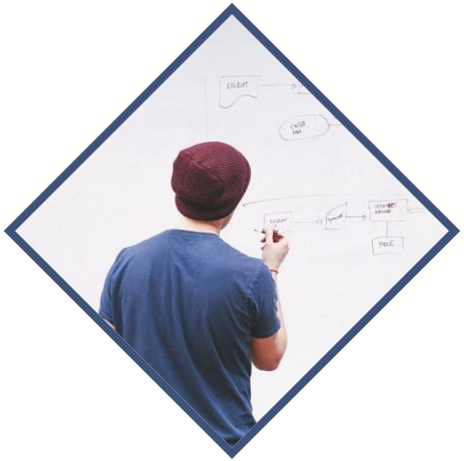
Managing Application Config and Secrets



HELLO!

I am Eng Teong Cheah

Microsoft MVP

You can find me at @walkercet

1

Introduction to Security

Introduction to Security

- Security is everyone’s responsibility and needs to be looked at holistically across the application life cycle.

SQL Injection Attack

SQL Injection (SQLi) is a type of an injection attack that makes it possible to execute malicious SQL statements.

2

Implement Secure & Compliant Development Processes

Threat Modeling

- Define security requirements
- Create an application diagram
- Identify threats
- Mitigate threats
- Validate that threats have been mitigated

Key Validation Points

- Continuous security validation should be added at each step from development through production

Continuous Integration

- The CI build should be executed as part of the pull request (PR-CI) process and once the merge is complete
- Be sure to scan third party packages for vulnerabilities and check OSS license usage

Infrastructure Vulnerabilities

- Be sure to validate the infrastructure
- Use the Azure Security Center and Azure Policies

Application Deployment to DEV and TEST

- OWASP ZAP can be used for penetration testing
- Testing can be active or passive
- Conduct a quick baseline scan to identify vulnerabilities
- Conduct nightly more intensive scans

Results and Bugs

- OWASP ZAP provides a report with results and bugs
- Use a holistic and layered approach to security

3

Rethinking Application Config Data

Rethinking Application Config Data

- Configuration information is stored in files
- Changes can require downtime and administrative overhead
- Challenging to mange changes to local configurations across multiple running instance of the applications

Separation of Concerns

- Configuration Custodian
- Configuration Consumer
- Configuration Store
- Secret Store

External Configuration Store Patterns

- Store the configuration in external storage
- Provide an interface to quickly and efficiently read and update

Integrating Azure Key Vault with Azure Pipeline

- Allows you to manage your organization’s secrets and certificates in a centralized repository

4

Manage Secrets, Tokens, and Certificates

Manage Secrets, Tokens & Certificates

- Centralize application secrets
- Security store secrets and keys
- Monitor access and use
- Simplified administration of application secret
- Integrate with other Azure services

Kubernetes and Azure Key Vault

- Use Kubernetes and Azure Key Vault together to get the best security benefits:
- Azure Key Vault Secret store
- Kubernetes ConfigMaps
- Kubernets Secrets

5

Implement Tools for Managing Security and Compliance

SonarCloud

- Technical debt – measure between the codebase’s current state and an optimal state
- SonarQube

Implement Continuous Security Validation

- Reduce cost by moving DevSecOps to the left
  Use automated tooling and processes to identify problems

THANKS!

Any questions?

You can find me at
@walkercet

CREDITS

- Microsoft Docs