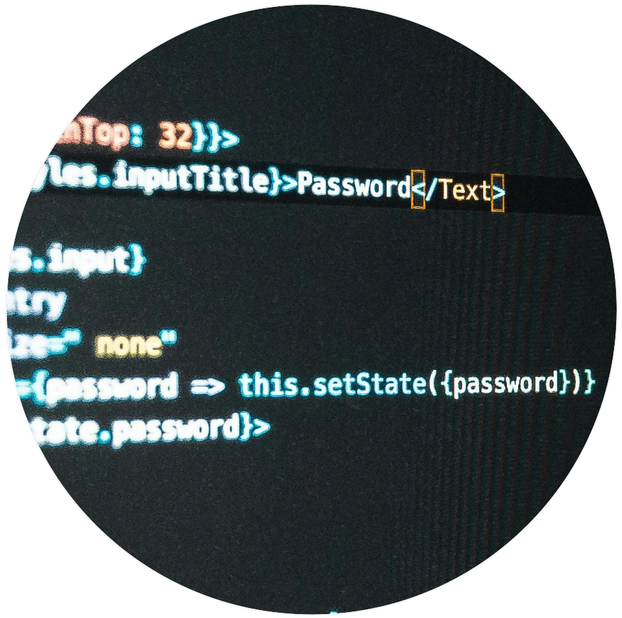
Manage Sensitive Data

Antonio J. Piedra
Senior DevOps Engineer

www.linkedin.com/in/ajpiedra



Remove Hardcoded Secrets

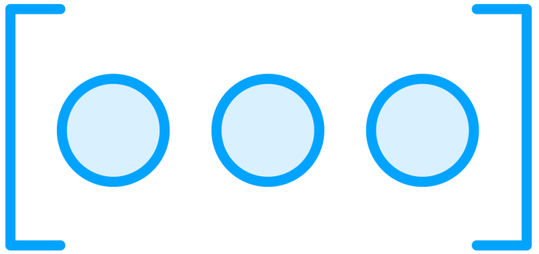
Eliminate usernames, password and API keys from your code

Never commit sensitive data to source control

Rotate secrets frequently!

If leaked, secrets rotation can greatly reduce the impact of the attack.

Inject Secrets at Runtime



Environment variables or runtime parameters

Secret management tools, like HashiCorp Vault

HashiCorp Vault

Tool to securely manage secrets

How it works

- Apps authenticate against Vault
- Secrets are retrieved via API or CLI

Benefits

- Dynamic secret rotation
- Fine-grained policies
- Audit logs

Demo: Remove Hardcoded Secrets

Prevent accidental exposure

Demo: Use Environment Variables for Secrets

Separate sensitive configs from code, injecting them at runtime

Demo: Install HashiCorp Vault

Secure secret storage and access control

Demo: Use Secrets Stored in HashiCorp Vault

Retrieve secrets securely at runtime