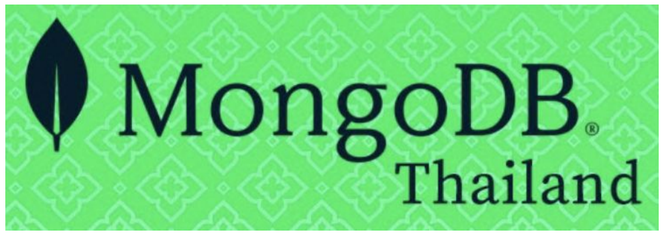
Workshop: Github Actions Crash Course

Piti Champeethong (Fyi/ฟี่)

PyLanna Co-founder (Python User Group)
MongoDB Thailand User Group Buddy
https://github.com/ninefyi



Agenda

- GitHub Actions components.
- GitHub Codespaces.
- Secrets and variables.
- OWASP Zap.
- Cloudflare Pages Pipeline.
- Key takeaway
- Q&A

Prerequisites

- Cloudflare Account: https://developers.cloudflare.com/fundamentals/account/create-account/
- GitHub Account: https://github.com/join

Agenda

- GitHub Actions components.
- GitHub Codespaces.
- Secrets and variables.
- OWASP Zap.
- Cloudflare Pages Pipeline.
- Key takeaway
- Q&A

GitHub Actions components

- **Workflows**: Automation defined in *.github/workflows/*.yml*.
- **Triggers**: Events like *push* or *deployment_status*.
- **Jobs & Steps**: Units of work running on GitHub-hosted runners / Self-hosted runners.
- **Actions**: Reusable plugins: *zaproxy/action-baseline*.

Agenda

- GitHub Actions components.
- GitHub Codespaces.
- Secrets and variables.
- OWASP Zap.
- Cloudflare Pages Pipeline.
- Key takeaway
- Q&A

GitHub Codespaces

- **Standardized Dev Environment**: Defined by *.devcontainer.json*.
- **Pre-installed Tools**: Includes GitHub CLI and Node/Python runtimes.
- **Security First**: Safe environment to manage secrets and test headers.
- **Cloud-Native**: Code and test from any browser.

Agenda

- GitHub Actions components.
- GitHub Codespaces.
- Secrets and variables.
- OWASP Zap.
- Cloudflare Pages Pipeline.
- Key takeaway
- Q&A

Secrets and variables.

- **Secrets**: Encrypted storage for API Tokens (Cloudflare).
- **Variables**: Plain-text config for environment URLs.
- **Context**: Accessed via *${{ secrets.GITHUB_TOKEN }}*.
- **Safety**: Automatically masked in execution logs.

Agenda

- GitHub Actions components.
- GitHub Codespaces.
- Secrets and variables.
- OWASP Zap.
- Cloudflare Pages Pipeline.
- Key takeaway
- Q&A

OWASP Zap (Zed Attack Proxy)

- Dynamic Application Security Testing (DAST).
- **Baseline Scan**: Checks for missing security headers (Rule 10035, 10038).
- **Automation**: Integrated via the Official ZAP GitHub Action.
- Generates a detailed HTML vulnerability report.

Agenda

- GitHub Actions components.
- GitHub Codespaces.
- Secrets and variables.
- OWASP Zap.
- Cloudflare Pages Pipeline.
- Key takeaway
- Q&A

Cloudflare Pages Pipeline

1. **Push**: Code committed to GitHub.
2. **Deploy**: Cloudflare builds and serves at the edge.
3. **Notify**: GitHub receives *deployment_status*.
4. **Scan**: ZAP crawls the live **.pages.dev* URL.
5. **Report**: Results saved as GitHub **Artifacts**.

Agenda

- GitHub Actions components.
- GitHub Codespaces.
- Secrets and variables.
- OWASP Zap.
- Cloudflare Pages Pipeline.
- Key takeaway
- Q&A

Key takeaway

- **Shift-Left**: Test security as soon as the site is live.
- **Audit Trails**: Keep a history of scan reports in GitHub.
- **Hardening**: Use Cloudflare headers to block 90% of common attacks.

References

- https://github.com/ninefyi/tech-on-the-rock-2025
- https://www.zaproxy.org/docs/alerts/
- https://github.com/zaproxy/action-full-scan
- https://learn.microsoft.com/en-us/training/modules/introduction-to-github-actions/
- https://docs.github.com/en/actions/how-tos

THANK YOU!