UNIVERSITY of WASHINGTON

Software Design for Data Science

Secrets

Melissa Winstanley
University of Washington
March 13, 2025

Sharing Secrets

- Secrets?
  - Passwords
  - API tokens
  - Access keys
  - …
- NEVER EVER IN A FILE IN YOUR GITHUB REPOSITORY!
  - If a secret is ever leaked by uploading to GitHub repo, CHANGE IT

Secret management tools

A few secret sharing tools that you might see in the real world

- AWS Secrets Manager
- HashiCorp Vault
- 1Password
- Google Cloud Secrets Manager
- Doppler
- Azure Key Vault
- Infisical
- …

Using secrets: environment variables

Environment variables are just variables in bash:

```
MY_VARIABLE=foobar
```

Access them with the dollar sign:

```
echo "$MY_VARIABLE"
```

These are often used for storing secrets in Python:

```
os.getenv('GCP_PROJECT_ID')
```

.env files

Common way to store secrets as environment variables (documentation)

Repo documentation must include

- Which secrets are needed
- Where to get the secrets from

Also an option: Streamlit secrets.toml

DO NOT UPLOAD A .env FILE TO GITHUB!!!!

Example .env file

```
# environment variables defined inside a .env file
MY_PROJECT_ID=my-secret-project-id
AWS_ACCESS_TOKEN=supersecrettoken
CHATGPT_SECRET=123456
```

DO NOT UPLOAD THIS FILE TO GITHUB!!!!!

And then in Python:

```
import os
from dotenv import load_dotenv

load_dotenv()

AWS_ACCESS_TOKEN = os.getenv(AWS_ACCESS_TOKEN)
```

Example .gitignore file

```
# ignore .env files
.env

# for streamlit secrets, ignore the secrets file
.streamlit/secrets.toml
```

Secrets in Continuous Integration

What about tests that need a secret?

Repo > Settings > Security > Secrets & Variables > Actions > Secrets

And then use it as an environment variable:

```
steps:
  - name: Hello world action
    env:
      SUPER_SECRET: ${{ secrets.SuperSecret }}
```

Using secrets in GitHub Actions

Exercise: Any Secrets in Your Project?

- Use a proper secrets-management practice
  - .env
  - secrets.toml for Streamlit
- Use .gitignore
- Generate a new secret if you already uploaded to GitHub
- Update the secret in GitHub for continuous integration