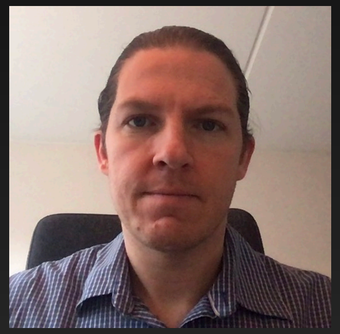
Hack din egen pipeline

Cloud Native Day Bergen 2025

Bilde: https://www.pipeliner.com.au



nav

POLITIET
POLITIETS IT-ENHET

/emilalbrektsson

/jksolbakken

Har DU trusselmodellert dine pipelines?

The malicious package versions contain a worm that executes a post-installation script. This malware scans the compromised environment for sensitive credentials, including:

- `.npmrc` files (for npm tokens)
- Environment variables and configuration files specifically targeting GitHub Personal Access Tokens (PATs) and API keys for cloud services like:
  - Amazon Web Services (AWS)
  - Google Cloud Platform (GCP)
  - Microsoft Azure

Token Exfiltration Campaign via GitHub Actions Workflows

Summary

I recently responded to an attack campaign where malicious actors injected code into GitHub Actions workflows attempting to steal PyPI publishing tokens. PyPI was not compromised, and no PyPI packages were published by the attackers.

News

ctrl/tinycolor and 40+ NPM Packages Compromised

The popular @ctrl/tinycolor package with over 2 million weekly downloads has been compromised alongside 40+ other NPM packages in a sophisticated supply chain attack dubbed "Shai-Hulud". The malware self-propagates across maintainer packages, harvests AWS/GCP/Azure credentials using TruffleHog, and establishes persistence through GitHub Actions backdoors - representing a major escalation in NPM ecosystem threats.

News

Harden-Runner detection: tj-actions/changed-files action is compromised

SUPPLY-CHAIN ATTACKS EVERYWHERE

Software packages with more than 2 billion weekly downloads hit in supply-chain attack

Incident hitting npm users is likely the biggest supply-chain attack ever.

Compromised SpotBugs Token Led to GitHub Actions Supply Chain Hack

Evidence shows a SpotBugs token compromised in December 2024 was used in the March 2025 GitHub Actions supply chain attack.

GitHub Action Compromise Puts CI/CD Secrets at Risk in Over 23,000 Repositories

Nx S1ingularity

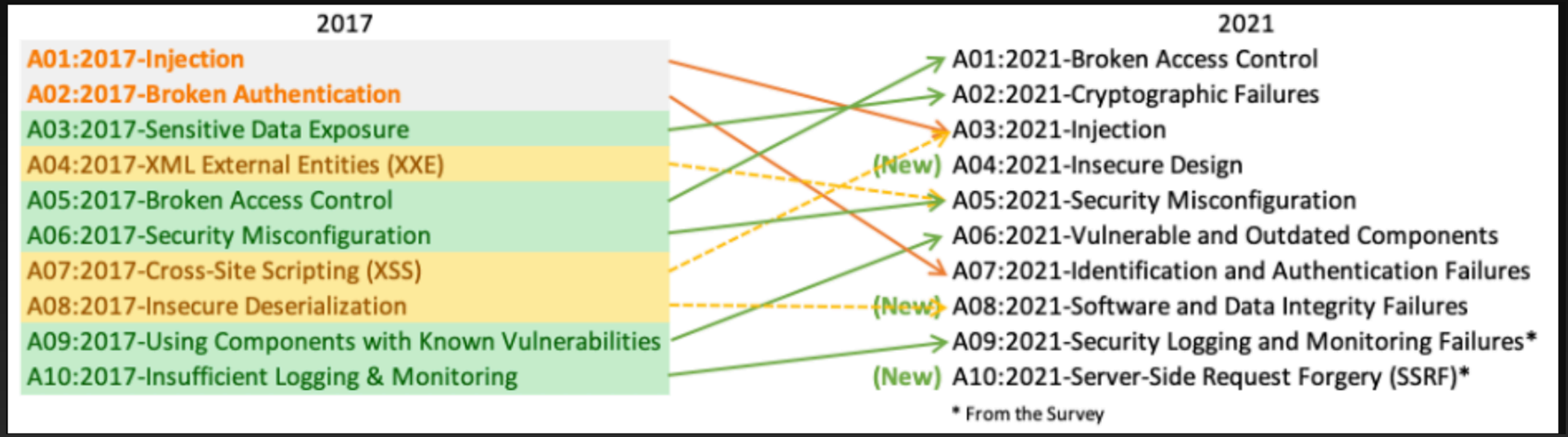
Shell injection in GitHub Action with `pull_request_target` trigger and unnecessary read/write permissions[1], used to extract a npm token.

Root cause: pull_request_target.

Contributing factors: read/write CI permissions, long-lived credential exfiltration, post-install scripts.

https://words.filippo.io/compromise-survey/

Trusler

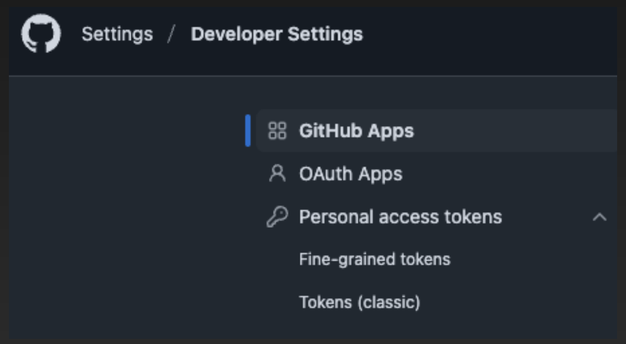

2017
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring
2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*
* From the Survey

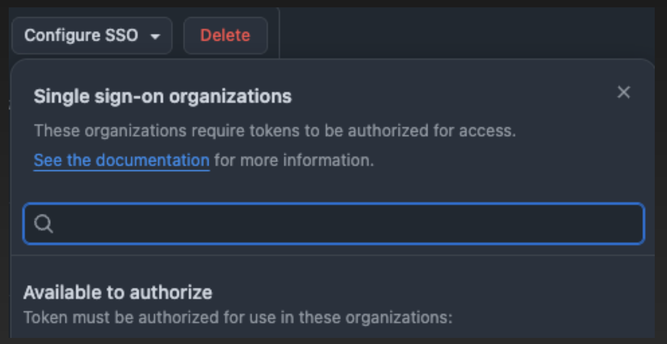
Kompromitterte credentials

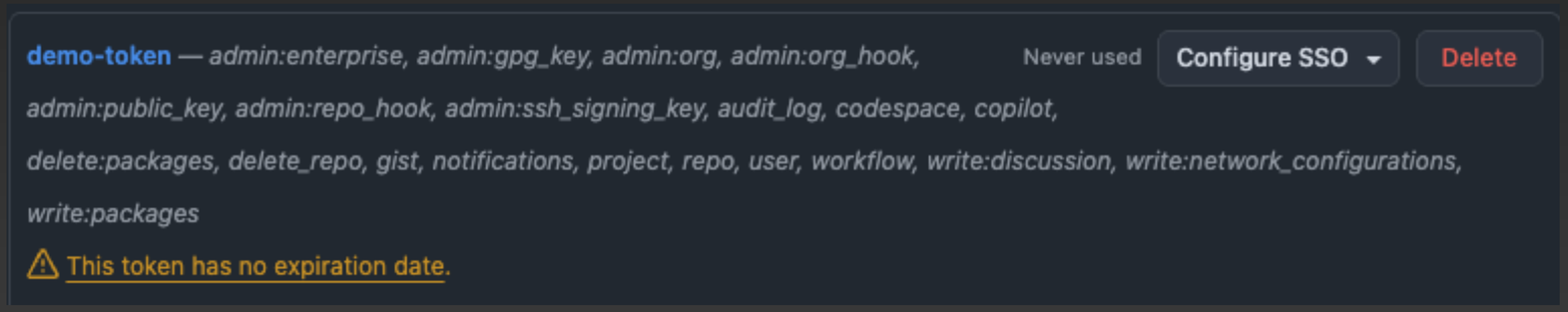
```yaml
- name: Log in to registry
  run: echo "${{ secrets.GITHUB_TOKEN }}" | docker login ghcr.io -u ${{ github.actor }} --password-stdin
```

GITHUB_TOKEN

Learn what `GITHUB_TOKEN` is, how it works, and why it matters for secure automation in GitHub Actions workflows.







Mutable actions

GitHub Advisory Database / GitHub Reviewed / CVE-2025-30066

tj-actions changed-files through 45.0.7 allows remote attackers to discover secrets by reading actions logs.

High severity | GitHub Reviewed | Published on Mar 15 to the GitHub Advisory Database • Updated on Mar 24

Vulnerability details | Dependabot alerts 0

Package	Affected versions	Patched versions
tj-actions/changed-files (GitHub Actions)	<= 45.0.7	46.0.1

Description

Summary

A supply chain attack compromised the **tj-actions/changed-files** GitHub Action, impacting over 23,000 repositories. Attackers retroactively modified multiple version tags to reference a malicious commit, exposing CI/CD secrets in workflow logs. The vulnerability existed between **March 14 and March 15, 2025**, and has since been mitigated. This poses a significant risk of unauthorized access to sensitive information.

This has been patched in v46.0.1.

Details

The attack involved modifying the **tj-actions/changed-files** GitHub Action to execute a malicious Python script. This script extracted secrets from the Runner Worker process memory and printed them in GitHub Actions logs, making them publicly accessible in repositories with public workflow logs.

Severity

High 8.6 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	None
Availability	None

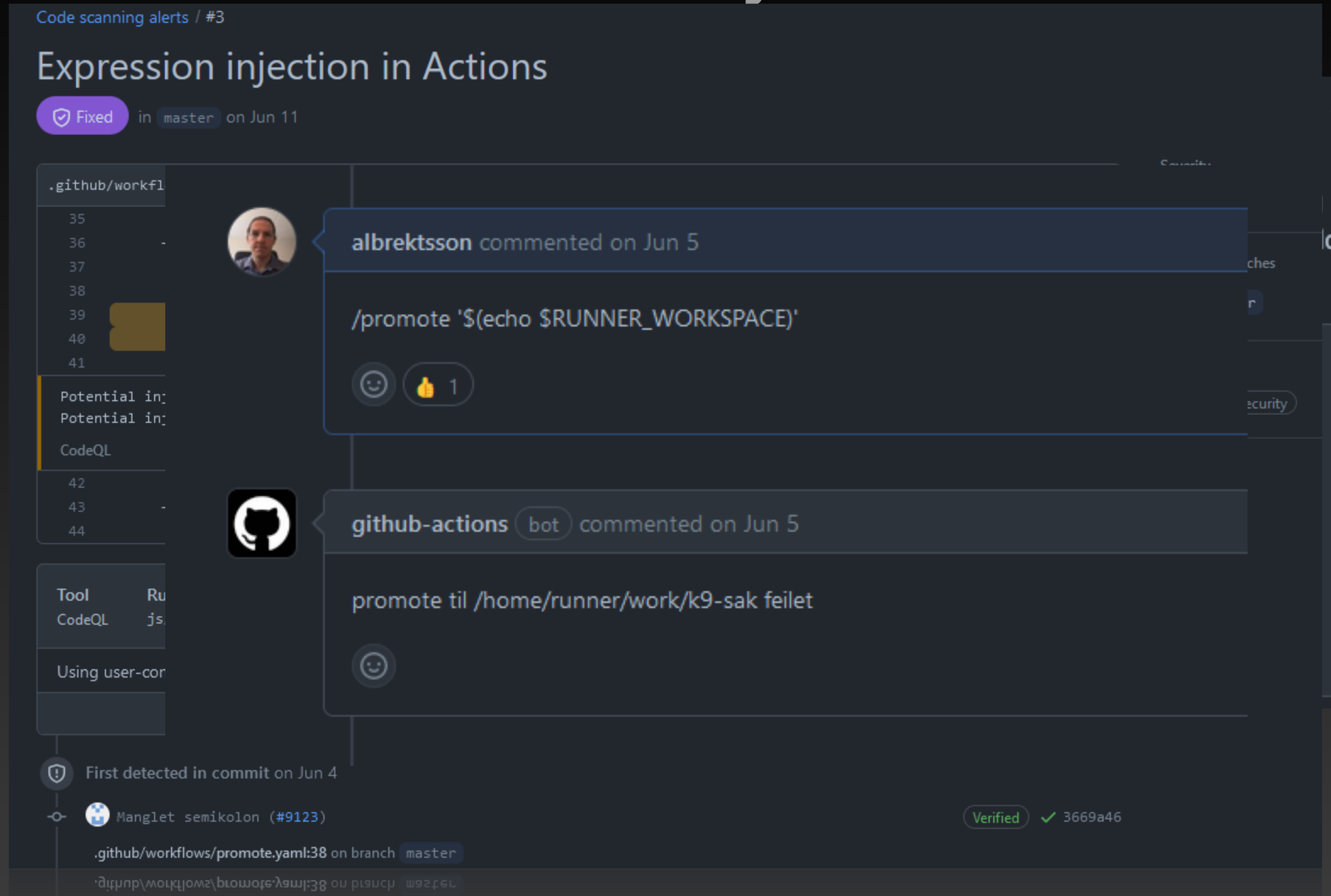
Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

EPSS score

88.385% (99th percentile)

Code Injection



Konfigurasjonen av repo

Branch rules

- [ ] **Restrict creations**
  Only allow users with bypass permission to create matching refs.

- [ ] **Restrict updates**
  Only allow users with bypass permission to update matching refs.

- [x] **Restrict deletions**
  Only allow users with bypass permissions to delete matching refs.

- [ ] **Require linear history**
  Prevent merge commits from being pushed to matching refs.

- [ ] **Require deployments to succeed**
  Choose which environments must be successfully deployed to before refs can be pushed into a ref that matches this rule.

- [ ] **Require signed commits**
  Commits pushed to matching refs must have verified signatures.

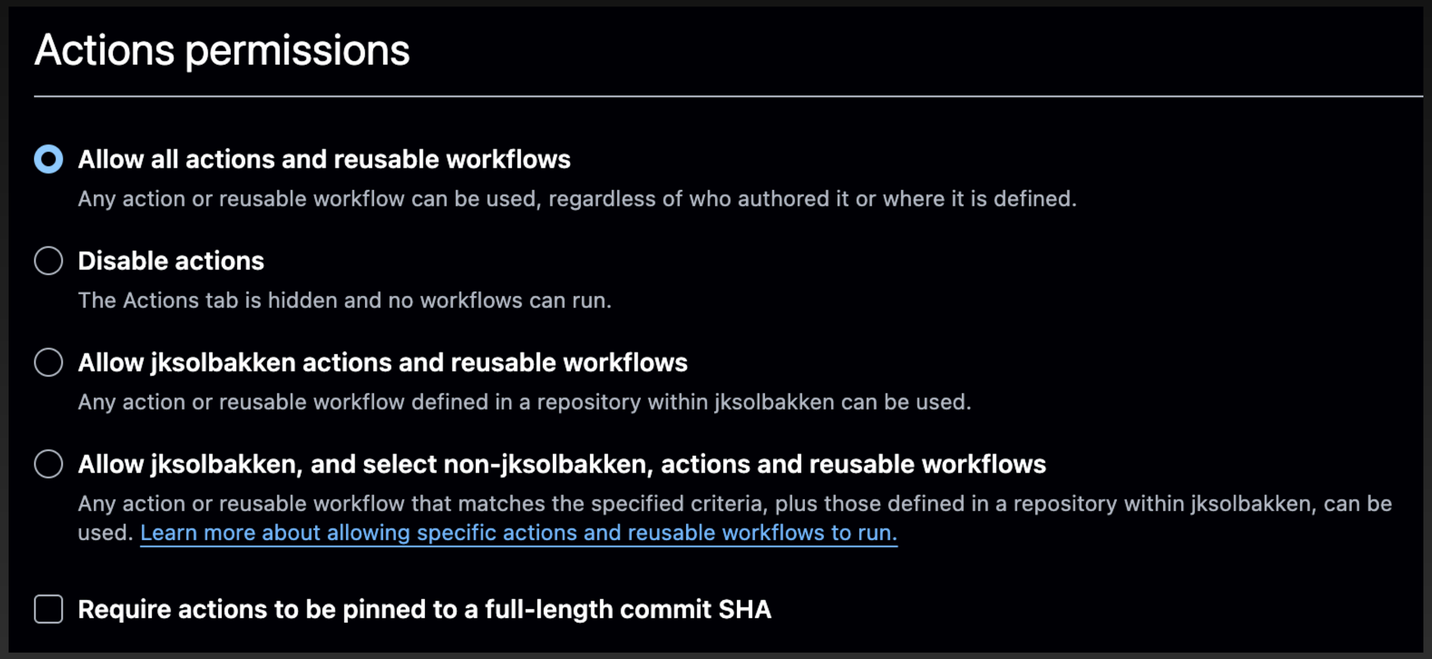
- [ ] **Require a pull request before merging**
  Require all commits be made to a non-target branch and submitted via a pull request before they can be merged.

- [ ] **Require status checks to pass**
  Choose which status checks must pass before the ref is updated. When enabled, commits must first be pushed to another ref where the checks pass.

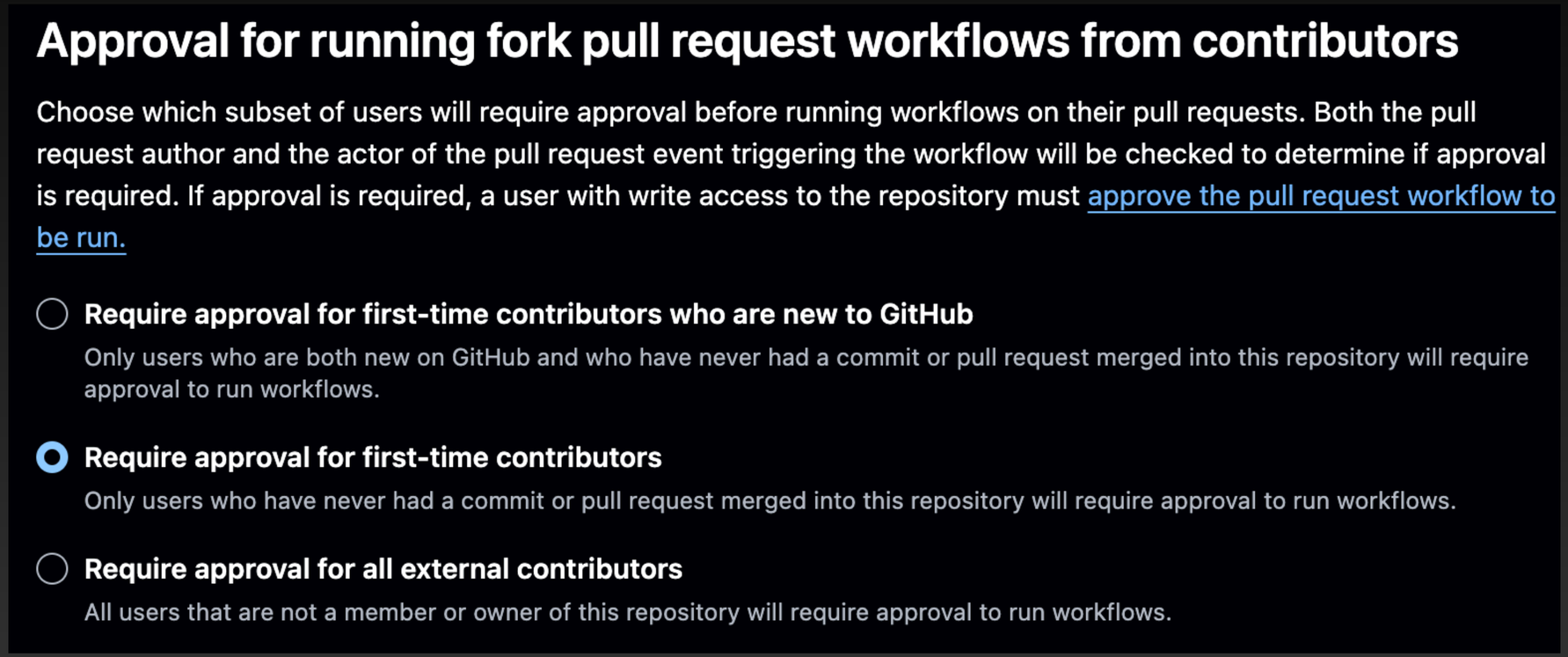
- [x] **Block force pushes**
  Prevent users with push access from force pushing to refs.

- [ ] **Require code scanning results**
  Choose which tools must provide code scanning results before the reference is updated. When configured, code scanning must be enabled and have results for both the commit and the reference being updated.

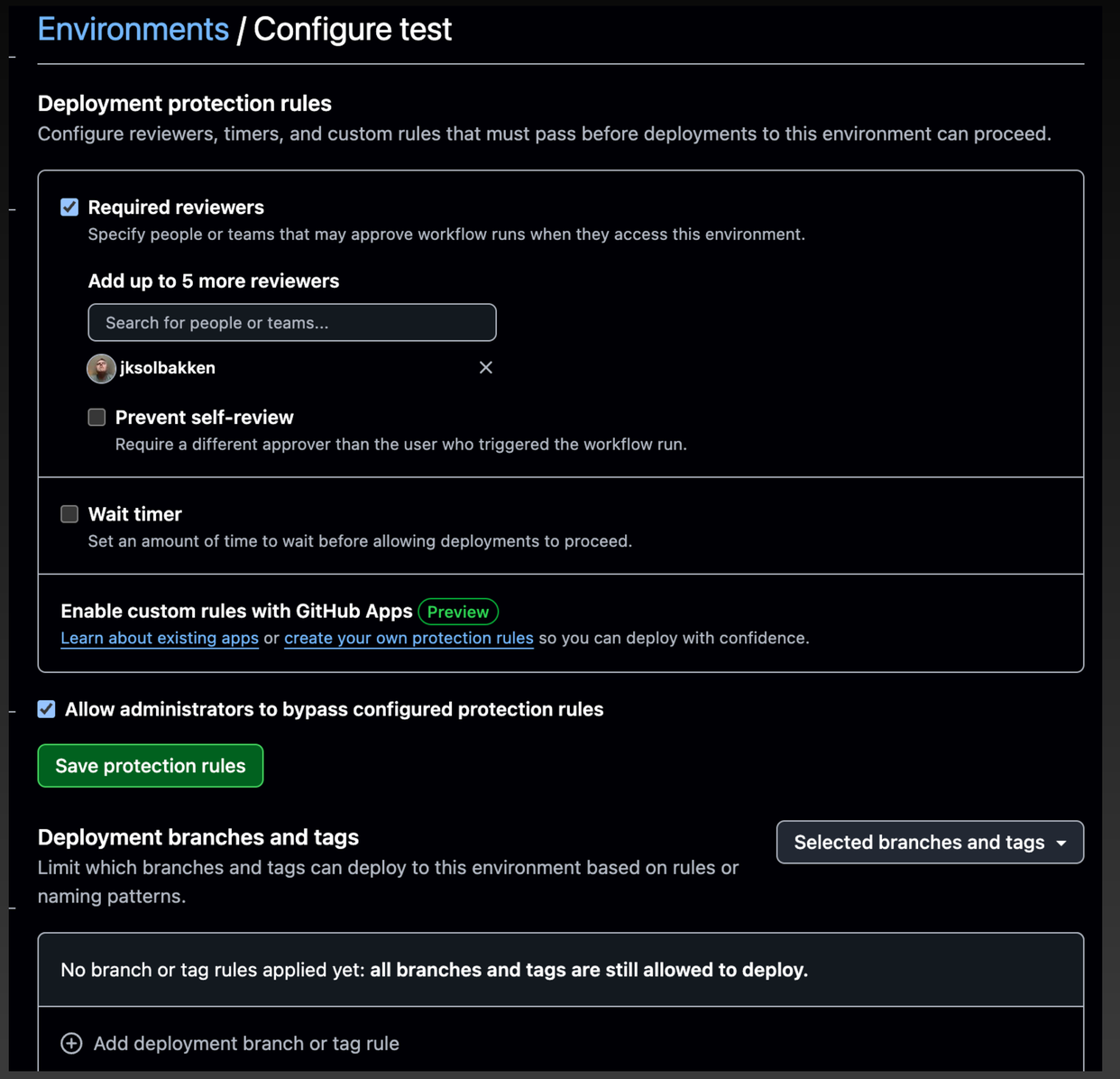
Konfigurasjonen av repo



Konfigurasjonen av repo



Konfigurasjonen av repo



Time for arbeidsbutikk!

Forke eller klone amazing-app.

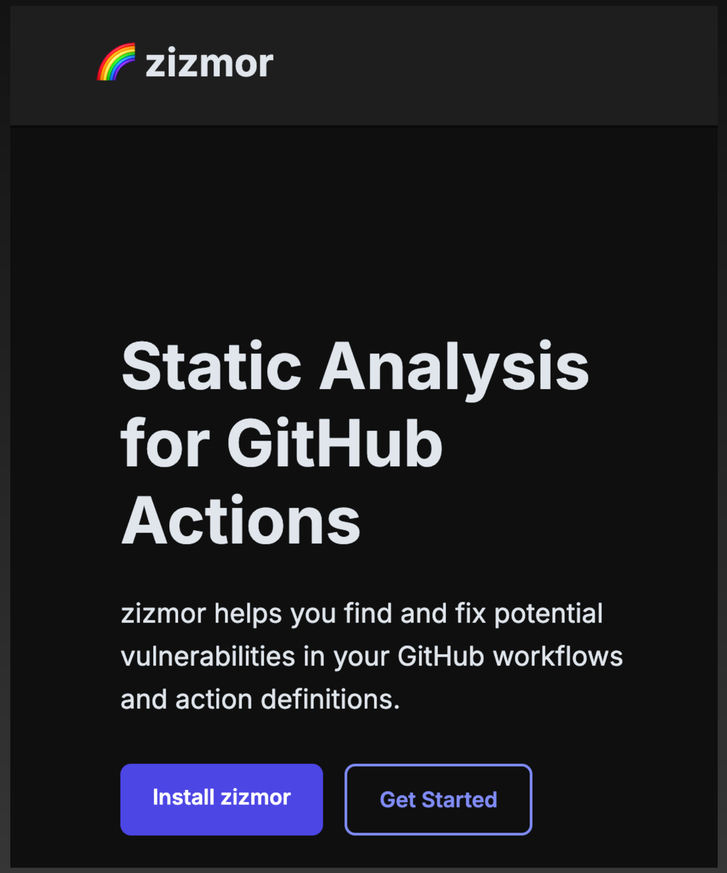
Git clone https://github.com/CND-Bergen/amazing-app.git

Gh clone repo CND-Bergen/amazing-app

Bruk 10 min og se om du finner noen sårbarheter i workflowsa her!

Zizmor

https://zizmor.sh/



Cache poisoning

Github specific ish vulnerability

Tl;dr: don’t use cache for releases or prod deployment

Bonusoppgaver

Tilbake til amazing-app
Bruk det du har lært til å eksfiltrere hemmeligheter
Finn det hemmelige repoet
Poste en issue med ditt alias > great success!

Thanks for all the phish!

Nyttige linker

- Preventing pwn requests
- Security hardening for GitHub Actions
- How to Harden GitHub Actions: The Unofficial Guide
- Zizmor
- Ratchet
- GitHub token permissions Monitor
- StepSecurity harden-runner
- Privesc vha workflow_run
- OpenSSF Scorecard
- Gato (Github Attack TOolkit) - Extreme Edition
- CodeQL query help for GitHub Actions