

DRAFT



GitHub Security + .NET

Application Security for .NET repos stored
on GitHub



Chad Bentz

@felickz / GitHub

About Me

- GitHub
- .NET Developer
- Security Advocate
- Open Source Contributor

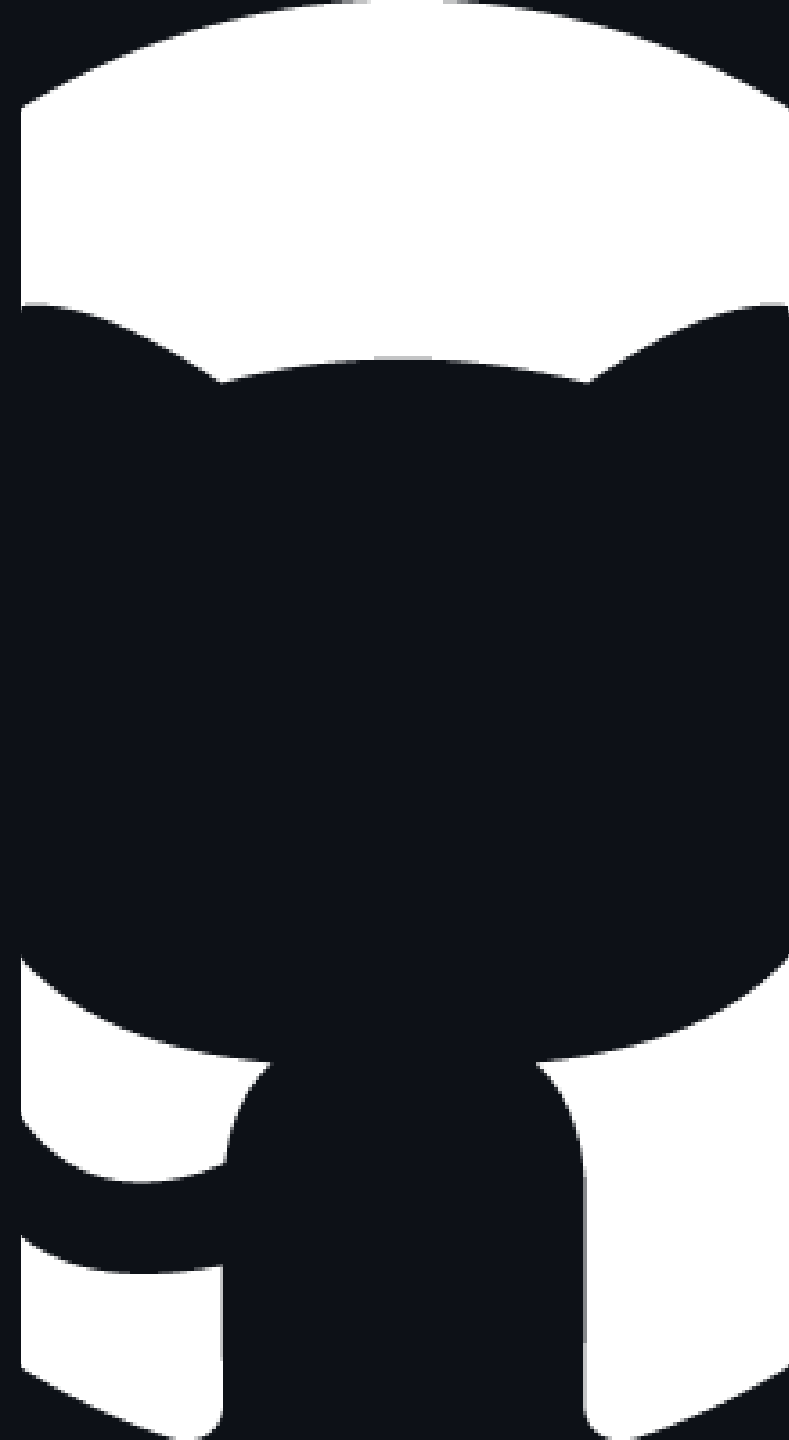


Why Security Matters for .NET

- Security is often an afterthought
- Open source vulnerabilities are increasing
- Growing attack surface in modern .NET apps
- NuGet ecosystem brings both power and risk
- Build security into your workflow, not on top

Agenda

1. GitHub Security Tools for .NET
2. Code Scanning with CodeQL
3. Dependency Management & SCA
4. Secret Protection
5. Copilot for Security
6. Demos



Real-World Example

Throughout this talk, we'll reference:

```
https://github.com/dotnet-felickz/monorepo
```

- Contains .NET projects using:
 - MAUI
 - Blazor/MVC with ASP.NET Core
 - Shared libraries
 - GitHub Actions workflows

GitHub's Security Toolbox

- Dependency Graph/Review
- Dependabot Alerts & Updates
- CodeQL
- Secret Scanning
- GitHub Actions Security
- Copilot Security Assistance

All FREE for open source projects!



Code Scanning with CodeQL

What is it?

- Static Application Security Testing (SAST)
- Queries your code as data
- Finds security vulnerabilities
- Integrates with PR workflow

Key Benefits

- No false positives philosophy
- Deep understanding of .NET frameworks
- Fully supports C# 13 / .NET 9
- Can analyze without building (NEW!)

CodeQL Setup Options

Default Setup (Recommended)

```
# Simple setup in just a few clicks
name: "CodeQL"
```

```
on:
```

```
  push:
```

```
    branches: [ "main" ]
```

```
  pull_request:
```

```
    branches: [ "main" ]
```

```
  schedule:
```

```
    - cron: '17 0 * * 0'
```

```
jobs:
```

```
  analyze:
```

```
    name: Analyze
```

```
    runs-on: ubuntu-latest
```

```
    permissions:
```

```
      security-events: write
```

```
    steps:
```


Advanced CodeQL for .NET Monorepo

```
# From our monorepo sample
steps:
  # ...setup steps...
  - name: Initialize CodeQL
    uses: github/codeql-action/init@v3
    with:
      languages: csharp
      queries: security-extended,security-and-quality

  - name: Autobuild
    uses: github/codeql-action/autobuild@v3

# Or use custom build commands:
# - run: |
#     dotnet restore ./src/MyApp.sln
#     dotnet build ./src/MyApp.sln --configuration Release
```

CodeQL Tools for .NET Developers

- VSCode Extension
 - Write & test custom queries
 - Explore code databases
- CodeQL CLI
 - Multi-repo variant analysis
 - Vulnerability hunting at scale
- Query Libraries
 - Standard & extended security
 - .NET framework-specific queries



What CodeQL Finds in .NET

- SQL Injection
- CSRF vulnerabilities
- XSS in Razor views
- Insecure deserialization
- Hard-coded credentials
- Improper authentication
- Weak crypto implementations
- Potential DoS vectors
- And many more...

Software Composition Analysis (SCA)

Dependency Graph & Review

- Maps all NuGet packages
- Direct & transitive dependencies
- Review changes in PRs
- Integration with .NET SDK

Component Detection

```
- name: Component Detection
  uses: microsoft/component-detection-dependency-submission-action@v1.1.0
  with:
    detection-level: Direct
```



Dependabot: Automated Security

Security Updates

- Automatic PR for vulnerabilities
- Contextual security info
- Customizable via dependabot.yml

Version Updates

- Keep dependencies fresh
- .NET SDK updates (NEW!)
- 65% faster with native .NET

Secret Protection

Push Protection

- Prevents secrets from being committed
- Scans commits in real-time
- Blocks pushes with secrets

Secret Scanning

- Detects leaked secrets
- NuGet API keys
- Azure connection strings
- AWS & other cloud credentials
- Custom patterns



Latest .NET Security Features

NuGetAudit 2.0

- Enhanced security validation
- Trust and integrity checks
- Package signing verification

Immutable Releases

- Signed binaries with SBOM
- Software Bill of Materials
- Supply chain transparency

Agent Mode in Visual Studio

Copilot for Security

Copilot Autofix

- Automatically suggests fixes
- Contextual understanding of code
- One-click remediation

Copilot Chat

- Security-focused explanations
- "What does this code do?"
- "Is this code secure?"
- Remediation recommendations



MCP for Security Analysis

```
#get_code_scanning_alert
```

- Get vulnerability details
- Understand impact and context
- Security-aware code generation
- Explanation of complex issues

Demo Time!

What We'll See


1. Blocking PR with SCA vulnerability using Dependency Review
2. CodeQL alert in a PR with push protection
3. AI Autofix for simple vulnerabilities
4. MCP for complex security fixes

Key Takeaways

1. Security tools are **free** for open source
2. Integrate security early in development
3. Leverage AI for faster remediation
4. Stay updated with .NET security news
5. Community-driven security benefits everyone



Resources

-  Slides: github.com/felickz/talks
-  Demo repo: github.com/dotnet-felickz/monorepo
-  CodeQL docs: codeql.github.com
-  Advisory DB: github.com/advisories
-  Security Lab: securitylab.github.com

Thank You!

Questions?

- GitHub: @felickz
- Demo: github.com/dotnet-felickz/monorepo

"Secure code is quality code, and the open source community deserves both."

