pull_request.title }}
          if [[ $title =~ ^feat ]]; then
            echo "PR is a feature"
            exit 0
          else
            echo "PR is not a feature"
            exit 1
          fi
  safer-pr:
    runs-on: ubuntu-latest
```

```yaml
    steps:
      - name: Checkout code
        uses: actions/checkout@v4
      - name: Check PR title
        env:
          TITLE: ${{ github.event.pull_request.title }}
        run: |
          if [[ $TITLE =~ ^feat ]]; then
            echo "PR is a feature"
            exit 0
          else
            echo "PR is not a feature"
            exit 1
          fi
  js-safer-pr:
    runs-on: ubuntu-latest
    steps:
      - name: Checkout code
        uses: actions/checkout@v4
      - name: Check PR title
        uses: ./.github/actions/security-safe-input
        with:
          pr-title: ${{ github.event.pull_request.title }}
```

3. **Testing the Workflow:**

- **Commit Changes:** Commit the `25-01-Workflow-Security.yml` file to your repository.
- **Create a Pull Request:** Create a new pull request in your repository with a title starting with "feat".
- **Review Workflow Execution:**
  - Once the pull request is opened, GitHub Actions will trigger the workflow.
  - Check the Actions tab in your repository to see the workflow runs.
  - Review the logs of each job (`unsafe-pr`, `safer-pr`, `js-safer-pr`) to understand the behavior of different security implementations.
- **Test Different PR Titles:**
  - Create additional pull requests with different titles to test the behavior of each job in response to various PR titles.
  - Ensure that the workflow behaves as expected for both safe and unsafe PR titles.