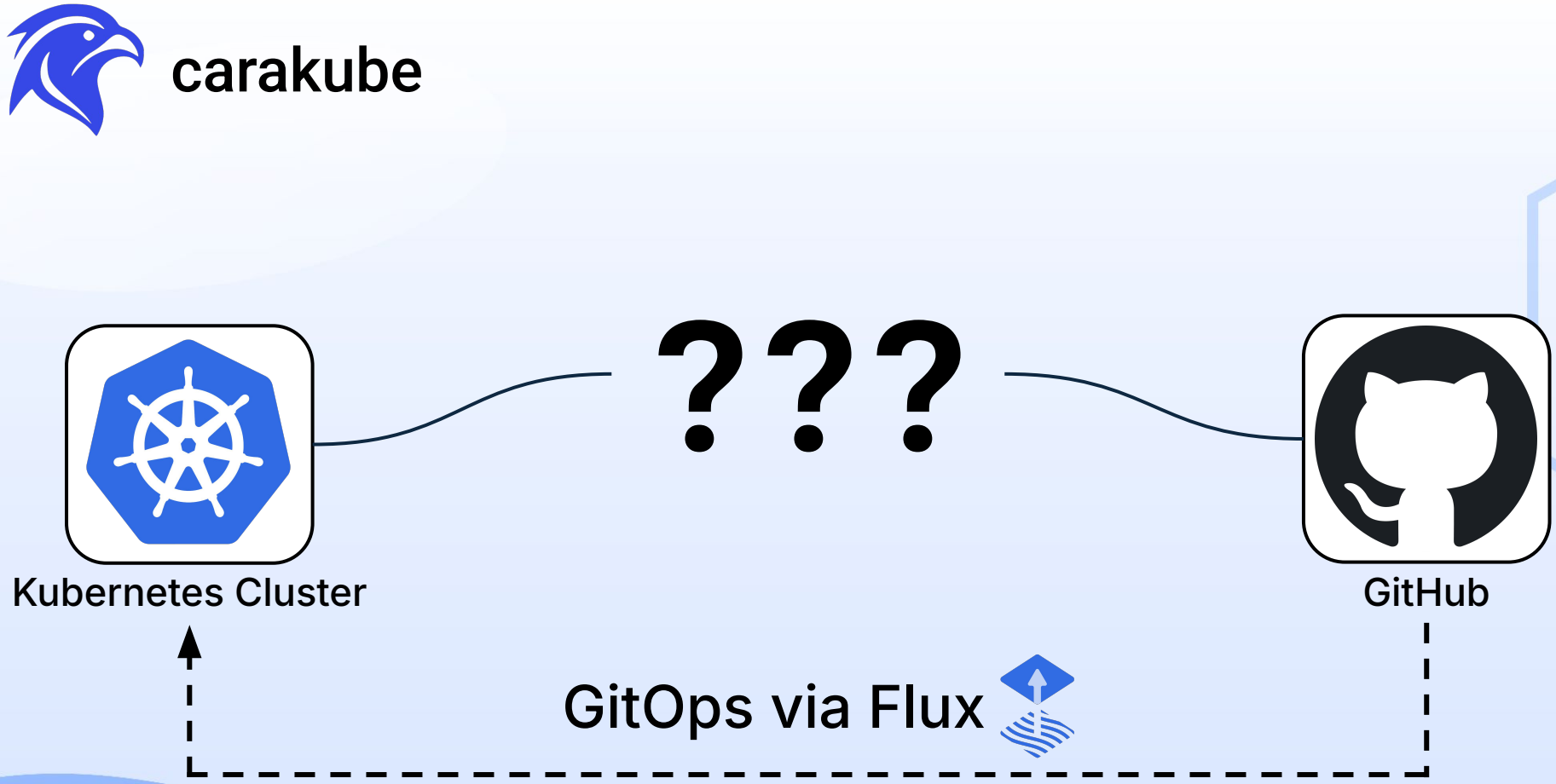
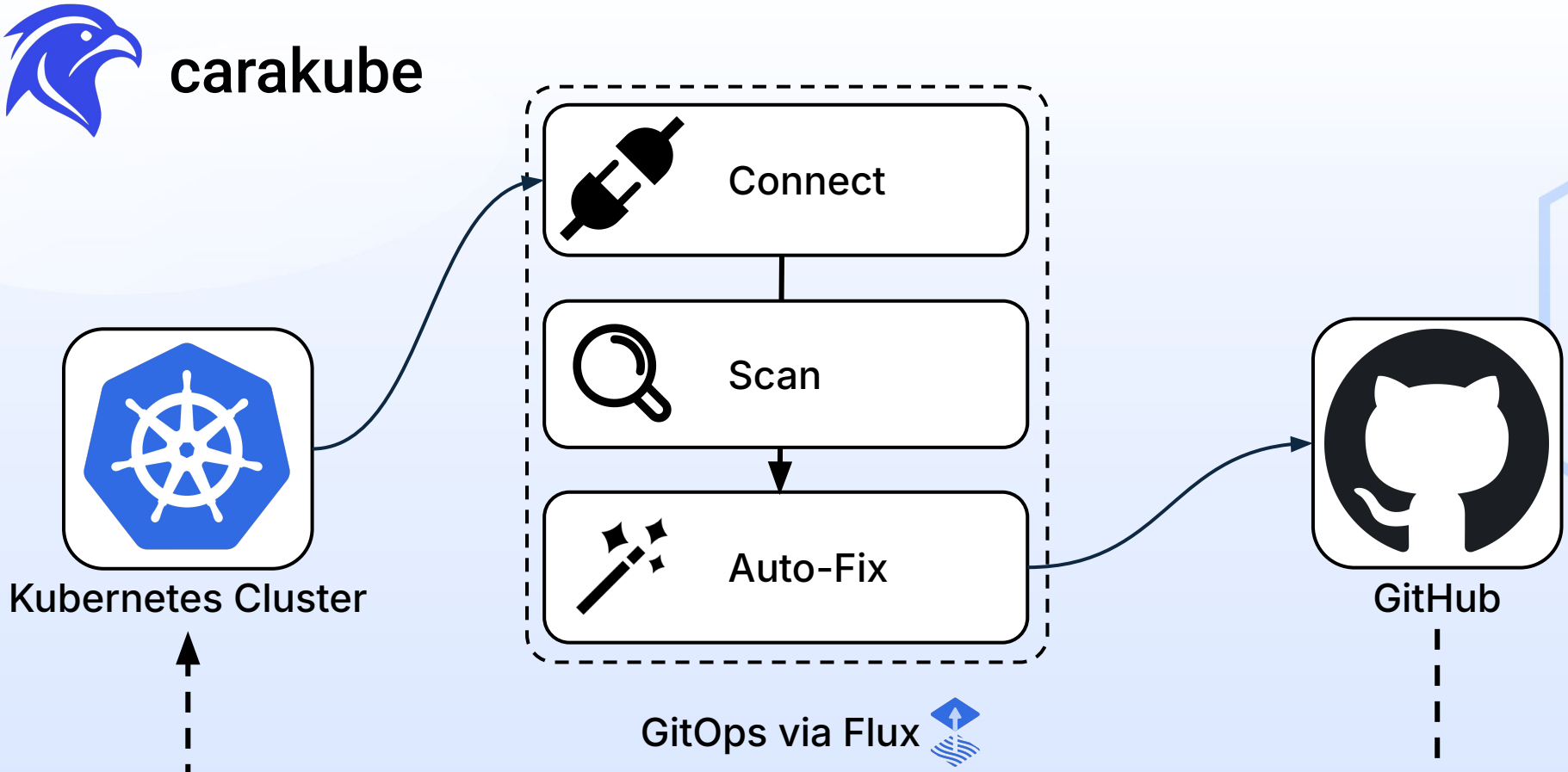
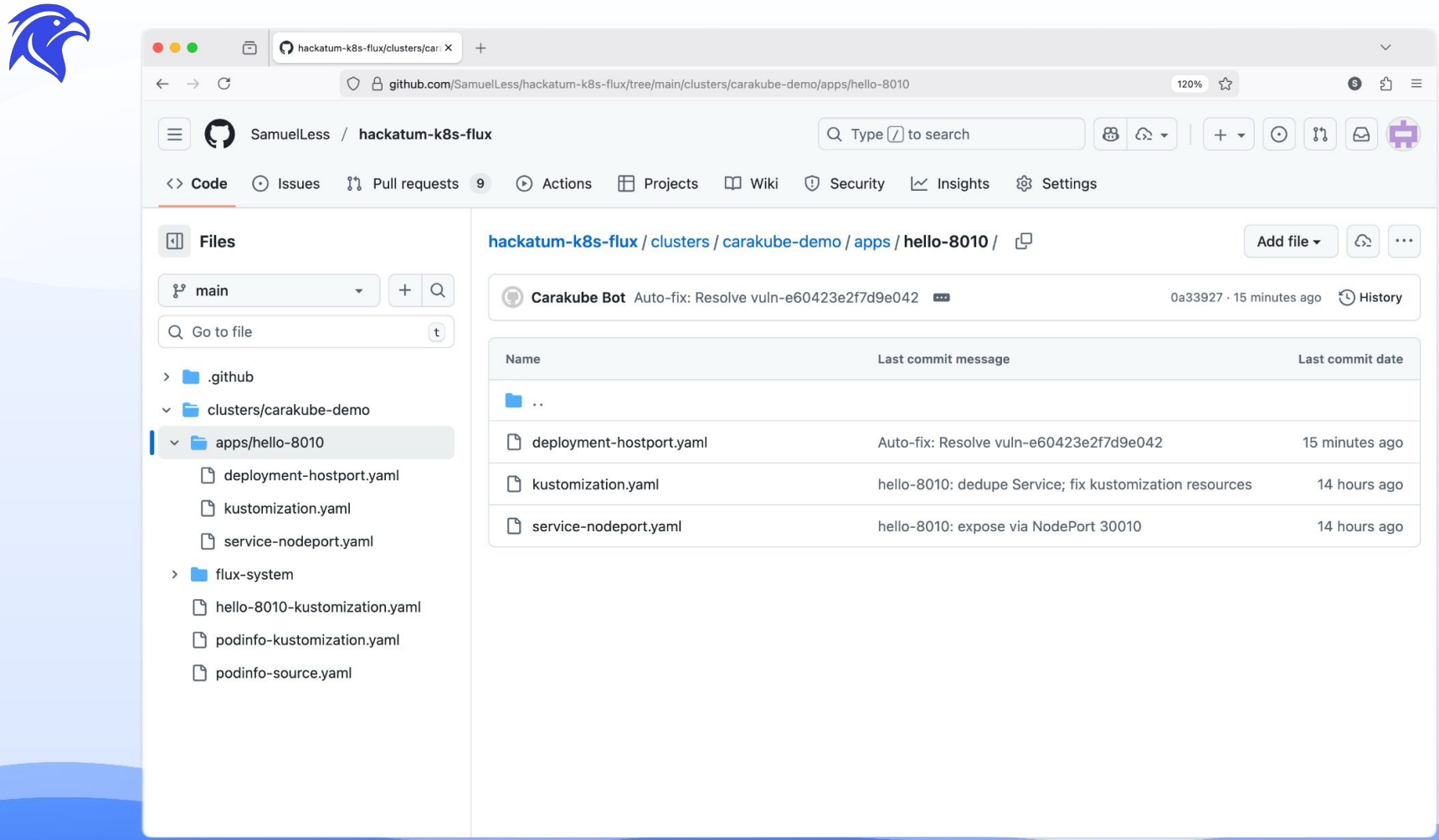
# carakube

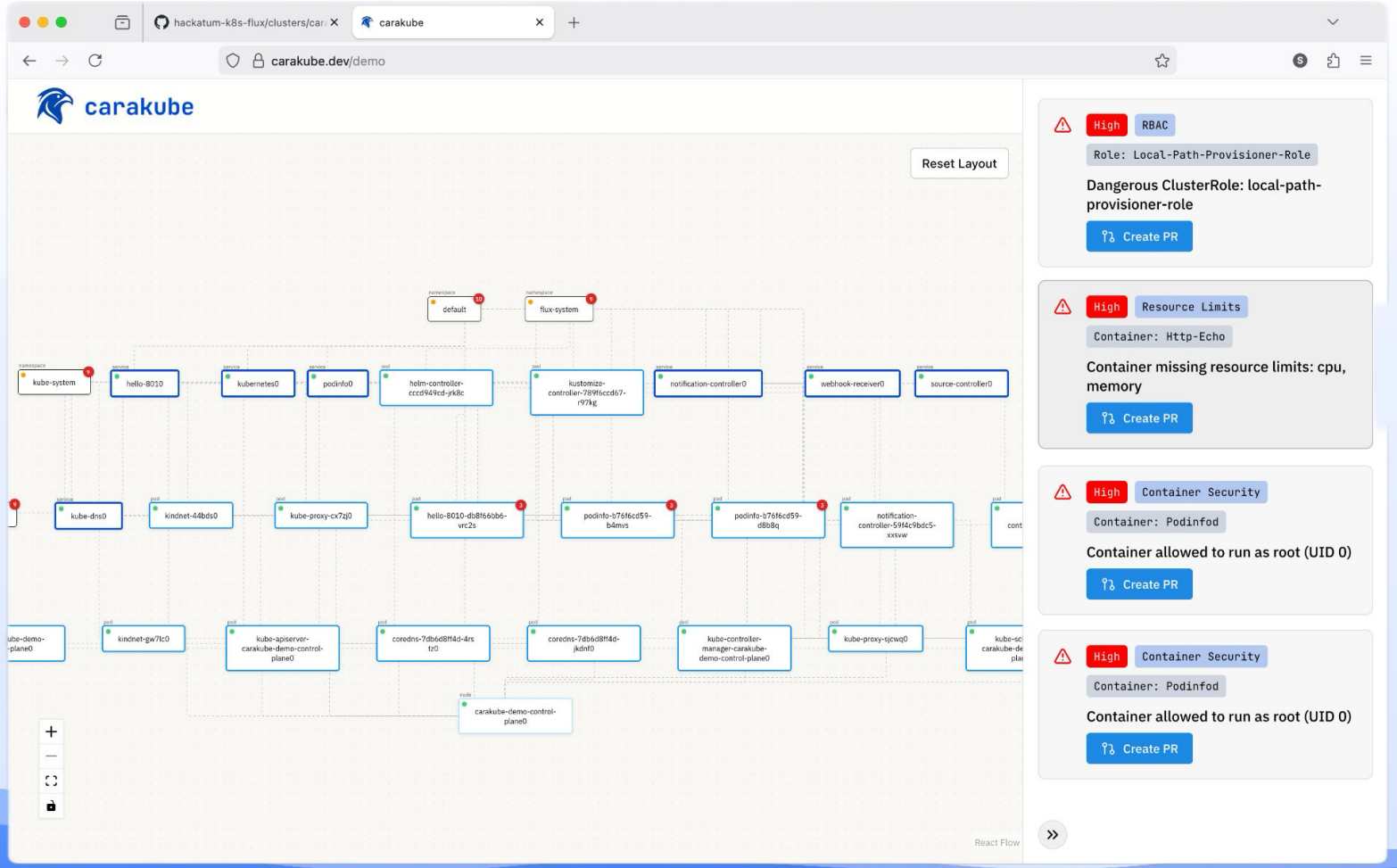

carakube
???
Kubernetes Cluster
GitHub
GitOps via Flux

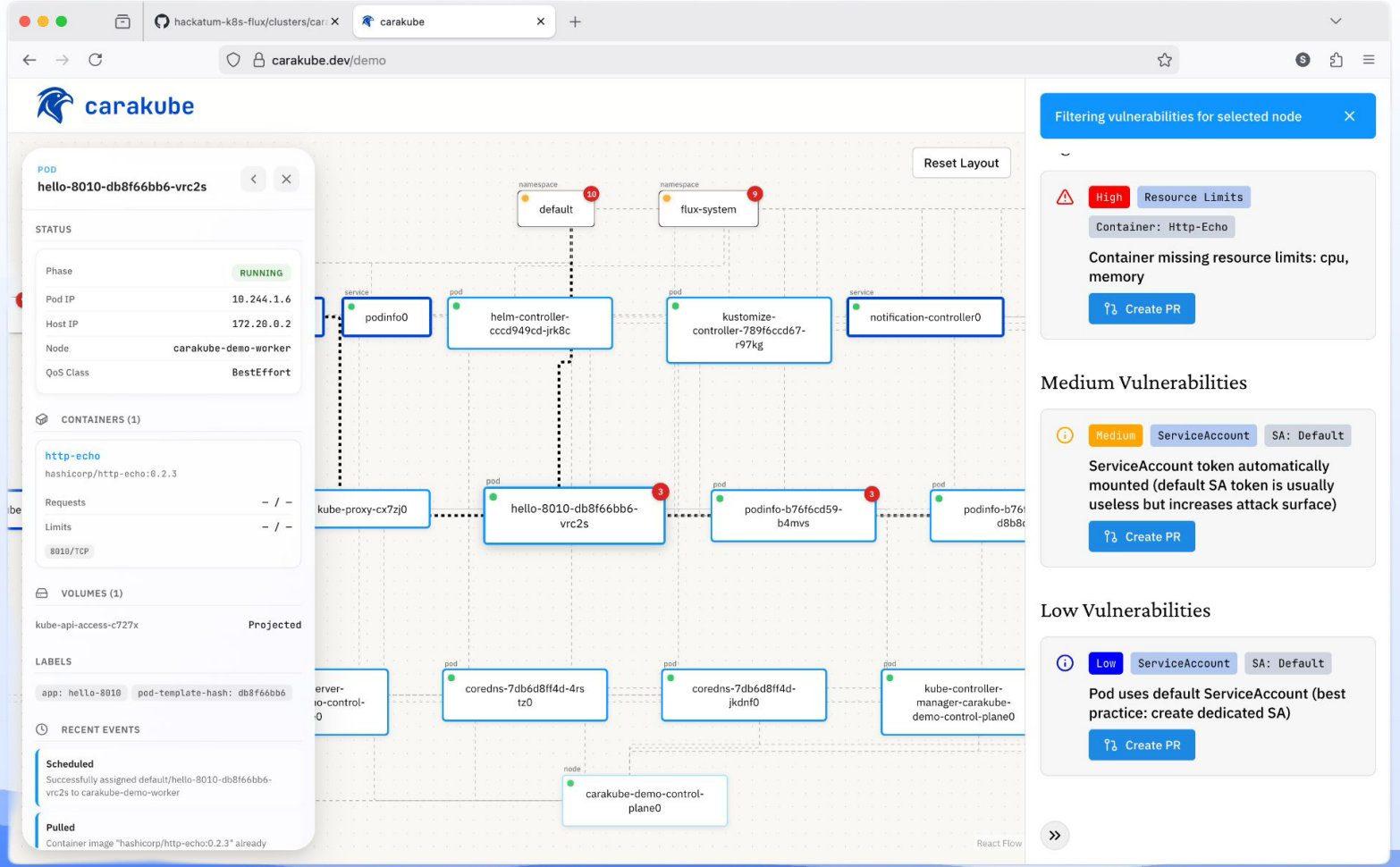

carakube
Connect
Scan
Auto-Fix
Kubernetes Cluster
GitHub
GitOps via Flux

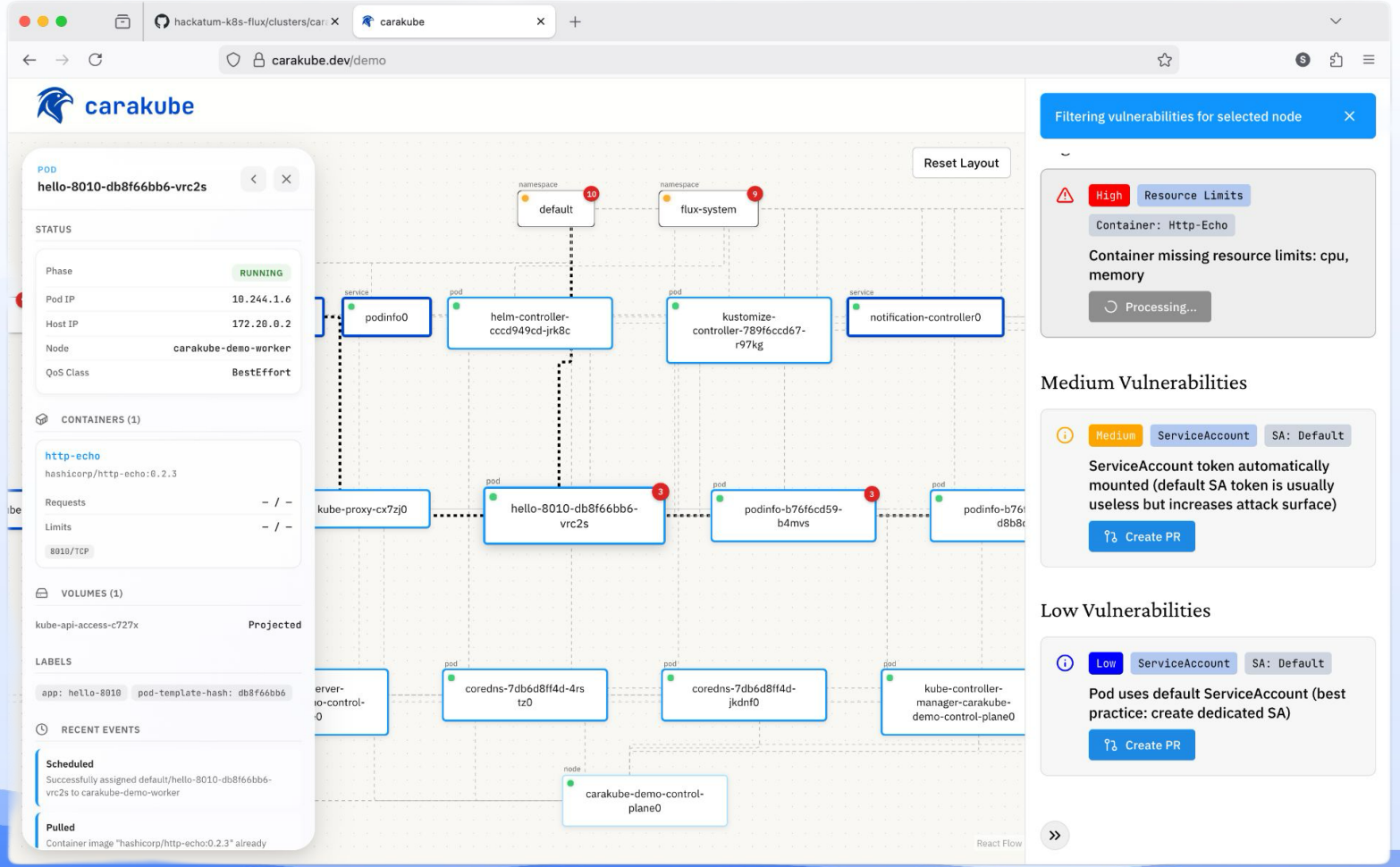
carakube

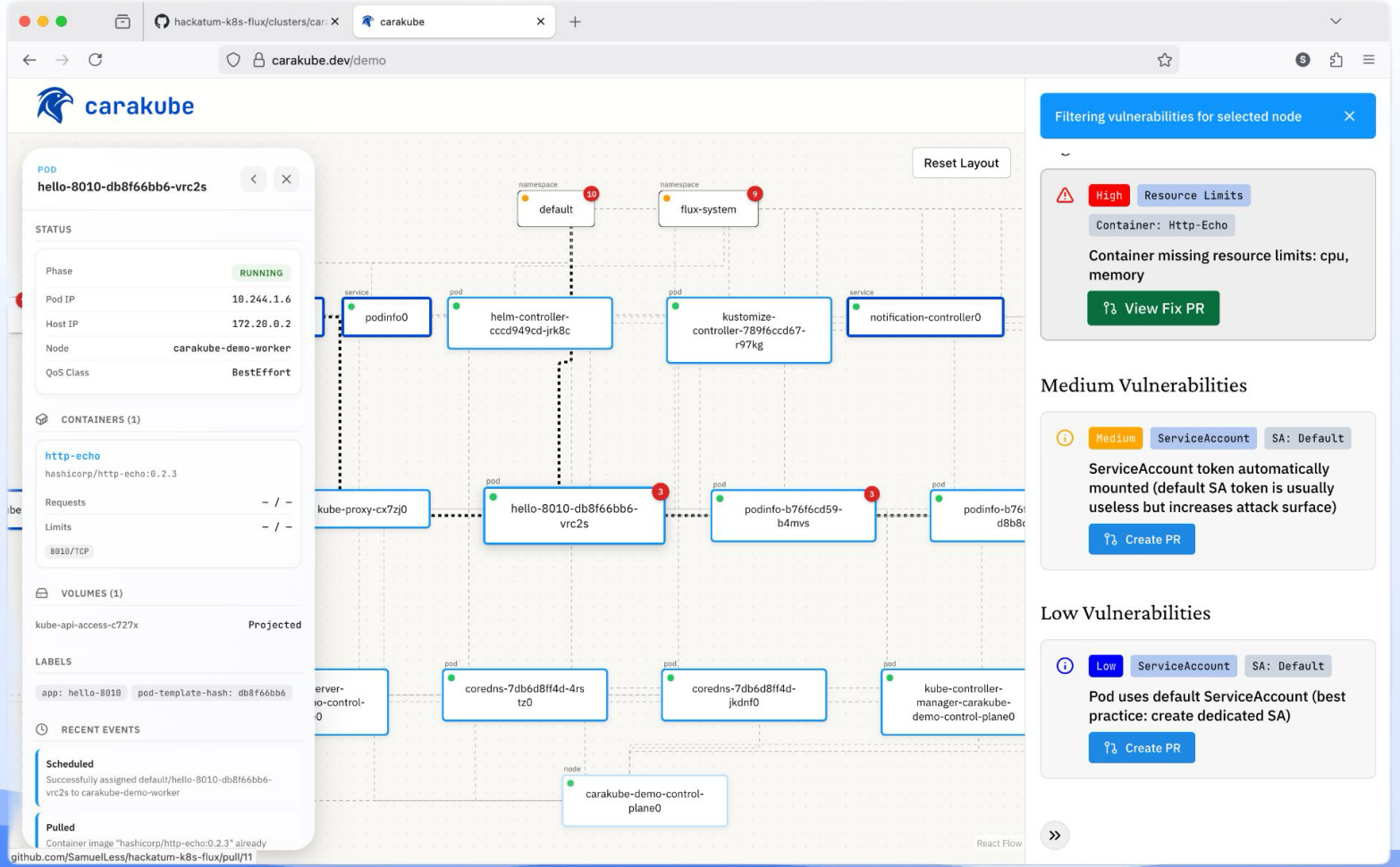
# Demo Time!


hackatum-k8s-flux/clusters/car
github.com/SamuelLess/hackatum-k8s-flux/tree/main/clusters/carakube-demo/apps/hello-8010
120%
SamuelLess / hackatum-k8s-flux
Type / to search
Code
Issues
Pull requests 9
Actions
Projects
Wiki
Security
Insights
Settings
Files
main
Go to file t
.github
clusters/carakube-demo
apps/hello-8010
deployment-hostport.yaml
kustomization.yaml
service-nodeport.yaml
flux-system
hello-8010-kustomization.yaml
podinfo-kustomization.yaml
podinfo-source.yaml
hackatum-k8s-flux / clusters / carakube-demo / apps / hello-8010 /
Add file
Carakube Bot Auto-fix: Resolve vuln-e60423e2f7d9e042
0a33927 · 15 minutes ago
History
Name
Last commit message
Last commit date
..
deployment-hostport.yaml
Auto-fix: Resolve vuln-e60423e2f7d9e042
15 minutes ago
kustomization.yaml
hello-8010: dedupe Service; fix kustomization resources
14 hours ago
service-nodeport.yaml
hello-8010: expose via NodePort 30010
14 hours ago

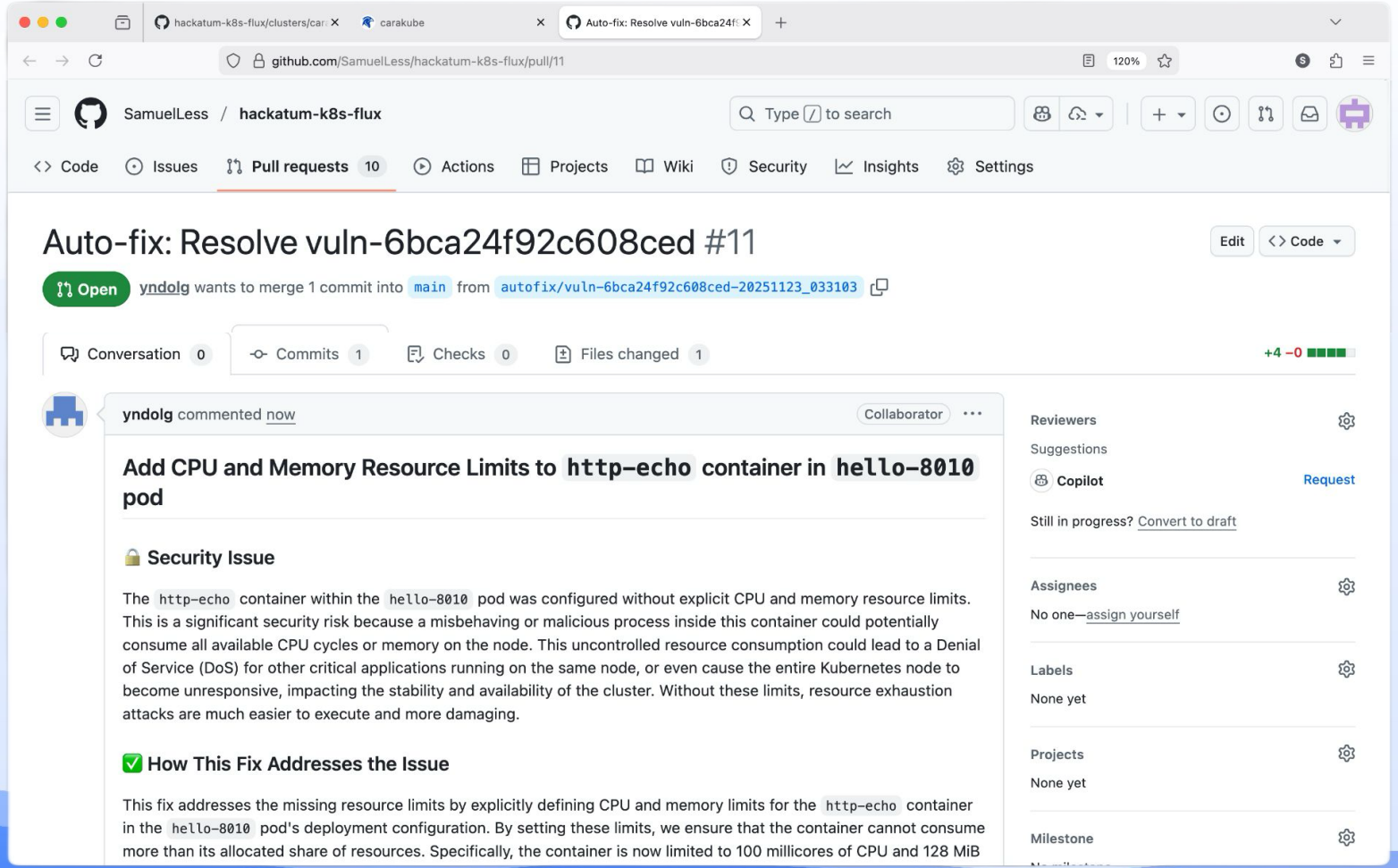

hackatum-k8s-flux/clusters/car
carakube
carakube.dev/demo
carakube
Reset Layout
default
flux-system
kube-system
hello-8010
kubernetes0
podinfo0
helm-controller-cccd949cd-jrk8c
kustomize-controller-789f6ccd67-r97kg
notification-controller0
webhook-receiver0
source-controller0
kube-dns0
kindnet-44bds0
kube-proxy-cx7zj0
hello-8010-db8f66bb6-vrc2s
podinfo-b76f6cd59-b4mvs
podinfo-b76f6cd59-d8b8q
notification-controller-59f4c9bdc5-xxsvw
kindnet-gw7lc0
kube-apiserver-carakube-demo-control-plane0
coredns-7db6d8ff4d-4rstr2
coredns-7db6d8ff4d-jkdnf0
kube-controller-manager-carakube-demo-control-plane0
kube-proxy-sjcwq0
carakube-demo-control-plane0
React Flow
High
RBAC
Role: Local-Path-Provisioner-Role
Dangerous ClusterRole: local-path-provisioner-role
Create PR
High
Resource Limits
Container: Http-Echo
Container missing resource limits: cpu, memory
Create PR
High
Container Security
Container: Podinfod
Container allowed to run as root (UID 0)
Create PR
High
Container Security
Container: Podinfod
Container allowed to run as root (UID 0)
Create PR

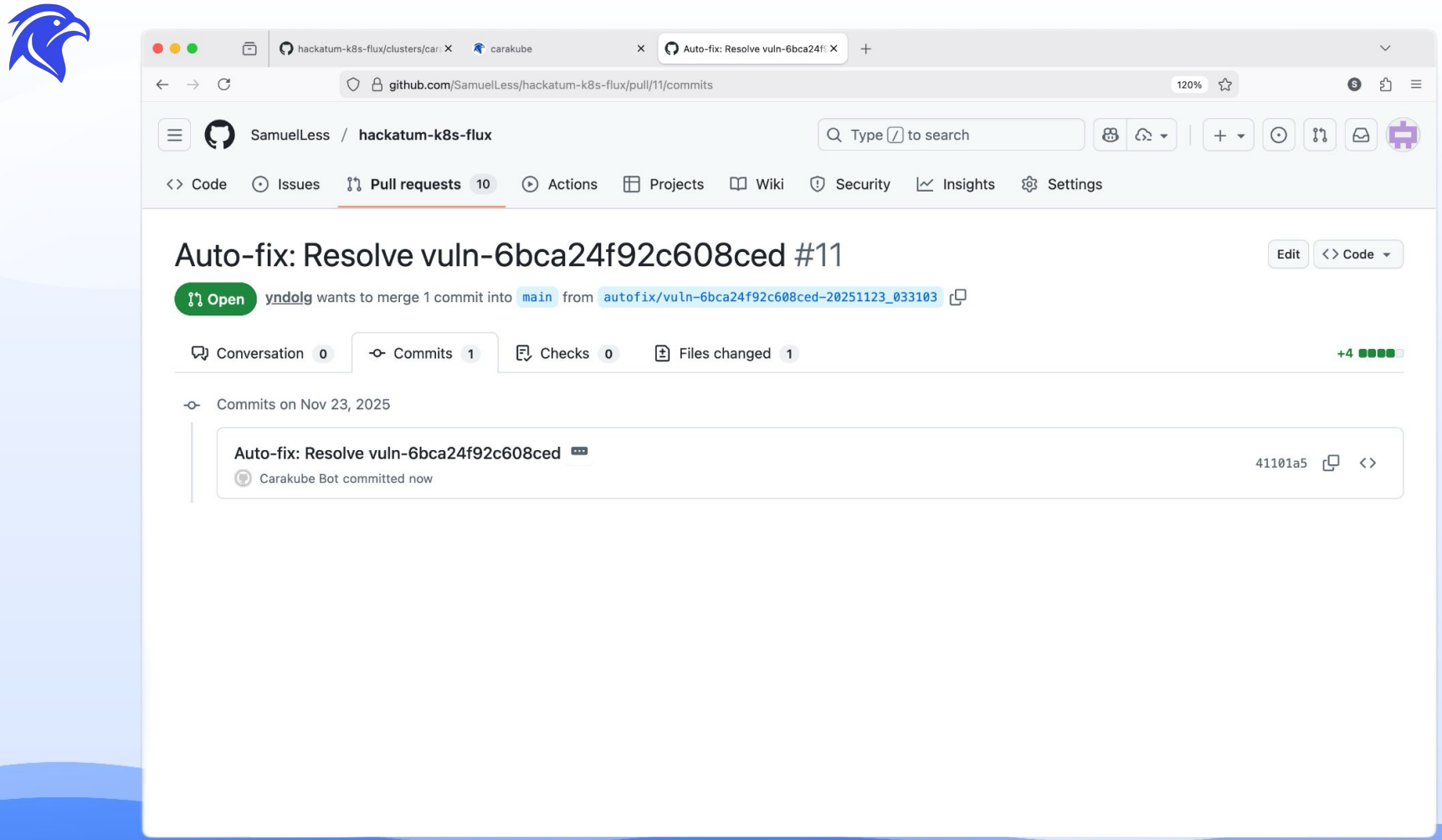

carakube.dev/demo
carakube
POD
hello-8010-db8f66bb6-vrc2s
STATUS
Phase
RUNNING
Pod IP
10.244.1.6
Host IP
172.20.0.2
Node
carakube-demo-worker
QoS Class
BestEffort
CONTAINERS (1)
http-echo
hashicorp/http-echo:0.2.3
Requests
– / –
Limits
– / –
8010/TCP
VOLUMES (1)
kube-api-access-c727x
Projected
LABELS
app: hello-8010
pod-template-hash: db8f66bb6
RECENT EVENTS
Scheduled
Successfully assigned default/hello-8010-db8f66bb6-vrc2s to carakube-demo-worker
Pulled
Container image "hashicorp/http-echo:0.2.3" already
Reset Layout
namespace
default
flux-system
podinfo0
helm-controller-cccd949cd-jrk8c
kustomize-controller-789f6ccd67-r97kg
notification-controller0
kube-proxy-cx7zj0
hello-8010-db8f66bb6-vrc2s
podinfo-b76f6cd59-b4mvs
coredns-7db6d8ff4d-4rstz0
coredns-7db6d8ff4d-jkdnf0
kube-controller-manager-carakube-demo-control-plane0
carakube-demo-control-plane0
React Flow
Filtering vulnerabilities for selected node
High
Resource Limits
Container: Http-Echo
Container missing resource limits: cpu, memory
Create PR
Medium Vulnerabilities
Medium
ServiceAccount
SA: Default
ServiceAccount token automatically mounted (default SA token is usually useless but increases attack surface)
Create PR
Low Vulnerabilities
Low
ServiceAccount
SA: Default
Pod uses default ServiceAccount (best practice: create dedicated SA)
Create PR

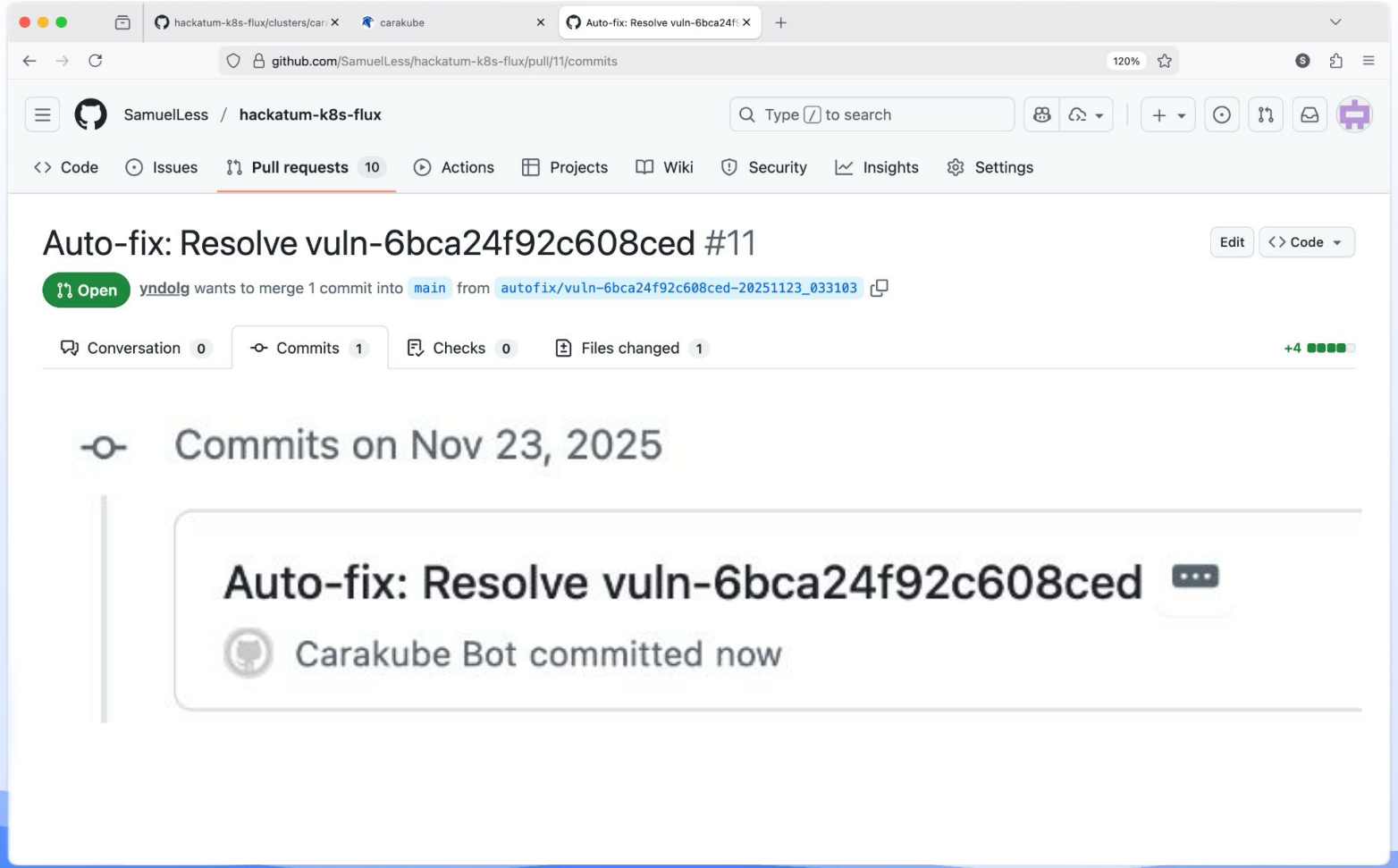

carakube.dev/demo
carakube
POD
hello-8010-db8f66bb6-vrc2s
STATUS
Phase
RUNNING
Pod IP
10.244.1.6
Host IP
172.20.0.2
Node
carakube-demo-worker
QoS Class
BestEffort
CONTAINERS (1)
http-echo
hashicorp/http-echo:0.2.3
Requests
– / –
Limits
– / –
8010/TCP
VOLUMES (1)
kube-api-access-c727x
Projected
LABELS
app: hello-8010
pod-template-hash: db8f66bb6
RECENT EVENTS
Scheduled
Successfully assigned default/hello-8010-db8f66bb6-vrc2s to carakube-demo-worker
Pulled
Container image "hashicorp/http-echo:0.2.3" already
Reset Layout
namespace
default
flux-system
podinfo0
helm-controller-cccd949cd-jrk8c
kustomize-controller-789f6ccd67-r97kg
notification-controller0
kube-proxy-cx7zj0
hello-8010-db8f66bb6-vrc2s
podinfo-b76f6cd59-b4mvs
coredns-7db6d8ff4d-4rstz0
coredns-7db6d8ff4d-jkdnf0
kube-controller-manager-carakube-demo-control-plane0
carakube-demo-control-plane0
React Flow
Filtering vulnerabilities for selected node
High
Resource Limits
Container: Http-Echo
Container missing resource limits: cpu, memory
Processing...
Medium Vulnerabilities
Medium
ServiceAccount
SA: Default
ServiceAccount token automatically mounted (default SA token is usually useless but increases attack surface)
Create PR
Low Vulnerabilities
Low
ServiceAccount
SA: Default
Pod uses default ServiceAccount (best practice: create dedicated SA)
Create PR

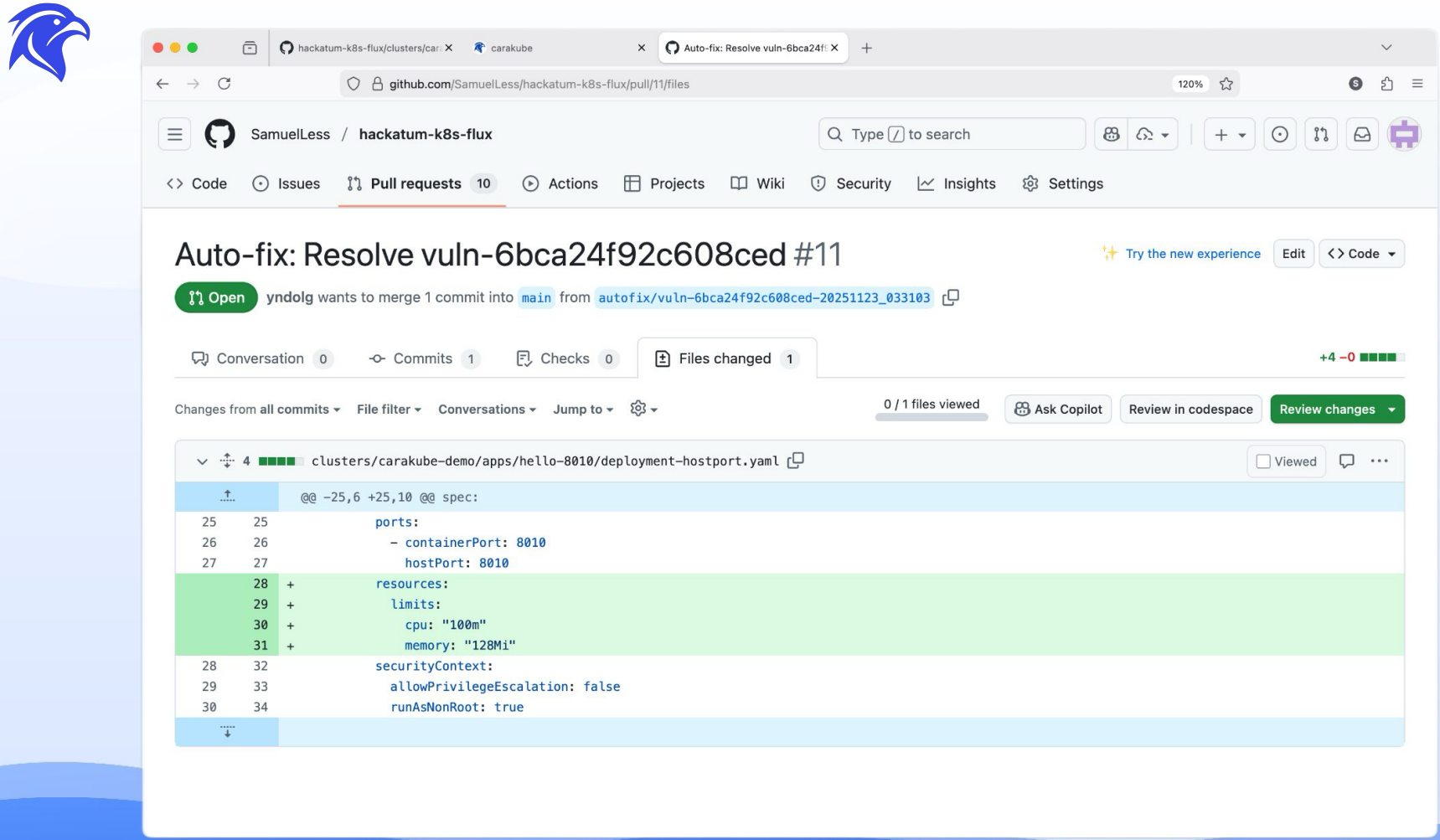


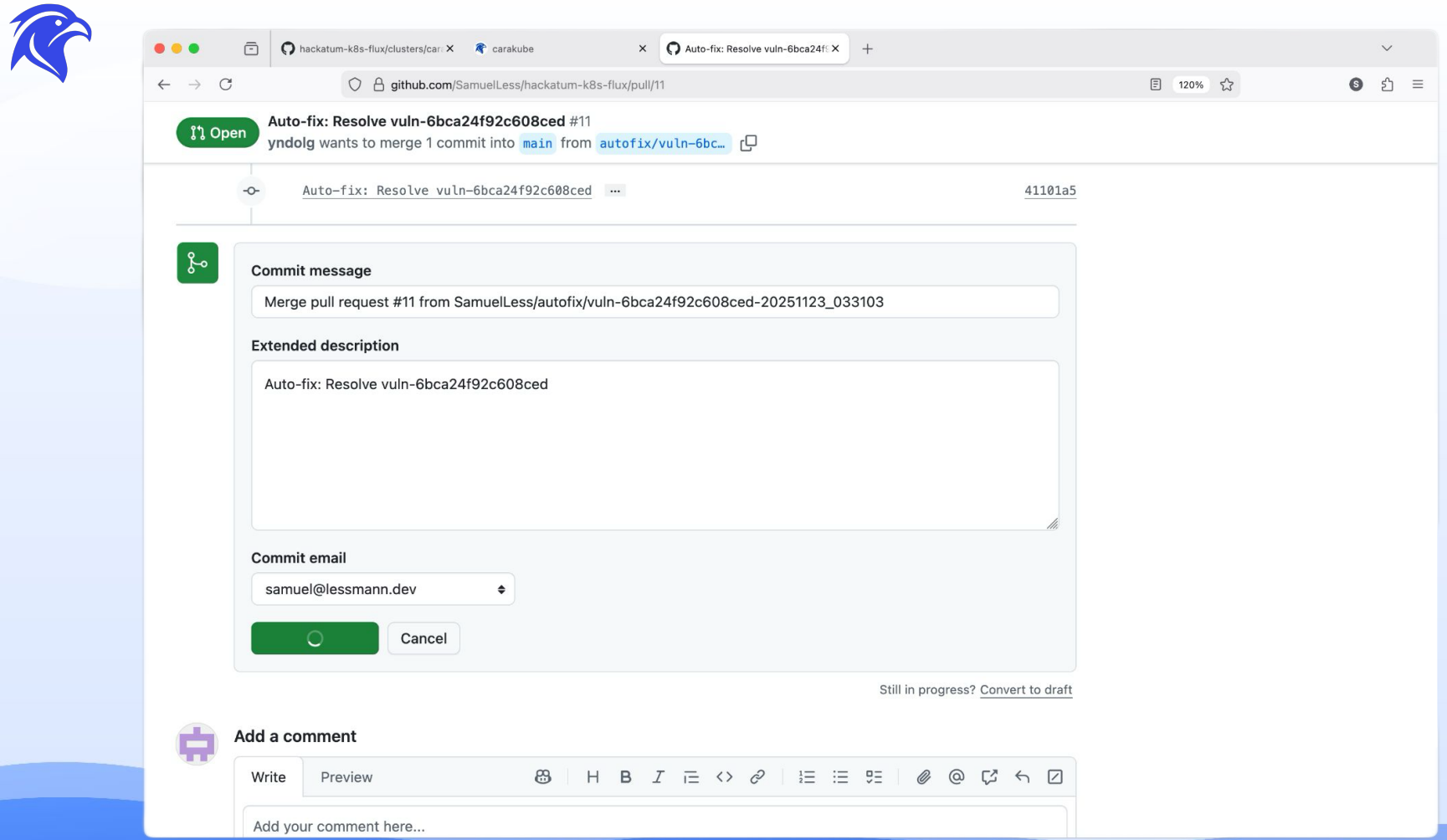

github.com/SamuelLess/hackatum-k8s-flux/pull/11

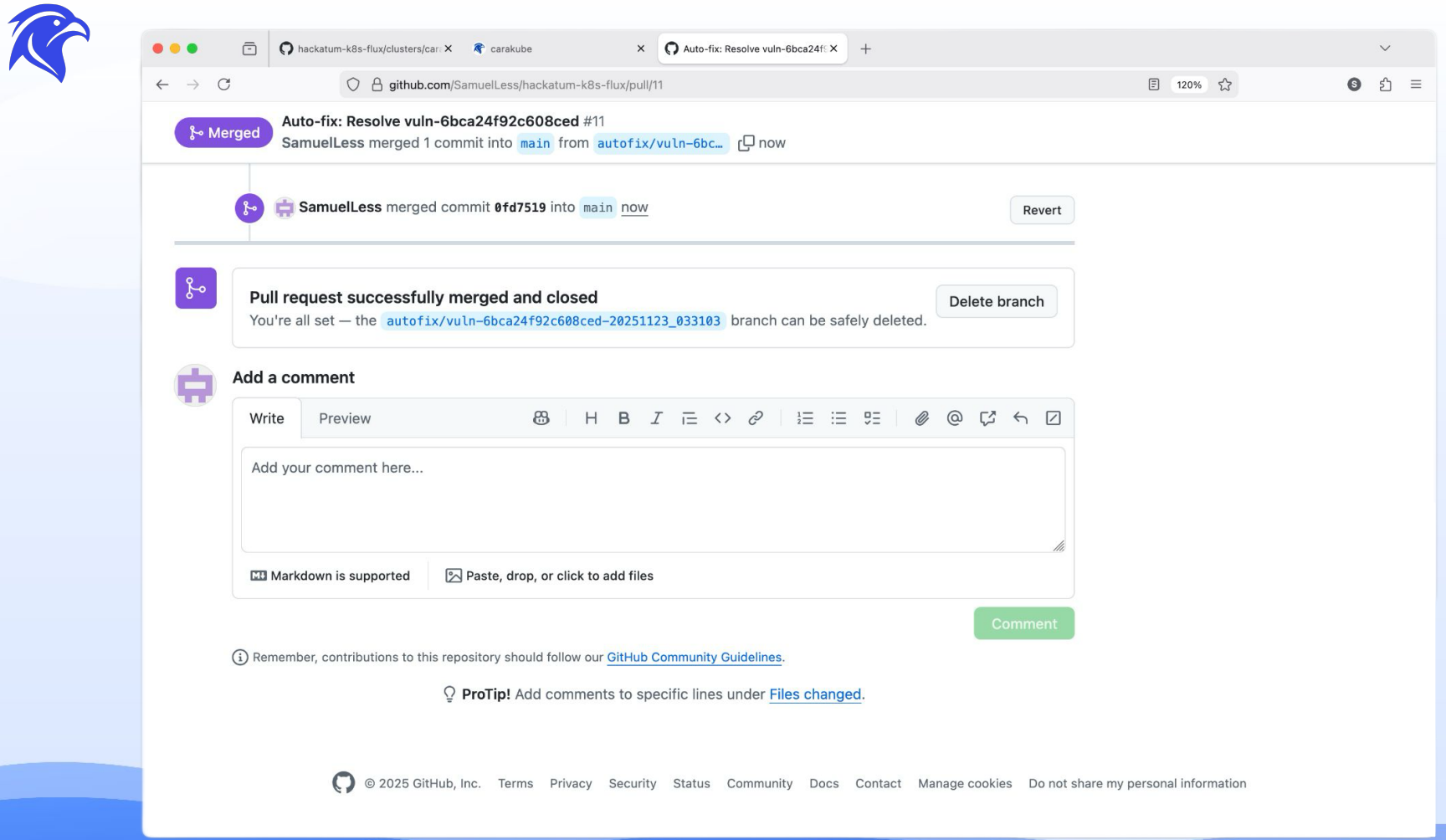

hackatum-k8s-flux/clusters/car
carakube
Auto-fix: Resolve vuln-6bca24f
github.com/SamuelLess/hackatum-k8s-flux/pull/11
120%
SamuelLess / hackatum-k8s-flux
Type / to search
Code
Issues
Pull requests 10
Actions
Projects
Wiki
Security
Insights
Settings
Auto-fix: Resolve vuln-6bca24f92c608ced #11
Edit
Code
Open
yndolg wants to merge 1 commit into main from autofix/vuln-6bca24f92c608ced-20251123_033103
Conversation 0
Commits 1
Checks 0
Files changed 1
+4 −0
yndolg commented now
Collaborator
Add CPU and Memory Resource Limits to http-echo container in hello-8010 pod
🔒 Security Issue
The http-echo container within the hello-8010 pod was configured without explicit CPU and memory resource limits. This is a significant security risk because a misbehaving or malicious process inside this container could potentially consume all available CPU cycles or memory on the node. This uncontrolled resource consumption could lead to a Denial of Service (DoS) for other critical applications running on the same node, or even cause the entire Kubernetes node to become unresponsive, impacting the stability and availability of the cluster. Without these limits, resource exhaustion attacks are much easier to execute and more damaging.
✅ How This Fix Addresses the Issue
This fix addresses the missing resource limits by explicitly defining CPU and memory limits for the http-echo container in the hello-8010 pod's deployment configuration. By setting these limits, we ensure that the container cannot consume more than its allocated share of resources. Specifically, the container is now limited to 100 millicores of CPU and 128 MiB
Reviewers
Suggestions
Copilot
Request
Still in progress? Convert to draft
Assignees
No one—assign yourself
Labels
None yet
Projects
None yet
Milestone

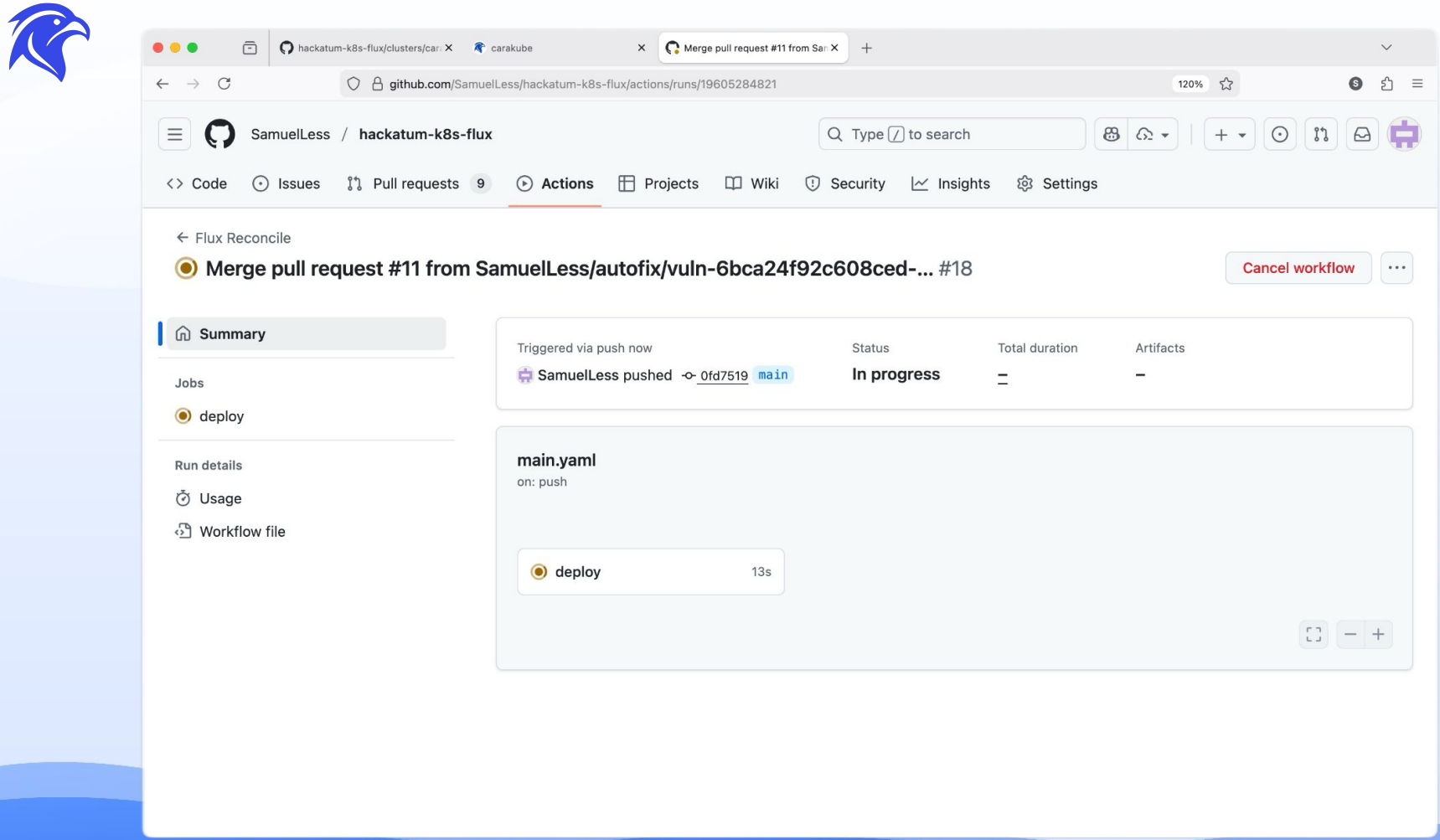

hackatum-k8s-flux/clusters/car
carakube
Auto-fix: Resolve vuln-6bca24f
github.com/SamuelLess/hackatum-k8s-flux/pull/11/commits
120%
SamuelLess / hackatum-k8s-flux
Type / to search
Code
Issues
Pull requests 10
Actions
Projects
Wiki
Security
Insights
Settings
Auto-fix: Resolve vuln-6bca24f92c608ced #11
Edit
Code
Open
yndolg wants to merge 1 commit into main from autofix/vuln-6bca24f92c608ced-20251123_033103
Conversation 0
Commits 1
Checks 0
Files changed 1
+4
Commits on Nov 23, 2025
Auto-fix: Resolve vuln-6bca24f92c608ced
Carakube Bot committed now
41101a5


hackatum-k8s-flux/clusters/car
carakube
Auto-fix: Resolve vuln-6bca24f
github.com/SamuelLess/hackatum-k8s-flux/pull/11/commits
120%
SamuelLess / hackatum-k8s-flux
Type / to search
Code
Issues
Pull requests 10
Actions
Projects
Wiki
Security
Insights
Settings
Auto-fix: Resolve vuln-6bca24f92c608ced #11
Edit
Code
Open
yndolg wants to merge 1 commit into main from autofix/vuln-6bca24f92c608ced-20251123_033103
Conversation 0
Commits 1
Checks 0
Files changed 1
+4
Commits on Nov 23, 2025
Auto-fix: Resolve vuln-6bca24f92c608ced
Carakube Bot committed now


hackatum-k8s-flux/clusters/car
carakube
Auto-fix: Resolve vuln-6bca24f
github.com/SamuelLess/hackatum-k8s-flux/pull/11/files
120%
SamuelLess / hackatum-k8s-flux
Type / to search
Code
Issues
Pull requests 10
Actions
Projects
Wiki
Security
Insights
Settings
Auto-fix: Resolve vuln-6bca24f92c608ced #11
Try the new experience
Edit
Code
Open
yndolg wants to merge 1 commit into main from autofix/vuln-6bca24f92c608ced-20251123_033103
Conversation 0
Commits 1
Checks 0
Files changed 1
+4 −0
Changes from all commits
File filter
Conversations
Jump to
0 / 1 files viewed
Ask Copilot
Review in codespace
Review changes
4
clusters/carakube-demo/apps/hello-8010/deployment-hostport.yaml
Viewed
@@ -25,6 +25,10 @@ spec:
25 25 ports:
26 26 - containerPort: 8010
27 27 hostPort: 8010
28 + resources:
29 + limits:
30 + cpu: "100m"
31 + memory: "128Mi"
28 32 securityContext:
29 33 allowPrivilegeEscalation: false
30 34 runAsNonRoot: true


hackatum-k8s-flux/clusters/car
carakube
Auto-fix: Resolve vuln-6bca24f
github.com/SamuelLess/hackatum-k8s-flux/pull/11
120%
Open
Auto-fix: Resolve vuln-6bca24f92c608ced #11
yndolg wants to merge 1 commit into main from autofix/vuln-6bc…
Auto-fix: Resolve vuln-6bca24f92c608ced
41101a5
Commit message
Merge pull request #11 from SamuelLess/autofix/vuln-6bca24f92c608ced-20251123_033103
Extended description
Auto-fix: Resolve vuln-6bca24f92c608ced
Commit email
samuel@lessmann.dev
Cancel
Still in progress? Convert to draft
Add a comment
Write
Preview
Add your comment here...


hackatum-k8s-flux/clusters/car
carakube
Auto-fix: Resolve vuln-6bca24f
github.com/SamuelLess/hackatum-k8s-flux/pull/11
120%
Merged
Auto-fix: Resolve vuln-6bca24f92c608ced #11
SamuelLess merged 1 commit into main from autofix/vuln-6bc…
now
SamuelLess merged commit 0fd7519 into main now
Revert
Pull request successfully merged and closed
You're all set — the autofix/vuln-6bca24f92c608ced-20251123_033103 branch can be safely deleted.
Delete branch
Add a comment
Write
Preview
Add your comment here...
Markdown is supported
Paste, drop, or click to add files
Comment
Remember, contributions to this repository should follow our GitHub Community Guidelines.
ProTip! Add comments to specific lines under Files changed.
© 2025 GitHub, Inc.
Terms
Privacy
Security
Status
Community
Docs
Contact
Manage cookies
Do not share my personal information


hackatum-k8s-flux/clusters/car
carakube
Merge pull request #11 from Sar
github.com/SamuelLess/hackatum-k8s-flux/actions/runs/19605284821
120%
SamuelLess / hackatum-k8s-flux
Type / to search
Code
Issues
Pull requests 9
Actions
Projects
Wiki
Security
Insights
Settings
Flux Reconcile
Merge pull request #11 from SamuelLess/autofix/vuln-6bca24f92c608ced-... #18
Cancel workflow
Summary
Jobs
deploy
Run details
Usage
Workflow file
Triggered via push now
SamuelLess pushed 0fd7519 main
Status
In progress
Total duration
–
Artifacts
–
main.yaml
on: push
deploy 13s

hackatum-k8s-flux/clusters/car | carakube | Merge pull request #11 from Sar

github.com/SamuelLess/hackatum-k8s-flux/actions/runs/19605284821/job/56142954159

120%

Summary

Jobs

deploy

Run details

Usage

Workflow file

**deploy**

Started 20s ago

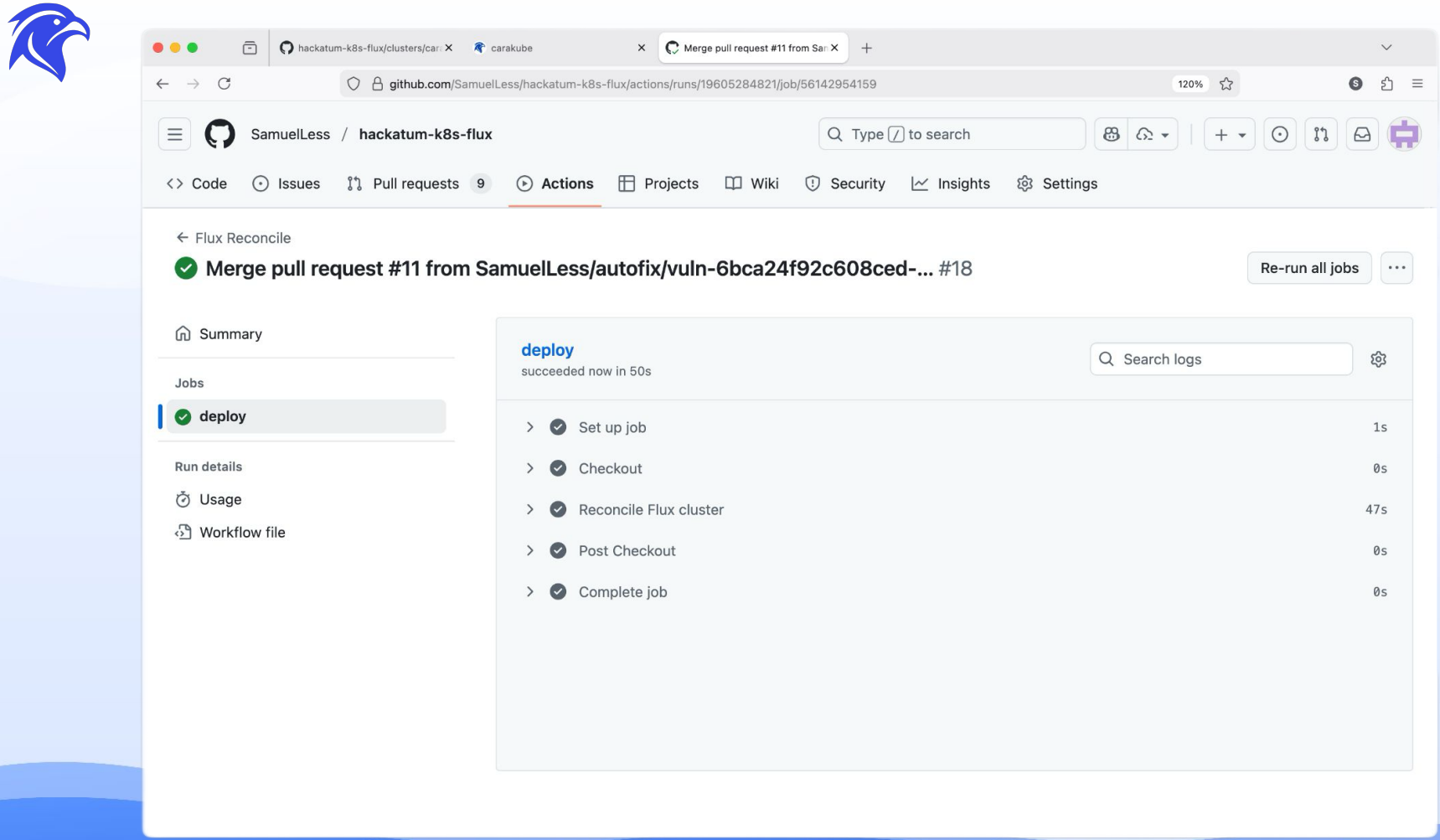
Search logs

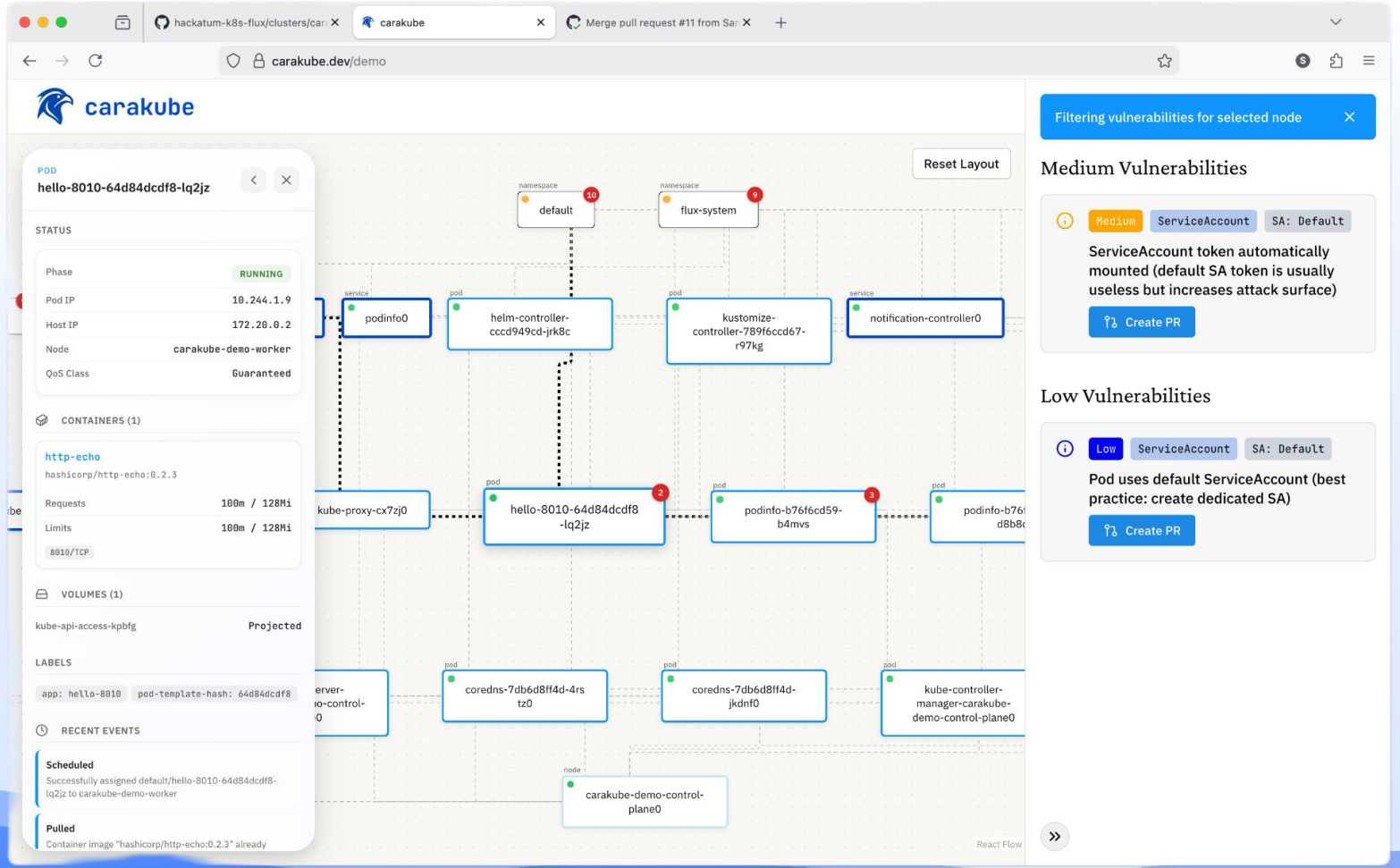
Reconcile Flux cluster 18s

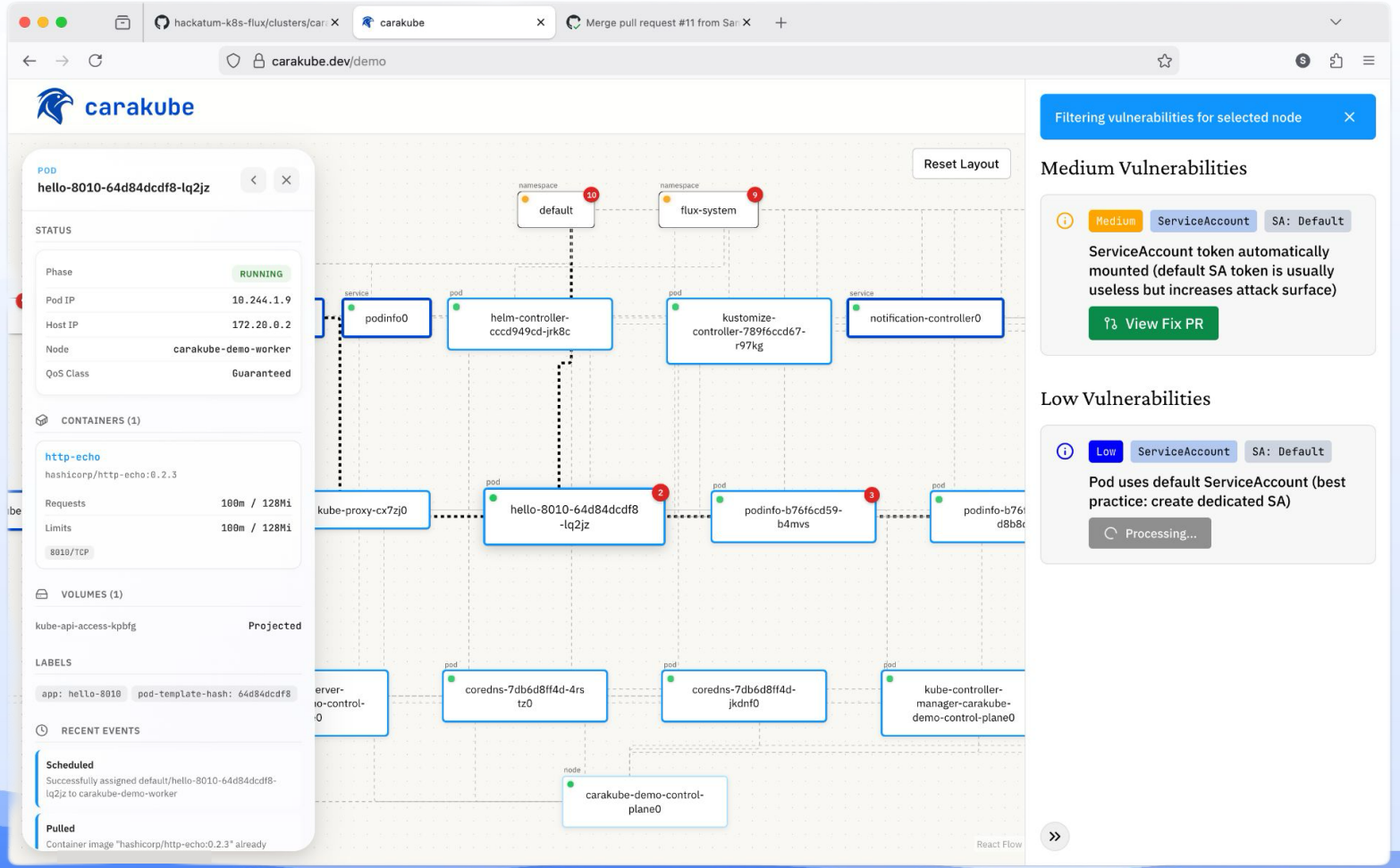
```
77  flux-system     main@sha1:1b0caa85     False          True    stored artifact for revision
    'main@sha1:1b0caa85'
78  ==> Forcing Git re-pull via Flux GitRepository 'flux-system' in ns 'flux-system'...
79  ► annotating GitRepository flux-system in flux-system namespace
80  ✔ GitRepository annotated
81  ◎ waiting for GitRepository reconciliation
82  ✔ fetched revision main@sha1:0fd7519009d8a853e563e9d20e63c52a823b613f
83  ==> Reconciling ALL Kustomizations across all namespaces (with-source)...
84  ----> Reconciling flux-system/flux-system
85  ► annotating GitRepository flux-system in flux-system namespace
86  ✔ GitRepository annotated
87  ◎ waiting for GitRepository reconciliation
88  ✔ fetched revision main@sha1:0fd7519009d8a853e563e9d20e63c52a823b613f
89  ► annotating Kustomization flux-system in flux-system namespace
90  ✔ Kustomization annotated
91  ◎ waiting for Kustomization reconciliation
92  ✔ applied revision main@sha1:0fd7519009d8a853e563e9d20e63c52a823b613f
93  ----> Reconciling flux-system/hello-8010
94  ► annotating GitRepository flux-system in flux-system namespace
95  ✔ GitRepository annotated
96  ◎ waiting for GitRepository reconciliation
97  ✔ fetched revision main@sha1:0fd7519009d8a853e563e9d20e63c52a823b613f
98  ► annotating Kustomization hello-8010 in flux-system namespace
99  ✔ Kustomization annotated
100 ◎ waiting for Kustomization reconciliation
```

Post Checkout

github.com/SamuelLess/hackatum-k8s-flux/actions/runs/19605284821/job/56142954159#step:3:94


hackatum-k8s-flux/clusters/car
carakube
Merge pull request #11 from Sar
github.com/SamuelLess/hackatum-k8s-flux/actions/runs/19605284821/job/56142954159
120%
SamuelLess / hackatum-k8s-flux
Type / to search
Code
Issues
Pull requests 9
Actions
Projects
Wiki
Security
Insights
Settings
Flux Reconcile
Merge pull request #11 from SamuelLess/autofix/vuln-6bca24f92c608ced-... #18
Re-run all jobs
Summary
Jobs
deploy
Run details
Usage
Workflow file
deploy
succeeded now in 50s
Search logs
Set up job 1s
Checkout 0s
Reconcile Flux cluster 47s
Post Checkout 0s
Complete job 0s


carakube
carakube.dev/demo
POD
hello-8010-64d84dcdf8-lq2jz
STATUS
Phase
RUNNING
Pod IP
10.244.1.9
Host IP
172.20.0.2
Node
carakube-demo-worker
QoS Class
Guaranteed
CONTAINERS (1)
http-echo
hashicorp/http-echo:0.2.3
Requests
100m / 128Mi
Limits
100m / 128Mi
8010/TCP
VOLUMES (1)
kube-api-access-kpbfg
Projected
LABELS
app: hello-8010
pod-template-hash: 64d84dcdf8
RECENT EVENTS
Scheduled
Successfully assigned default/hello-8010-64d84dcdf8-lq2jz to carakube-demo-worker
Pulled
Container image "hashicorp/http-echo:0.2.3" already
Reset Layout
namespace
default
flux-system
podinfo0
helm-controller-cccd949cd-jrk8c
kustomize-controller-789f6ccd67-r97kg
notification-controller0
kube-proxy-cx7zj0
hello-8010-64d84dcdf8-lq2jz
podinfo-b76f6cd59-b4mvs
coredns-7db6d8ff4d-4rstz0
coredns-7db6d8ff4d-jkdnf0
kube-controller-manager-carakube-demo-control-plane0
carakube-demo-control-plane0
Filtering vulnerabilities for selected node
Medium Vulnerabilities
Medium
ServiceAccount
SA: Default
ServiceAccount token automatically mounted (default SA token is usually useless but increases attack surface)
Create PR
Low Vulnerabilities
Low
ServiceAccount
SA: Default
Pod uses default ServiceAccount (best practice: create dedicated SA)
Create PR
React Flow


hackatum-k8s-flux/clusters/car
carakube
Merge pull request #11 from Sar
carakube.dev/demo
carakube
Reset Layout
POD
hello-8010-64d84dcdf8-lq2jz
STATUS
Phase
RUNNING
Pod IP
10.244.1.9
Host IP
172.20.0.2
Node
carakube-demo-worker
QoS Class
Guaranteed
CONTAINERS (1)
http-echo
hashicorp/http-echo:0.2.3
Requests
100m / 128Mi
Limits
100m / 128Mi
8010/TCP
VOLUMES (1)
kube-api-access-kpbfg
Projected
LABELS
app: hello-8010
pod-template-hash: 64d84dcdf8
RECENT EVENTS
Scheduled
Successfully assigned default/hello-8010-64d84dcdf8-lq2jz to carakube-demo-worker
Pulled
Container image "hashicorp/http-echo:0.2.3" already
namespace
default
10
namespace
flux-system
9
service
podinfo0
pod
helm-controller-cccd949cd-jrk8c
pod
kustomize-controller-789f6ccd67-r97kg
service
notification-controller0
kube-proxy-cx7zj0
pod
hello-8010-64d84dcdf8-lq2jz
2
pod
podinfo-b76f6cd59-b4mvs
3
pod
podinfo-b76f
d8b8
pod
coredns-7db6d8ff4d-4rstz0
pod
coredns-7db6d8ff4d-jkdnf0
pod
kube-controller-manager-carakube-demo-control-plane0
node
carakube-demo-control-plane0
React Flow
Filtering vulnerabilities for selected node
Medium Vulnerabilities
Medium
ServiceAccount
SA: Default
ServiceAccount token automatically mounted (default SA token is usually useless but increases attack surface)
View Fix PR
Low Vulnerabilities
Low
ServiceAccount
SA: Default
Pod uses default ServiceAccount (best practice: create dedicated SA)
Processing...

carakube.dev

CaraKube

## 🤖 GitOps by Design

## 🚀 Trivially Expandable

## 🧩 Seamless `kubectl` Integration

CaraKube

# Any Questions?