

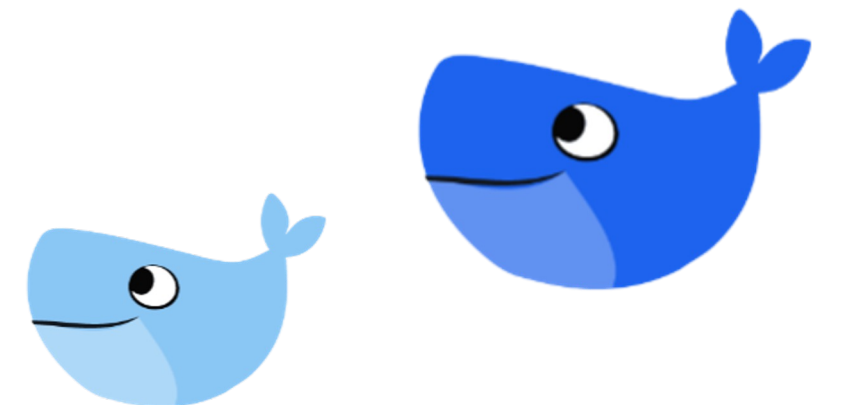
What's in My Container?

Docker Scout CLI and CI to the Rescue

Yves Brissaud

Senior Software Engineer | Docker 

X @_crev_

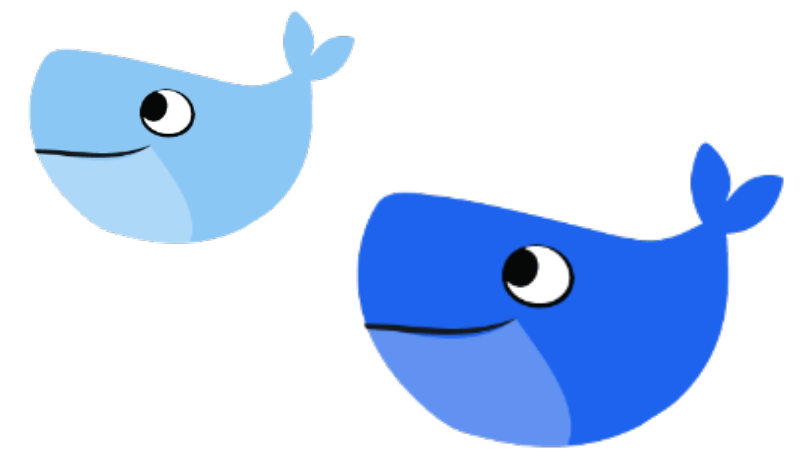




Yves Brissaud

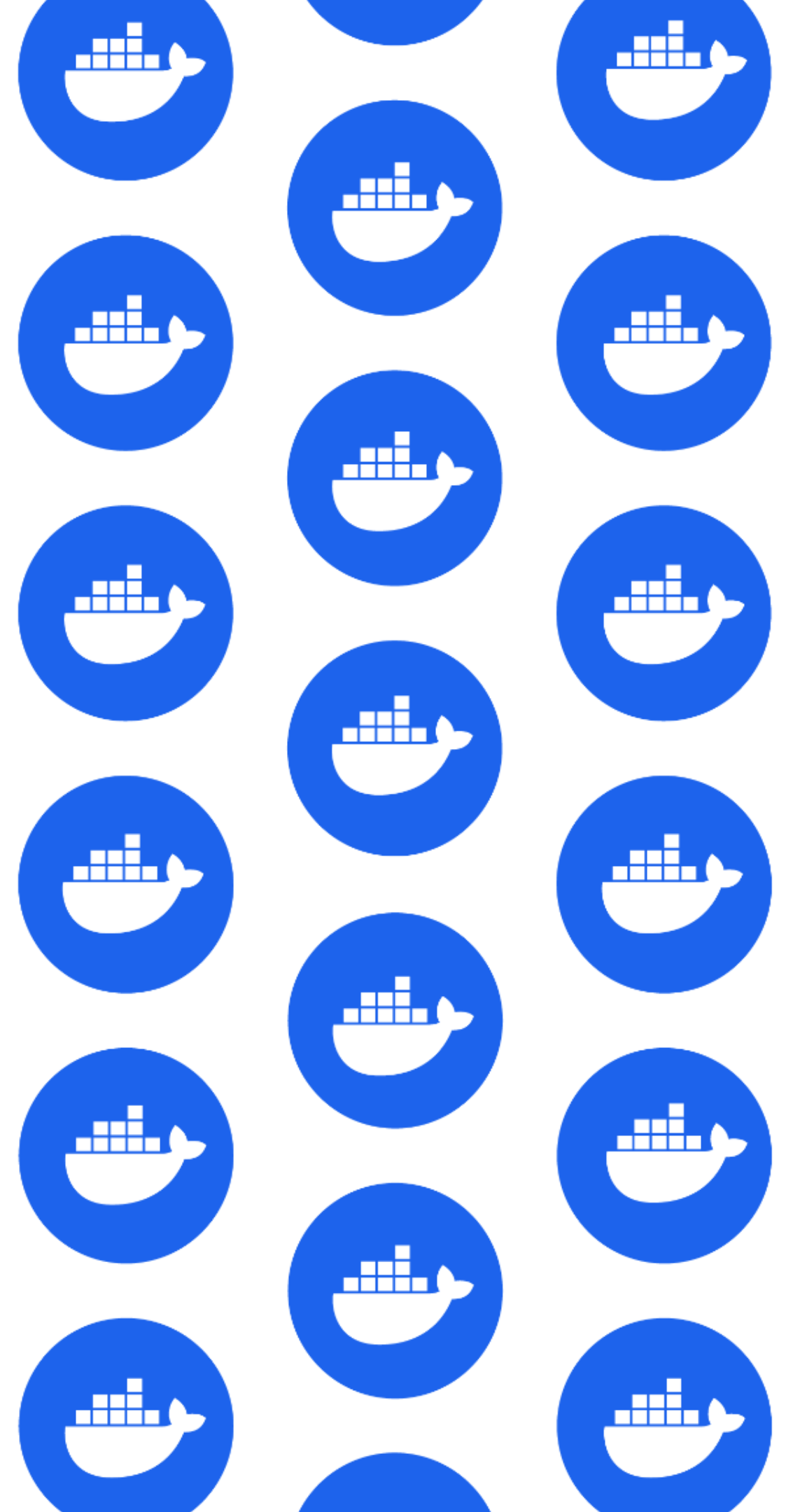
Senior Software Engineer | Docker

X @_crev_



00

Intro



Materials

Slides:

<https://speakerdeck.com/economie/scout>

Git Repository:

<https://github.com/economie/dc23hello>

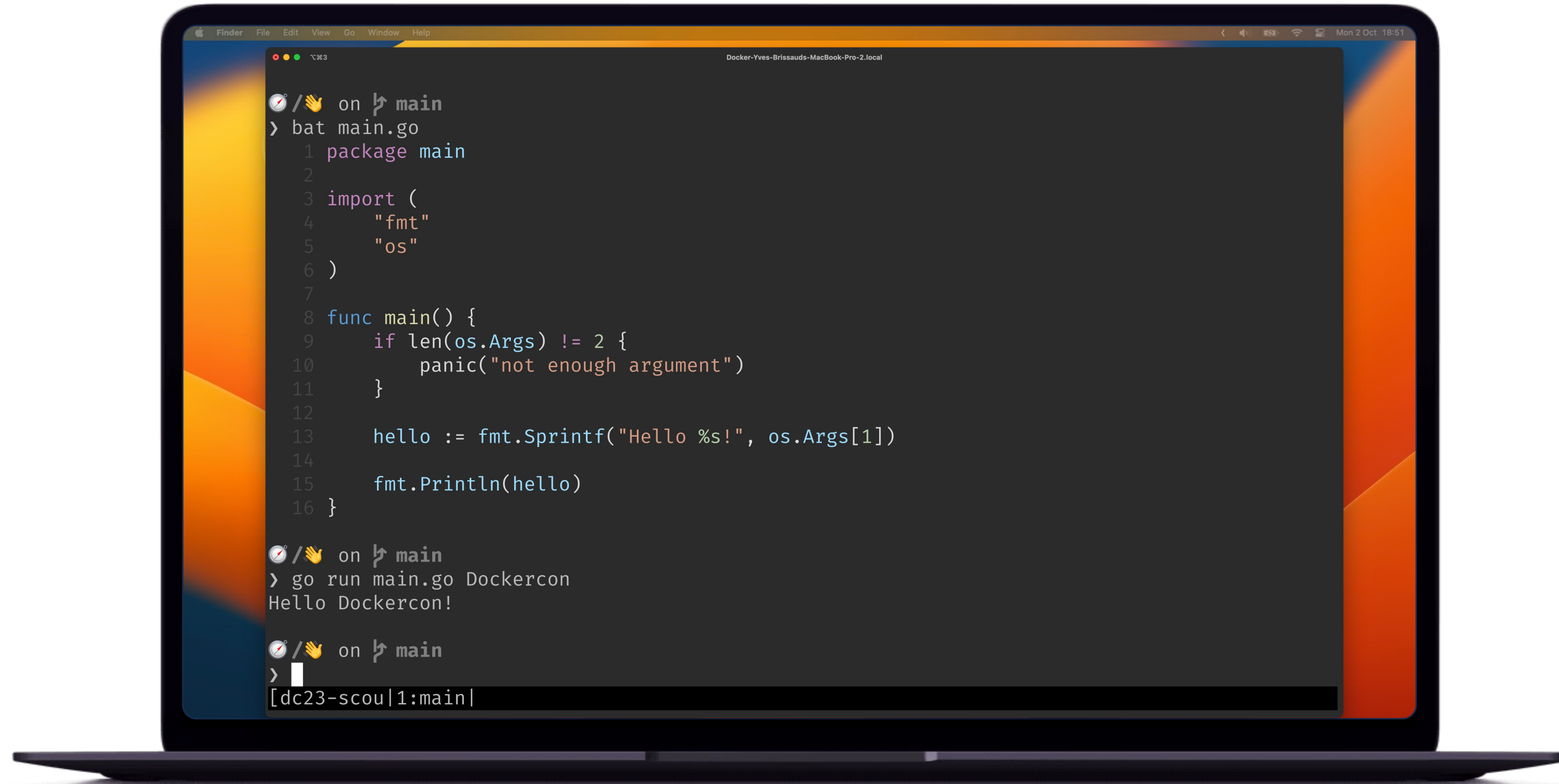


01

**Code
Update**



Hello 🙌



```
Finder File Edit View Go Window Help
Docker-Yves-Brissauds-MacBook-Pro-2.local

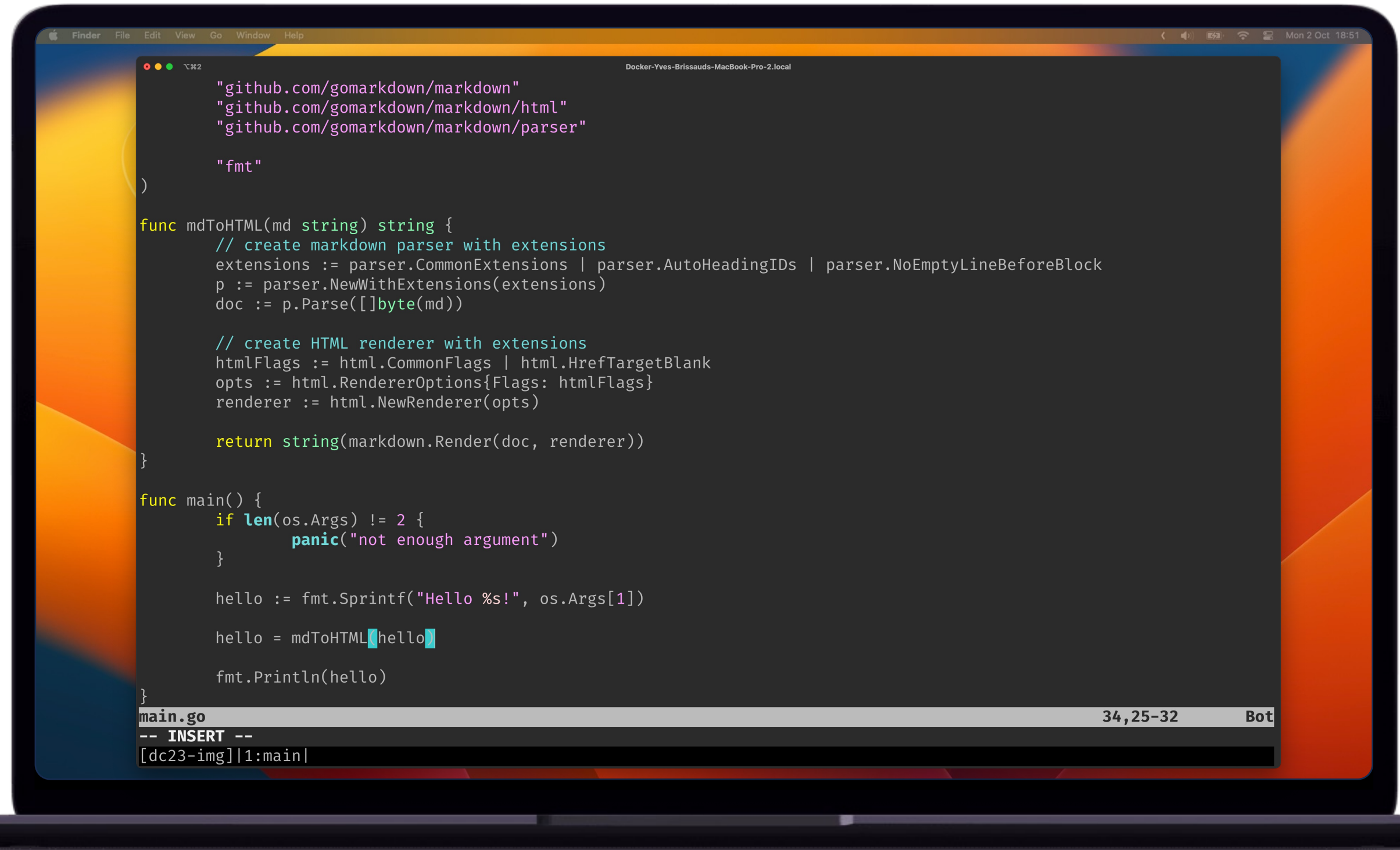
🕒/🙌 on ↩ main
> bat main.go
1 package main
2
3 import (
4     "fmt"
5     "os"
6 )
7
8 func main() {
9     if len(os.Args) != 2 {
10        panic("not enough argument")
11    }
12
13    hello := fmt.Sprintf("Hello %s!", os.Args[1])
14
15    fmt.Println(hello)
16 }

🕒/🙌 on ↩ main
> go run main.go Dockercon
Hello Dockercon!

🕒/🙌 on ↩ main
>
[dc23-scou|1:main|
```

Propose Changes

- Render as HTML
- Read input as markdown

A laptop screen showing a code editor with Go code. The code defines a function `mdToHTML` that takes a markdown string and returns its HTML representation. It uses the `github.com/gomarkdown/markdown` package for parsing and the `github.com/gomarkdown/markdown/html` package for rendering. The `main` function reads a command-line argument, formats it with "Hello %s!", and then calls `mdToHTML` to render the result. The code is displayed in a dark-themed editor with syntax highlighting. The status bar at the bottom of the editor shows the file name `main.go`, the current line and column `34,25-32`, and the word `Bot`.

```
Finder File Edit View Go Window Help
Docker-Yves-Brissauds-MacBook-Pro-2.local
"github.com/gomarkdown/markdown"
"github.com/gomarkdown/markdown/html"
"github.com/gomarkdown/markdown/parser"

"fmt"
)

func mdToHTML(md string) string {
    // create markdown parser with extensions
    extensions := parser.CommonExtensions | parser.AutoHeadingIDs | parser.NoEmptyLineBeforeBlock
    p := parser.NewWithExtensions(extensions)
    doc := p.Parse([]byte(md))

    // create HTML renderer with extensions
    htmlFlags := html.CommonFlags | html.HrefTargetBlank
    opts := html.RendererOptions{Flags: htmlFlags}
    renderer := html.NewRenderer(opts)

    return string(markdown.Render(doc, renderer))
}

func main() {
    if len(os.Args) != 2 {
        panic("not enough argument")
    }

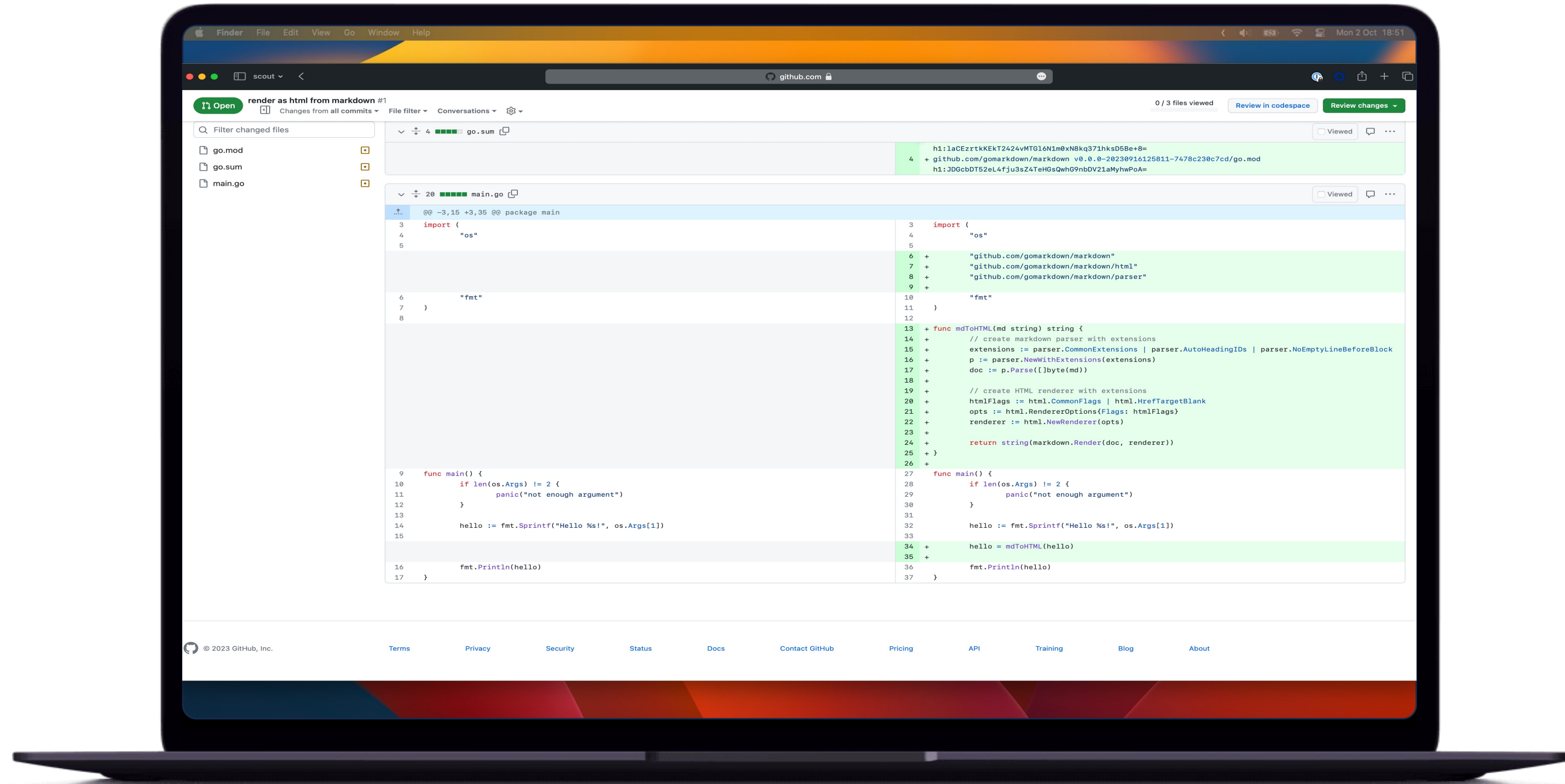
    hello := fmt.Sprintf("Hello %s!", os.Args[1])

    hello = mdToHTML(hello)

    fmt.Println(hello)
}
main.go 34,25-32 Bot
-- INSERT --
[dc23-img]|1:main|
```


Pull Request

- Build
- Test
- Review
- Merge
- Deploy
- ...



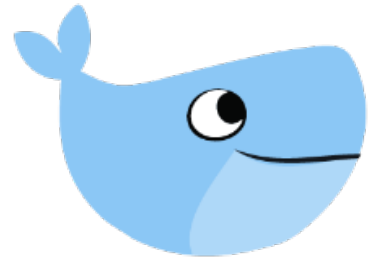
A vulnerability has been found before to be deployed in production!



<https://www.pexels.com/photo/red-led-traffic-cone-2743739/>

**Back to code, branch,
review, ...**





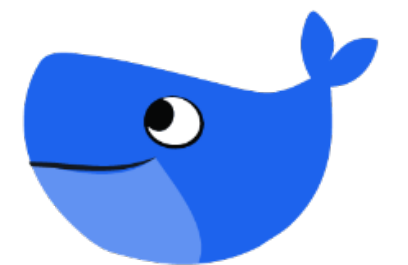
How to do it better?

Shift left

Find issues earlier

In developer friendly manner

Without wasting time



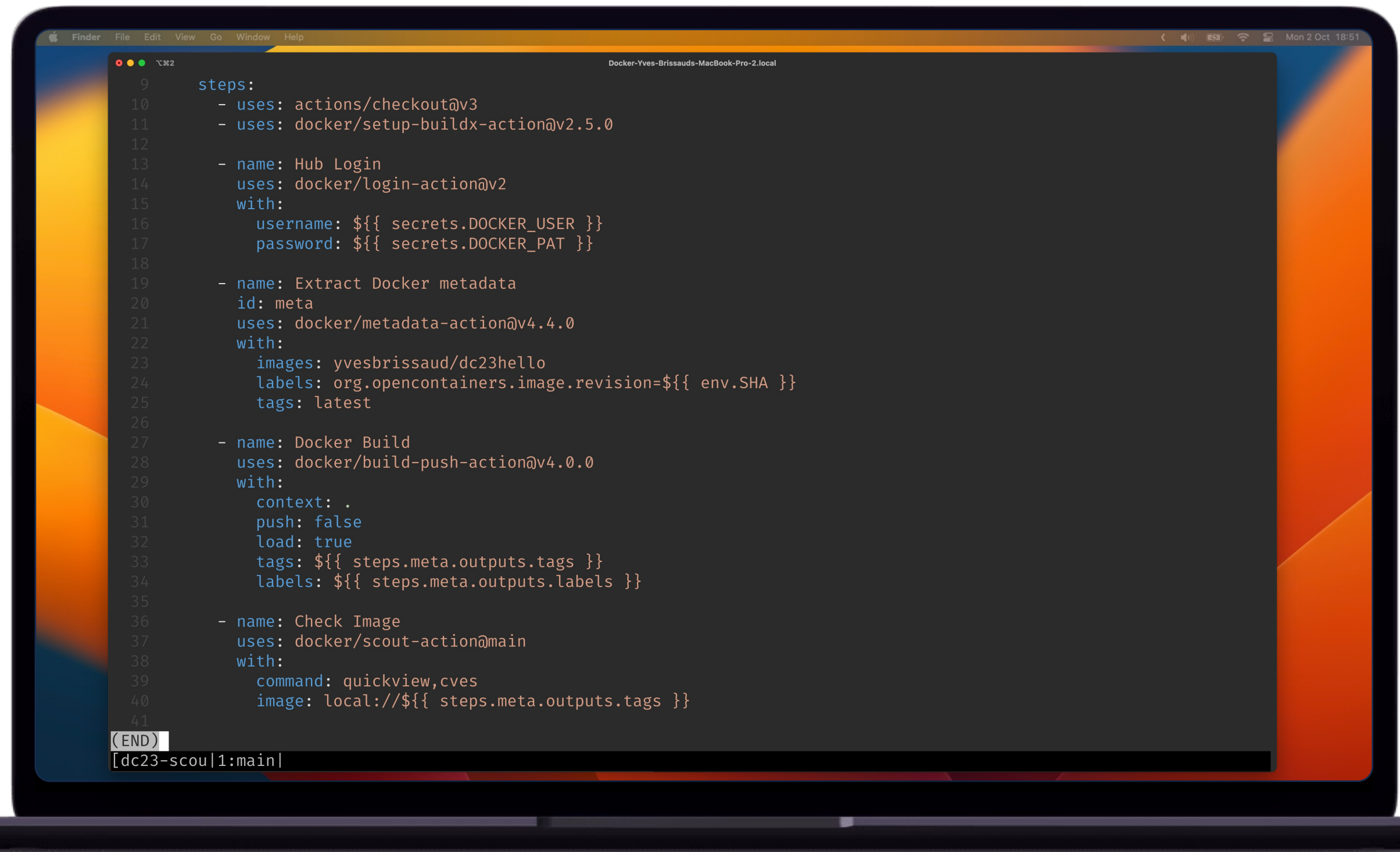
02

Continuous Integration



Docker Scout

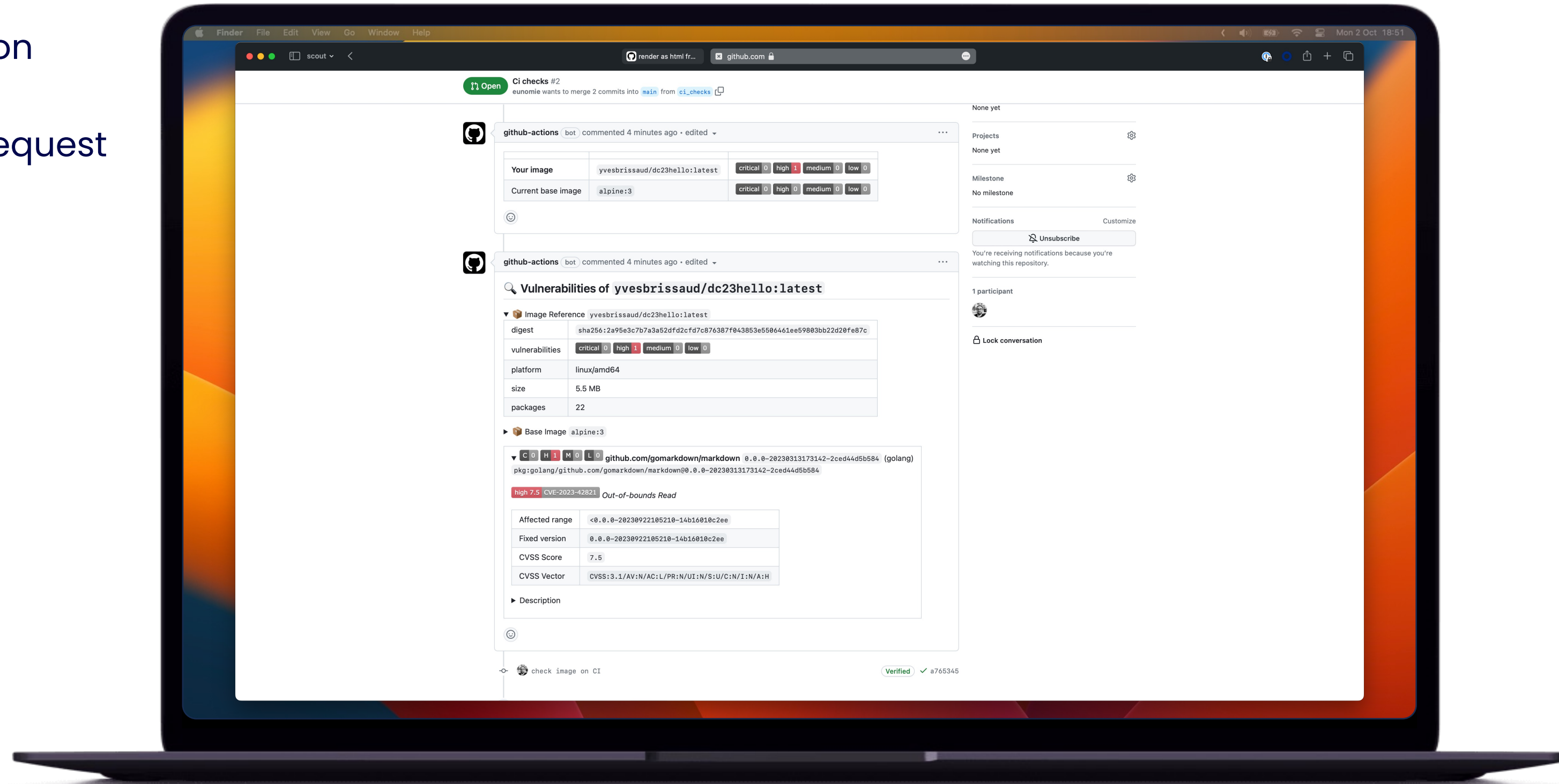
- As a GitHub Action

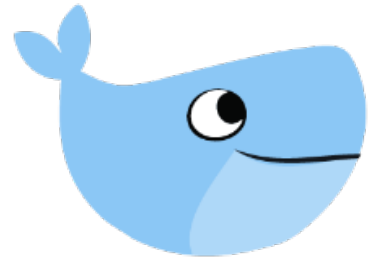


```
9  steps:
10   - uses: actions/checkout@v3
11   - uses: docker/setup-buildx-action@v2.5.0
12
13   - name: Hub Login
14     uses: docker/login-action@v2
15     with:
16       username: ${ secrets.DOCKER_USER }
17       password: ${ secrets.DOCKER_PAT }
18
19   - name: Extract Docker metadata
20     id: meta
21     uses: docker/metadata-action@v4.4.0
22     with:
23       images: yvesbrissaud/dc23hello
24       labels: org.opencontainers.image.revision=${ env.SHA }
25       tags: latest
26
27   - name: Docker Build
28     uses: docker/build-push-action@v4.0.0
29     with:
30       context: .
31       push: false
32       load: true
33       tags: ${ steps.meta.outputs.tags }
34       labels: ${ steps.meta.outputs.labels }
35
36   - name: Check Image
37     uses: docker/scout-action@main
38     with:
39       command: quickview,cves
40       image: local://${ steps.meta.outputs.tags }
41
42 (END)
[dc23-scou|1:main|
```

Docker Scout

- As a GitHub Action
- Comment Pull Request

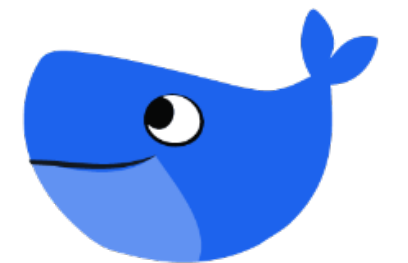




How to know it, before the CI?

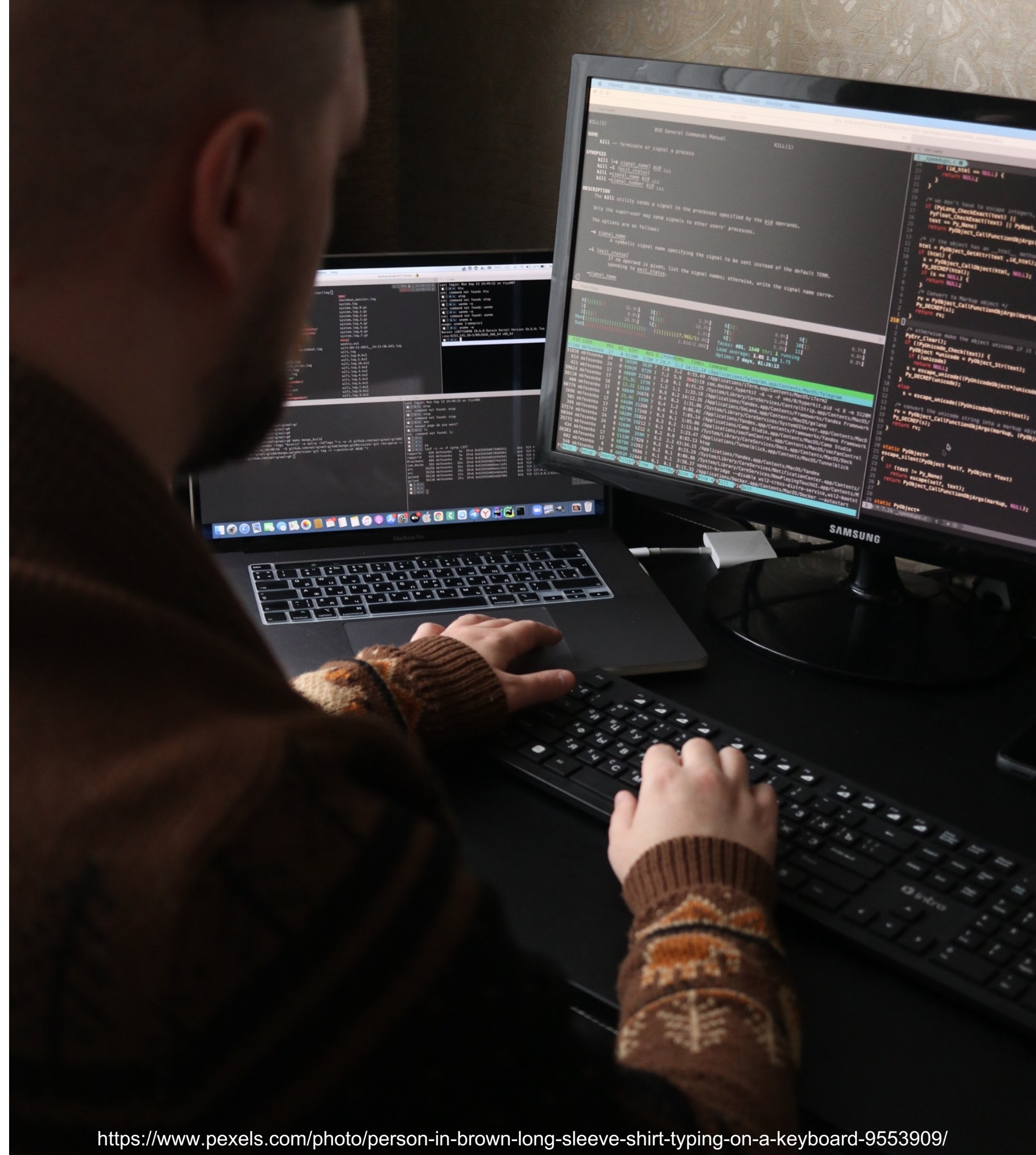
Shift left

Reduce time to discover issue



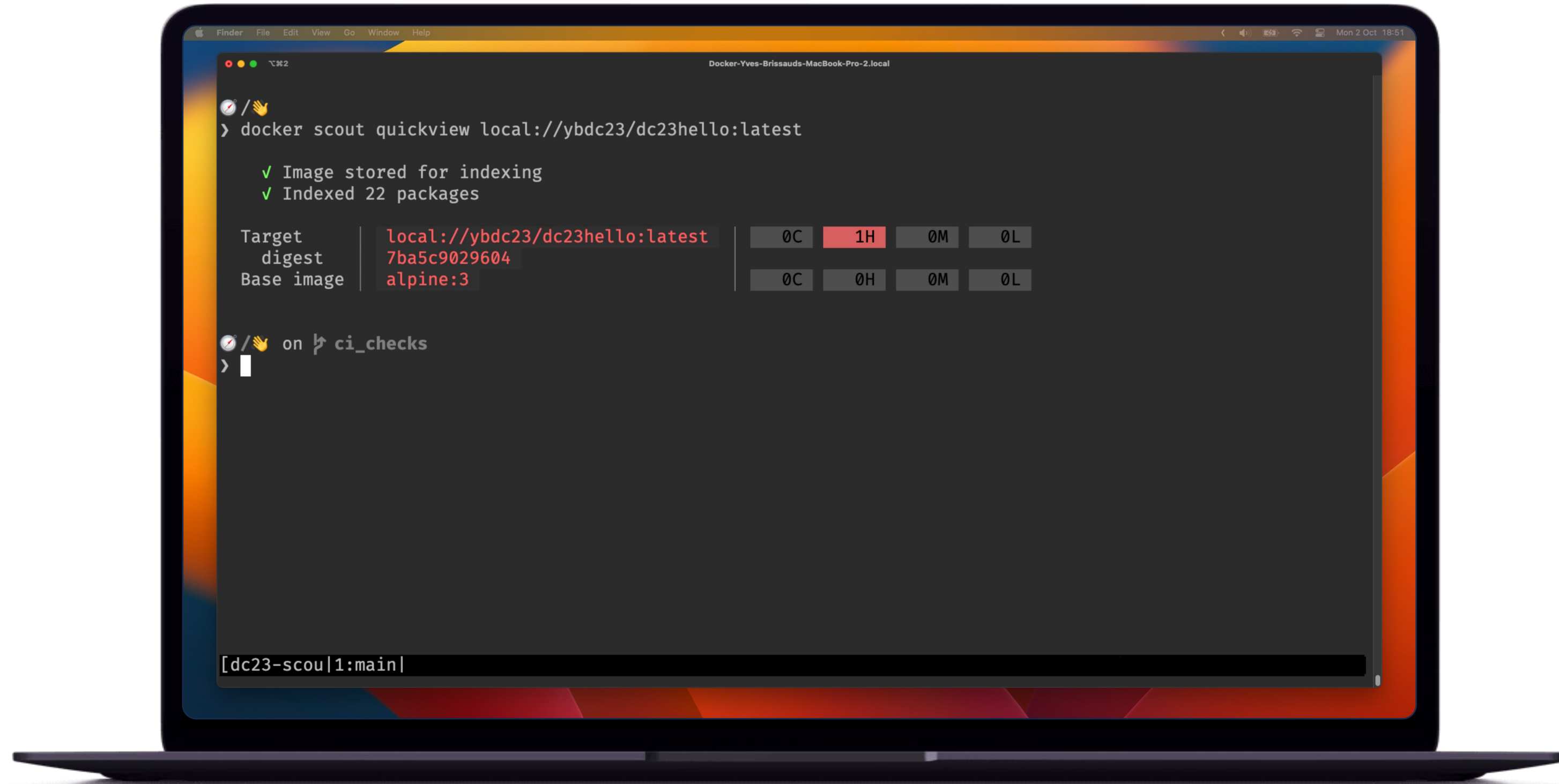
03

CLI



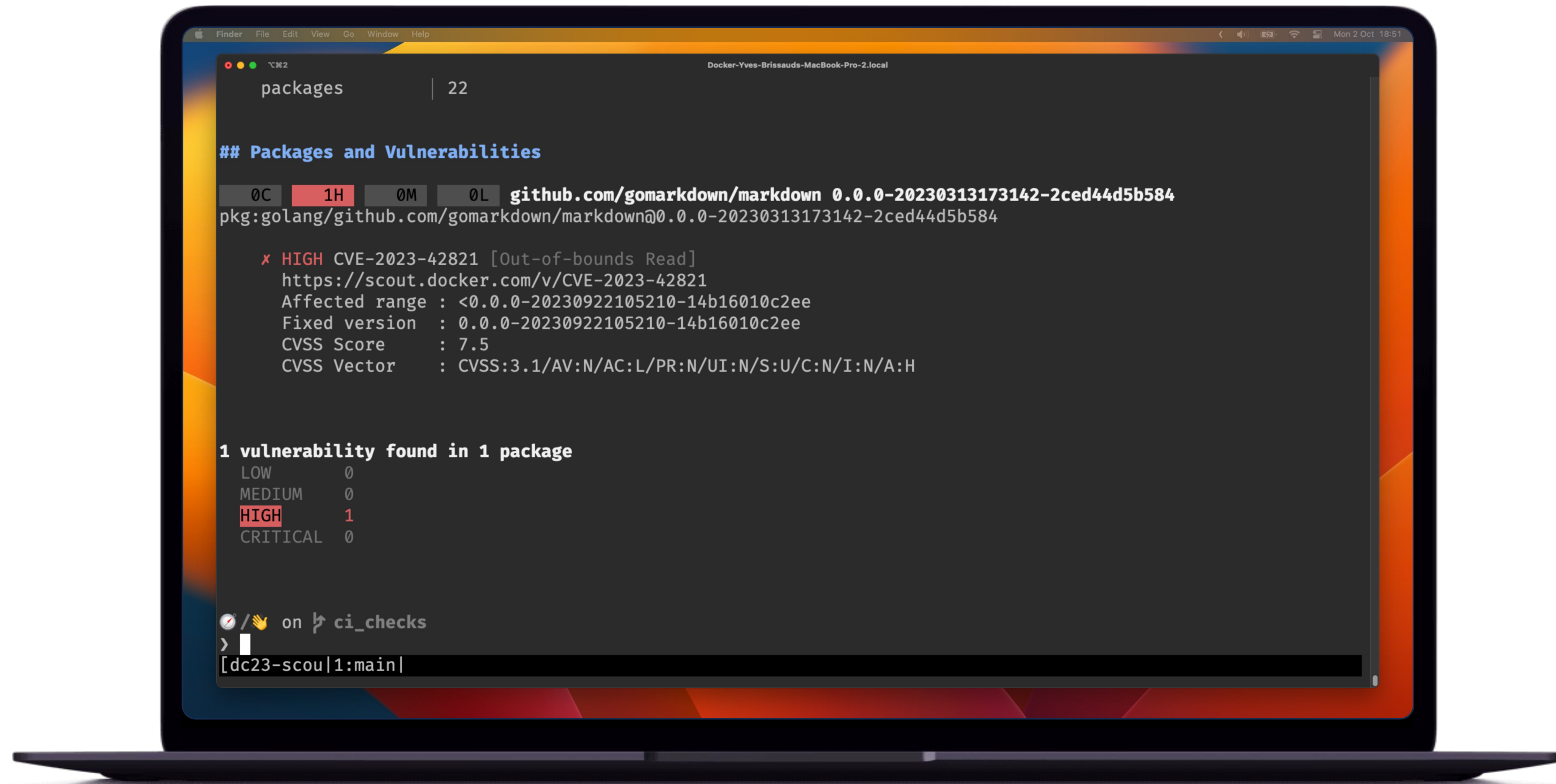
Docker Scout CLI

- quickview



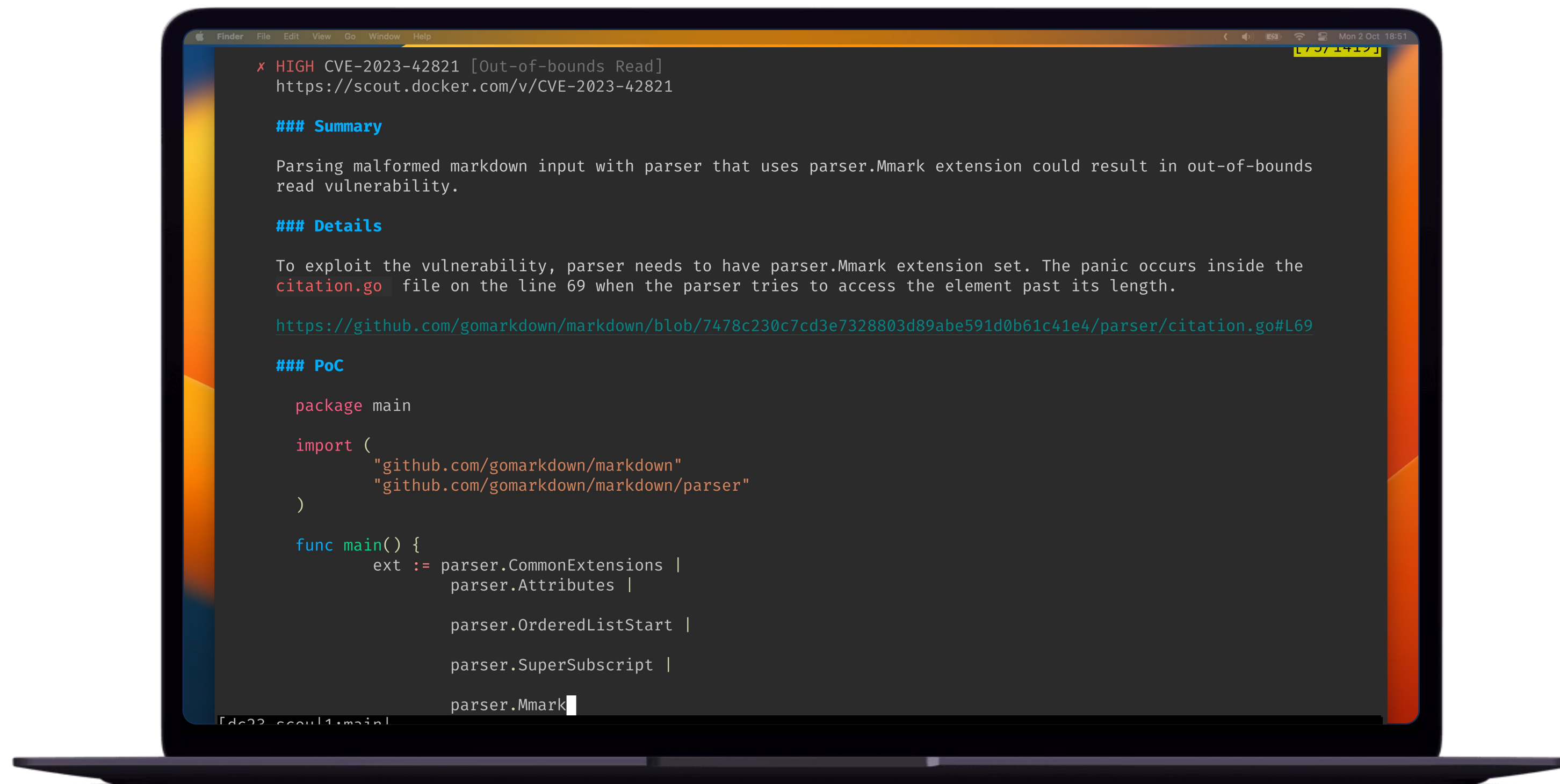
Docker Scout CLI

- quickview
- cves



Docker Scout CLI

- quickview
- cves
 - With details



Docker Scout CLI

- quickview
- cves
 - With details
 - By packages

```

Finder File Edit View Go Window Help
on ci_checks
> docker scout cves --format only-packages local://yvesbrissaud/dc23hello:latest
  ✓ SBOM of image already cached, 22 packages indexed
  ✗ Detected 1 vulnerable package with 1 vulnerability

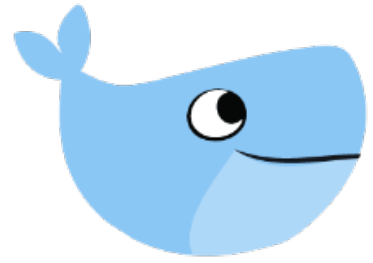
```

Name	Version	Type	Vulnerabilities			
alpine-baselayout	3.4.3-r1	apk	0C	0H	0M	0L
alpine-baselayout-data	3.4.3-r1	apk	0C	0H	0M	0L
alpine-keys	2.4-r1	apk	0C	0H	0M	0L
apk-tools	2.14.0-r2	apk	0C	0H	0M	0L
busybox	1.36.1-r2	apk	0C	0H	0M	0L
busybox-binsh	1.36.1-r2	apk	0C	0H	0M	0L
ca-certificates	20230506-r0	apk	0C	0H	0M	0L
ca-certificates-bundle	20230506-r0	apk	0C	0H	0M	0L
command-line-arguments	(devel)	golang	0C	0H	0M	0L
github.com/gomarkdown/markdown	0.0.0-20230313173142-2ced44d5b584	golang	0C	1H	0M	0L
libc-dev	0.7.2-r5	apk	0C	0H	0M	0L
libc-utils	0.7.2-r5	apk	0C	0H	0M	0L
libcrypto3	3.1.3-r0	apk	0C	0H	0M	0L
libssl3	3.1.3-r0	apk	0C	0H	0M	0L
musl	1.2.4-r1	apk	0C	0H	0M	0L
musl-utils	1.2.4-r1	apk	0C	0H	0M	0L
openssl	3.1.3-r0	apk	0C	0H	0M	0L
pax-utils	1.3.7-r1	apk	0C	0H	0M	0L
scanelf	1.3.7-r1	apk	0C	0H	0M	0L
ssl_client	1.36.1-r2	apk	0C	0H	0M	0L
stdlib	1.21.1	golang	0C	0H	0M	0L
zlib	1.2.13-r1	apk	0C	0H	0M	0L

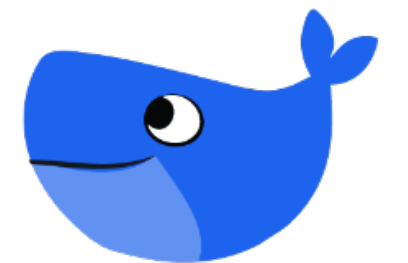
```

on ci_checks
>
[dc23-scout1:main]

```

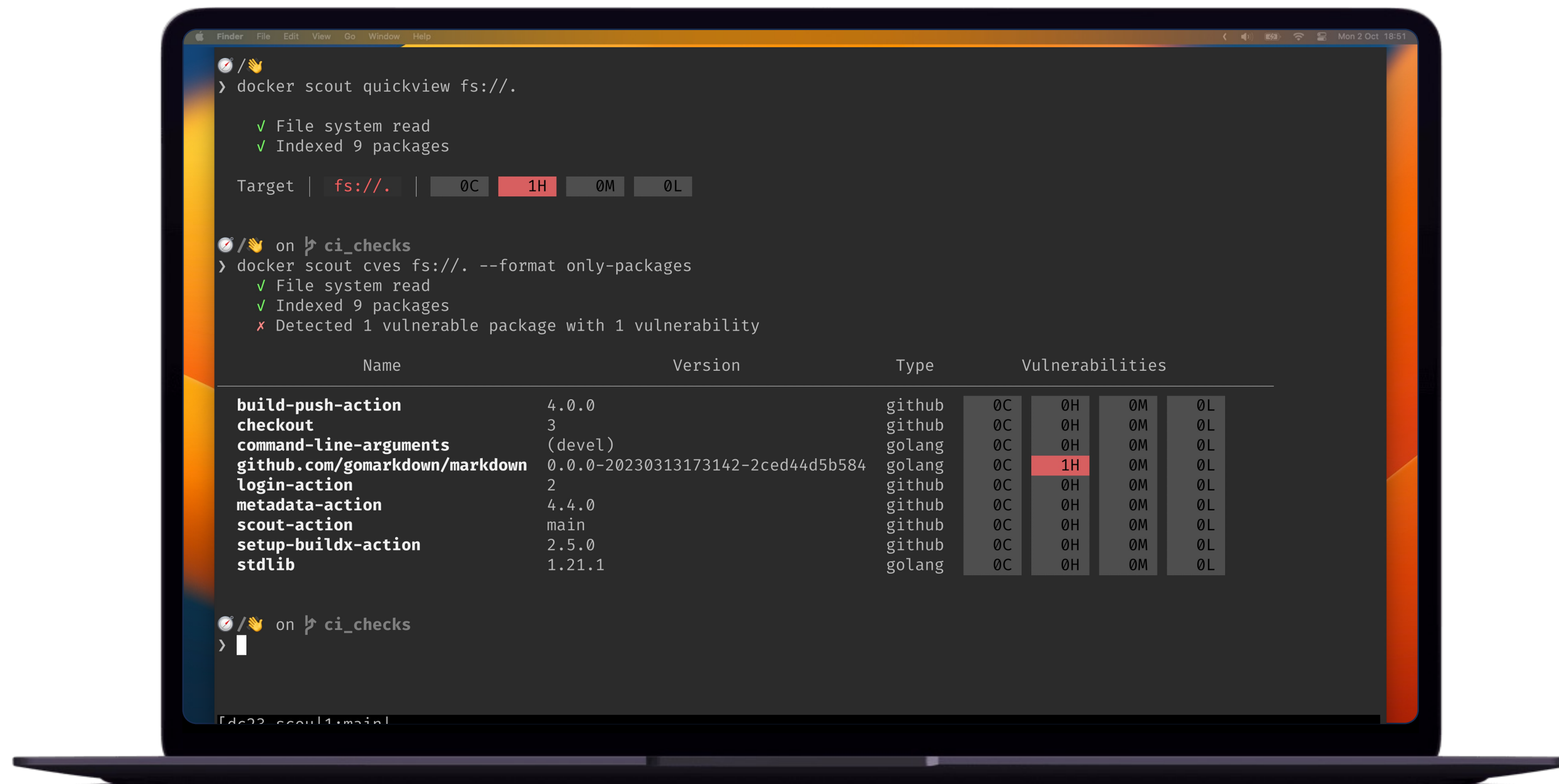



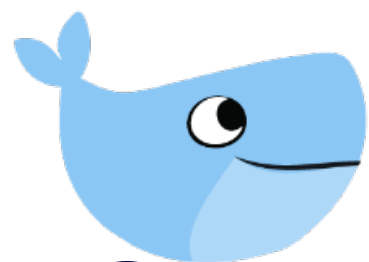
Why not be even faster?



Docker Scout CLI

- file system

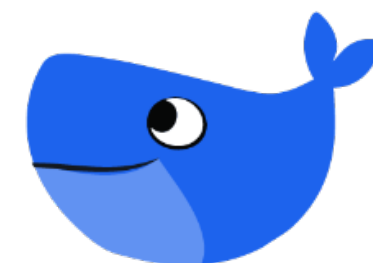




Can I see the impact of my changes?

Reduce noise

Straight to the decisions



04

Compare



Compare Images

- cli

```

> docker scout compare \
  --ignore-unchanged \
  local://ybdc23/dc23hello \
  --to registry://ybdc23/dc23hello

WARN 'docker scout compare' is experimental and its behaviour might change in the future
✓ SBOM of image already cached, 22 packages indexed
✓ SBOM of image already cached, 16 packages indexed

## Overview

```

	Analyzed Image	Comparison Image
Target	local://ybdc23/dc23hello:latest	registry://ybdc23/dc23hello:latest
digest	cbecb481f1c6	5cb20425be1e
platform	linux/arm64/v8	linux/arm64
provenance		https://github.com/eunomie/dc23hello
vulnerabilities	0C 1H 0M 0L +1	0C 0H 0M 0L
size	4.9 MB (+493 kB)	4.4 MB
packages	22 (+6)	16
Base image	alpine:3	alpine:3
tags	also known as • 3.18 • 3.18.4 • latest	also known as • 3.18 • 3.18.4 • latest
vulnerabilities	0C 0H 0M 0L	0C 0H 0M 0L

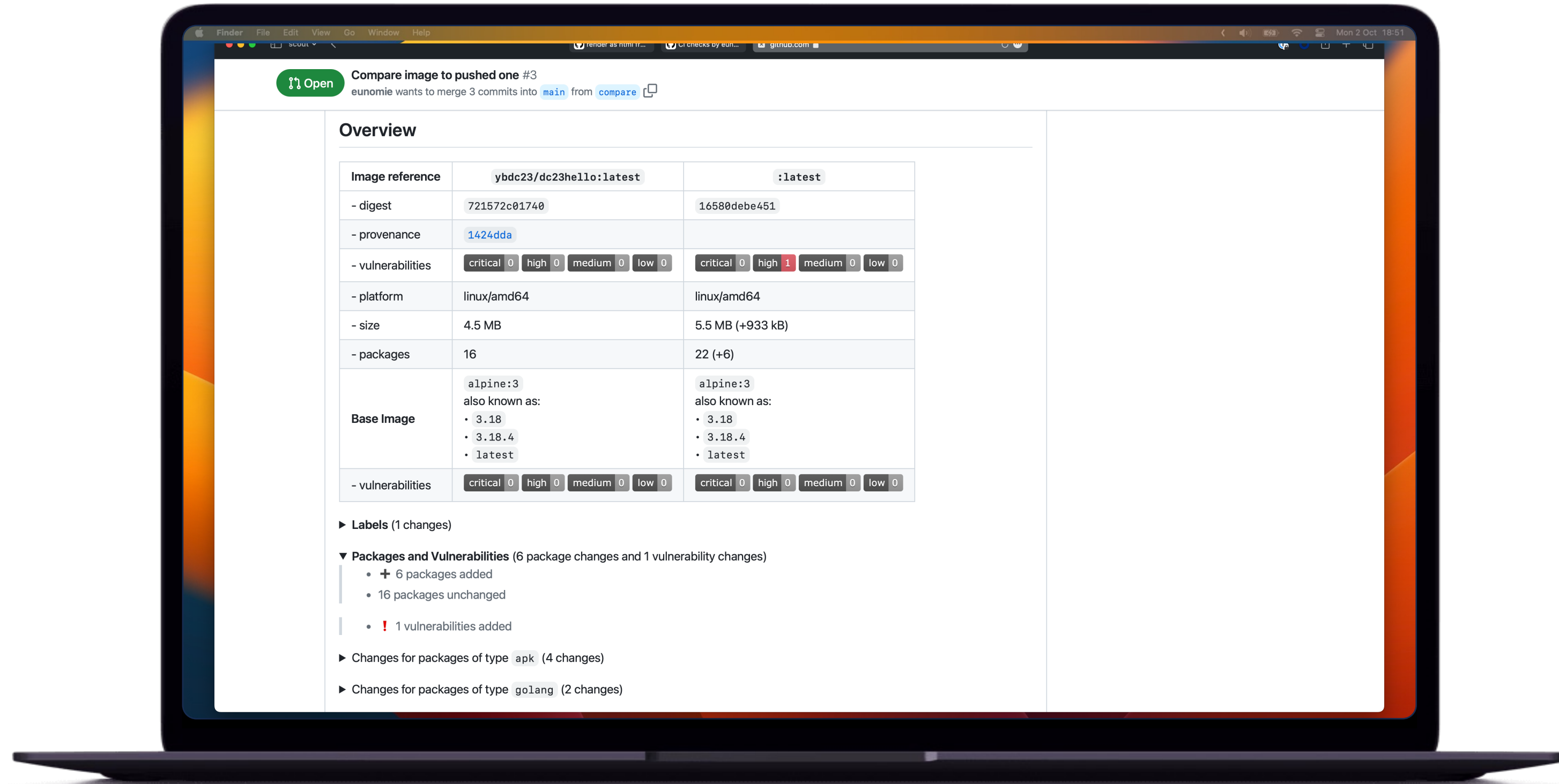
```

## Environment Variables
[dc23_scout1:main]

```

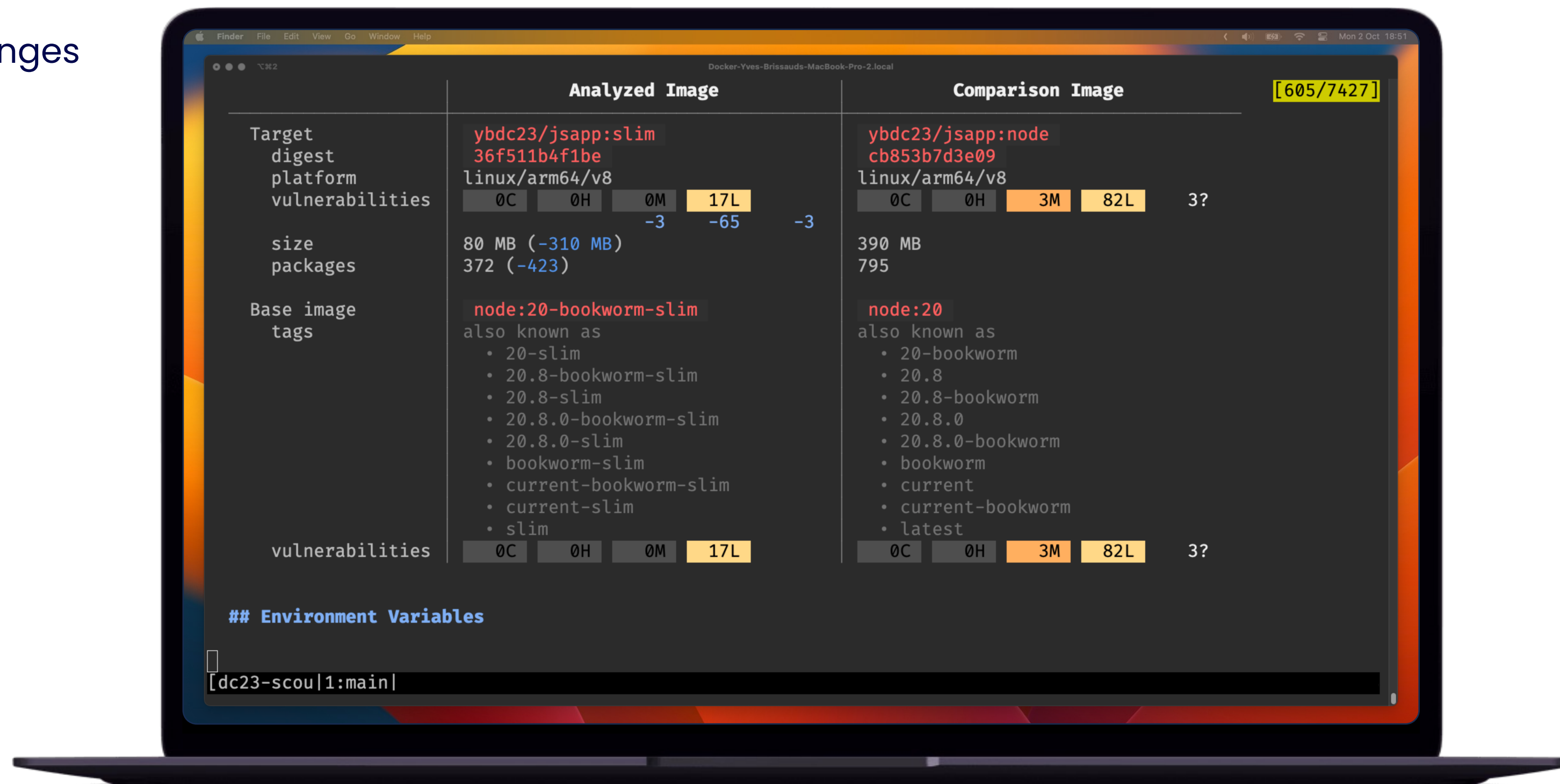
Compare Images

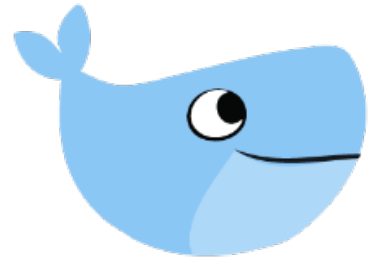
- cli
- GitHub Action



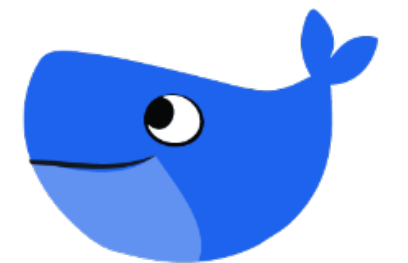
Compare more

- Base image changes





How can I compare to my
staging/production/...
image?



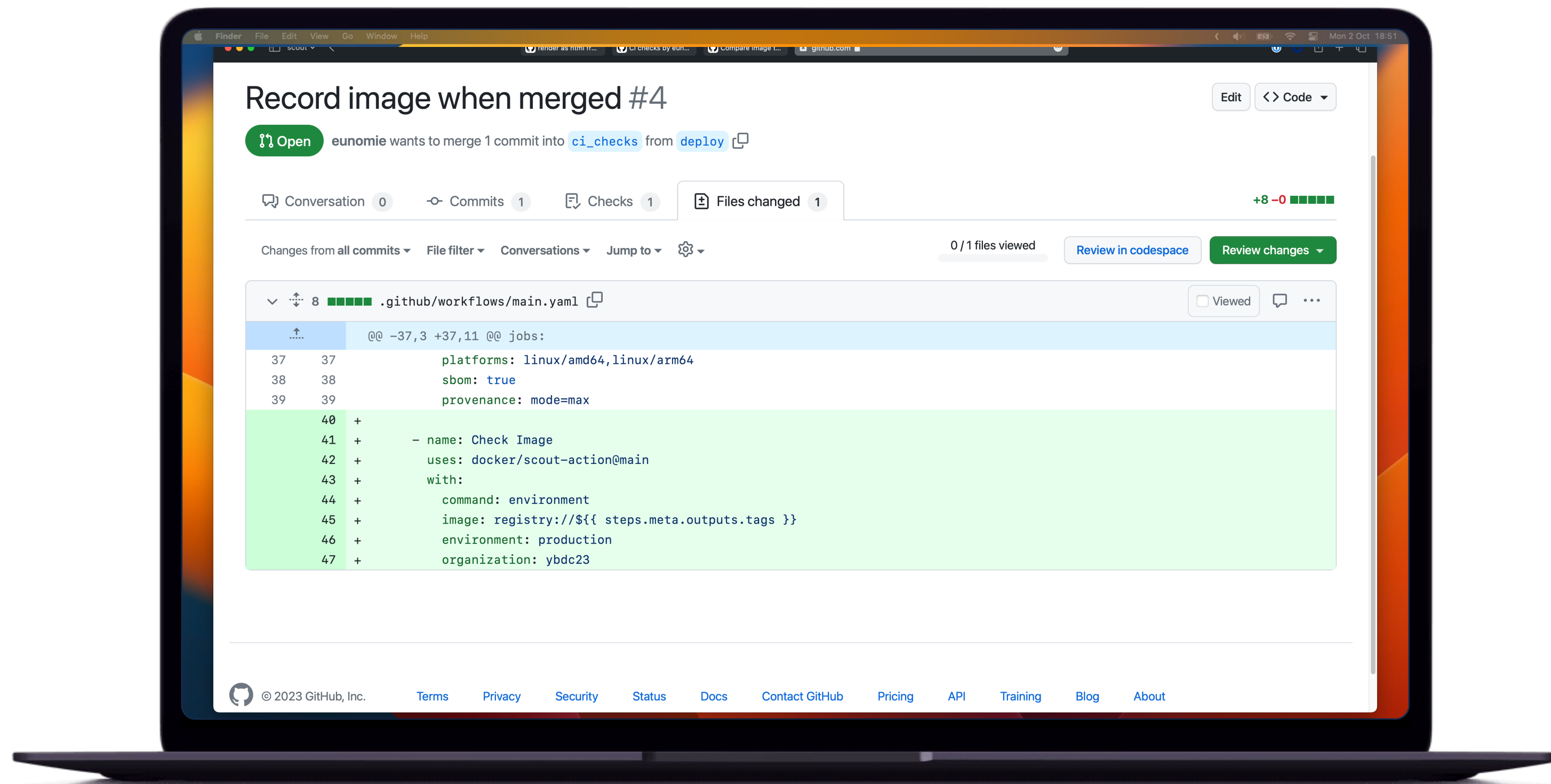
05

Environments



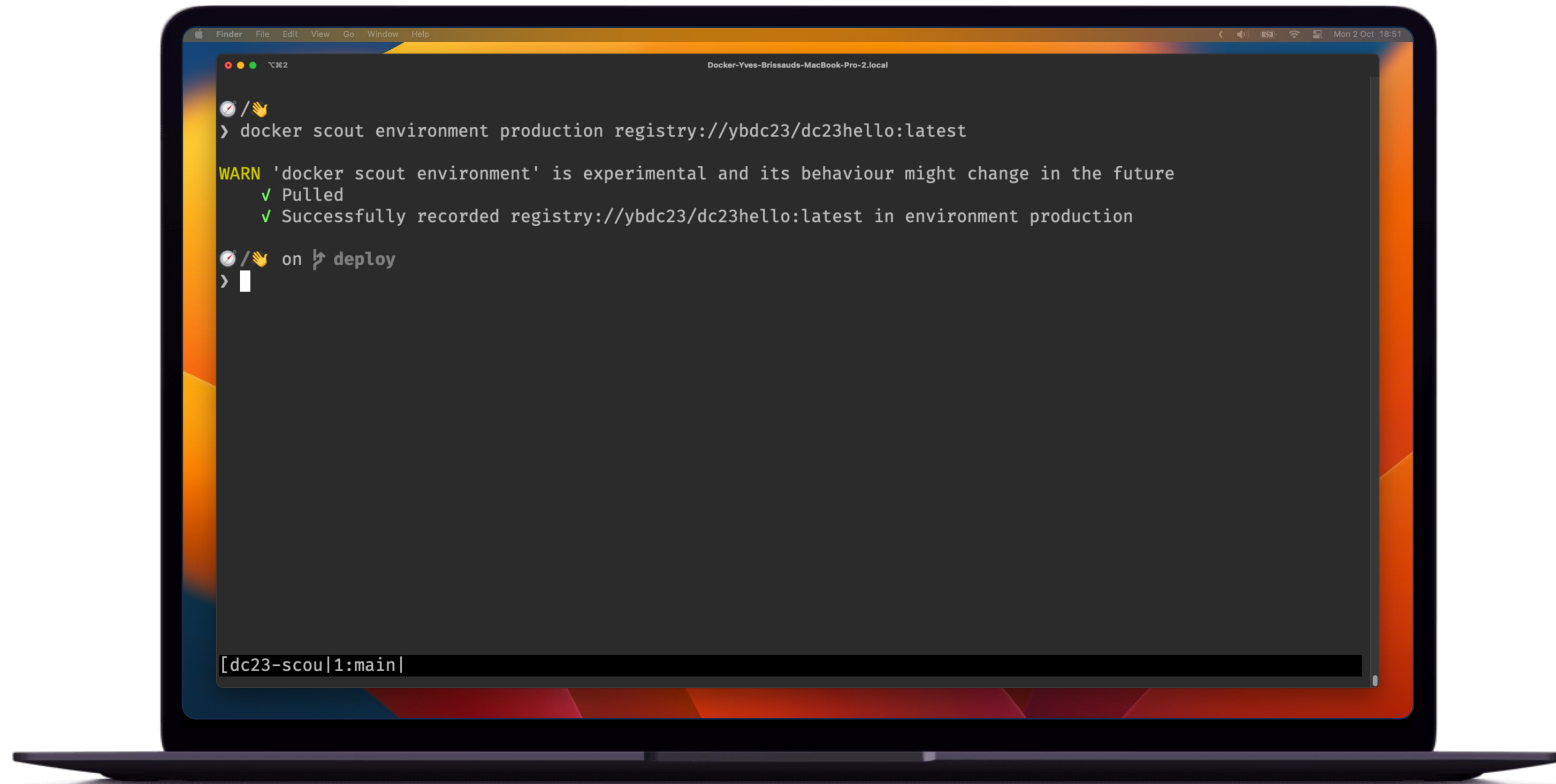
Record Image to an Environment

- GitHub Action

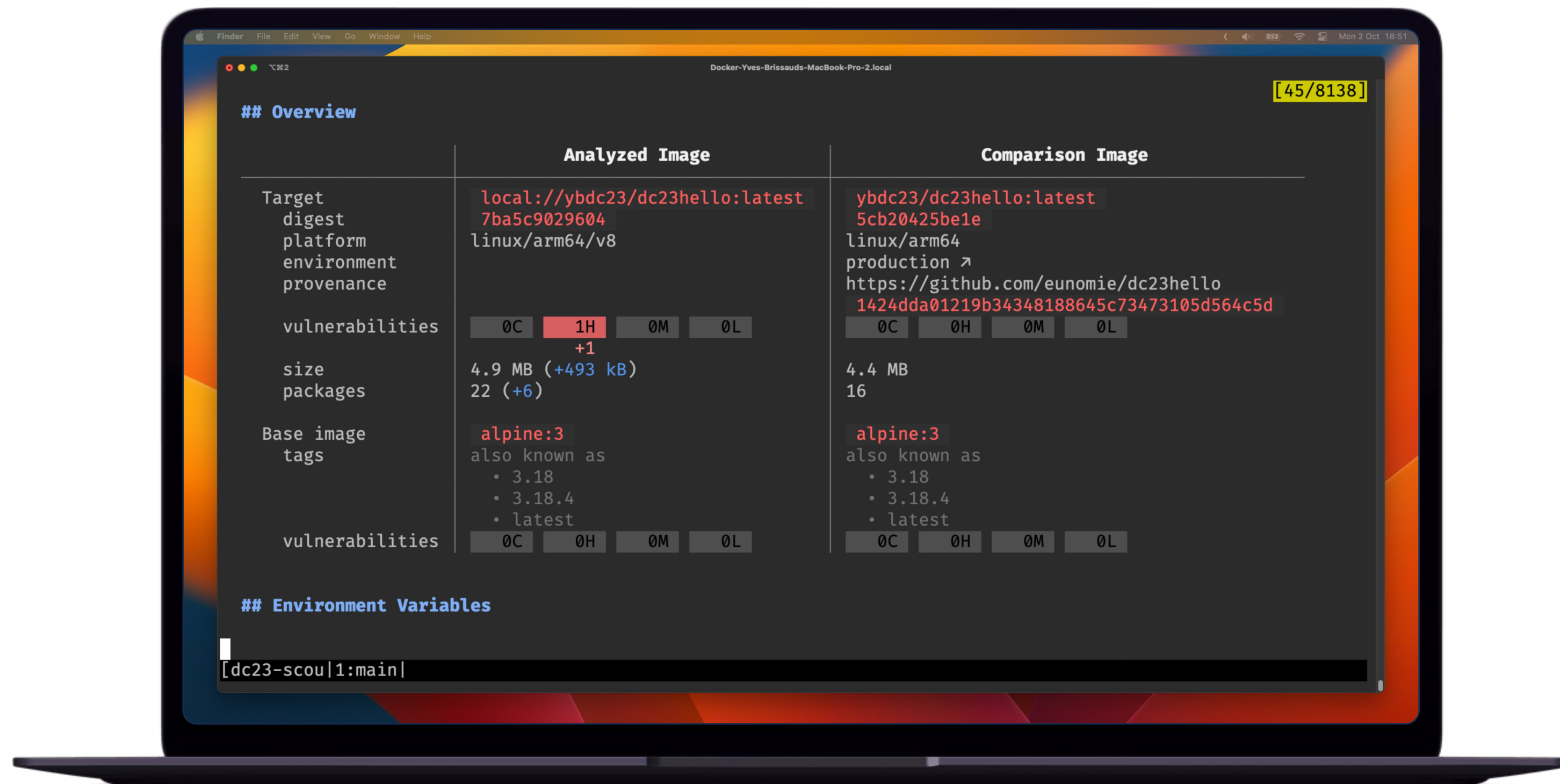


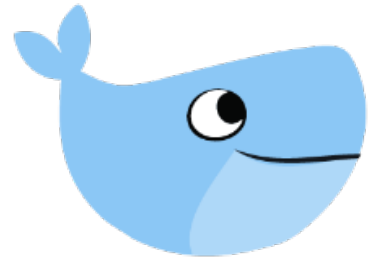
Record Image to an Environment

- GitHub Action
- cli



Compare to an Environment



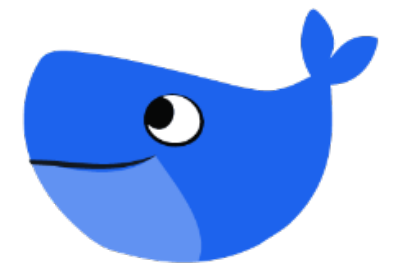


Could it be smarter?

Reduce noise

~~Straight to the decisions~~

Decide for me



06

Policies



Docker Scout CLI

- quickview

```

> docker scout quickview local://ybdc23/dc23hello:latest

✓ SBOM of image already cached, 22 packages indexed
✓ Policy evaluation completed

Target          local://ybdc23/dc23hello:latest  0C  1H  0M  0L
digest          7ba5c9029604
Base image      alpine:3                          0C  0H  0M  0L

Policy status FAILED (2/4 policies met, 1 missing data)

Status | Policy | Results
-----|-----|-----
✓       | All critical vulnerabilities | 0C  0H  0M  0L
?       | Base images not up-to-date  | No data
!       | Critical and high vulnerabilities with fixes | 0C  1H  0M  0L
✓       | Packages with AGPLv3, GPLv3 licenses | 0 packages

on ↵ deploy
> 
[dc23-scou|1:main|
  
```


Docker Scout CLI

- quickview
- policy

```

Finder  File  Edit  View  Go  Window  Help
Docker-Yves-Brissauds-MacBook-Pro-2.local

## Policies
Policy status FAILED (2/4 policies met, 1 missing data)



| Status | Policy                                       | Results     |
|--------|----------------------------------------------|-------------|
| ✓      | All critical vulnerabilities                 | 0C 0H 0M 0L |
| ?      | Base images not up-to-date                   | No data     |
| !      | Critical and high vulnerabilities with fixes | 0C 1H 0M 0L |
| ✓      | Packages with AGPLv3, GPLv3 licenses         | 0 packages  |



## "Critical and high vulnerabilities with fixes" policy evaluation results
Packages shouldn't contain any known vulnerabilities of critical/high severity that are fixable.



| Vulnerability                     | Severity | Current package version                                                     |
|-----------------------------------|----------|-----------------------------------------------------------------------------|
| Fix version                       |          |                                                                             |
| CVE-2023-42821                    | HIGH     | pkg:golang/github.com/gomarkdown/markdown@0.0.0-20230313173142-2ced44d5b584 |
| 0.0.0-20230922105210-14b16010c2ee |          |                                                                             |



🚨/👋 on ⚡ deploy
> 
[dc23-scou|1:main|

```


Docker Scout CLI

- quickview
- policy
- compare

```

Finder  File  Edit  View  Go  Window  Help
Docker-Yves-Brissauds-MacBook-Pro-2.local
- org.opencontainers.image.url=https://github.com/euonomie/dc23hello [20/9171]
- org.opencontainers.image.version=latest

## Policies

0 improved, 1 worsened, 1 missing data

Policy Analyzed Comparison Change
All critical vulnerabilities ✓ ✓
Base images not up-to-date No data ✓
Critical and high vulnerabilities with fixes 1 ✓ +1 Worsened
Packages with AGPLv3, GPLv3 licenses ✓ ✓

View policy details → docker scout policy ybdc23/dc23hello:latest

## Packages and Vulnerabilities

+ 6 packages added
  16 packages unchanged

[dc23-scou|1:main|

```

Docker Scout CLI

- quickview
- policy
- compare

Is my image
better or worse?

```

Finder  File  Edit  View  Go  Window  Help
Docker-Yves-Brissauds-MacBook-Pro-2.local
- org.opencontainers.image.url=https://github.com/euonomie/dc23hello [20/9171]
- org.opencontainers.image.version=latest

## Policies

0 improved, 1 worsened, 1 missing data

Policy Analyzed Comparison Change
All critical vulnerabilities ✓ ✓
Base images not up-to-date No data ✓
Critical and high vulnerabilities with fixes 1 ✓ +1 Worsened
Packages with AGPLv3, GPLv3 licenses ✓ ✓

View policy details → docker scout policy ybdc23/dc23hello:latest

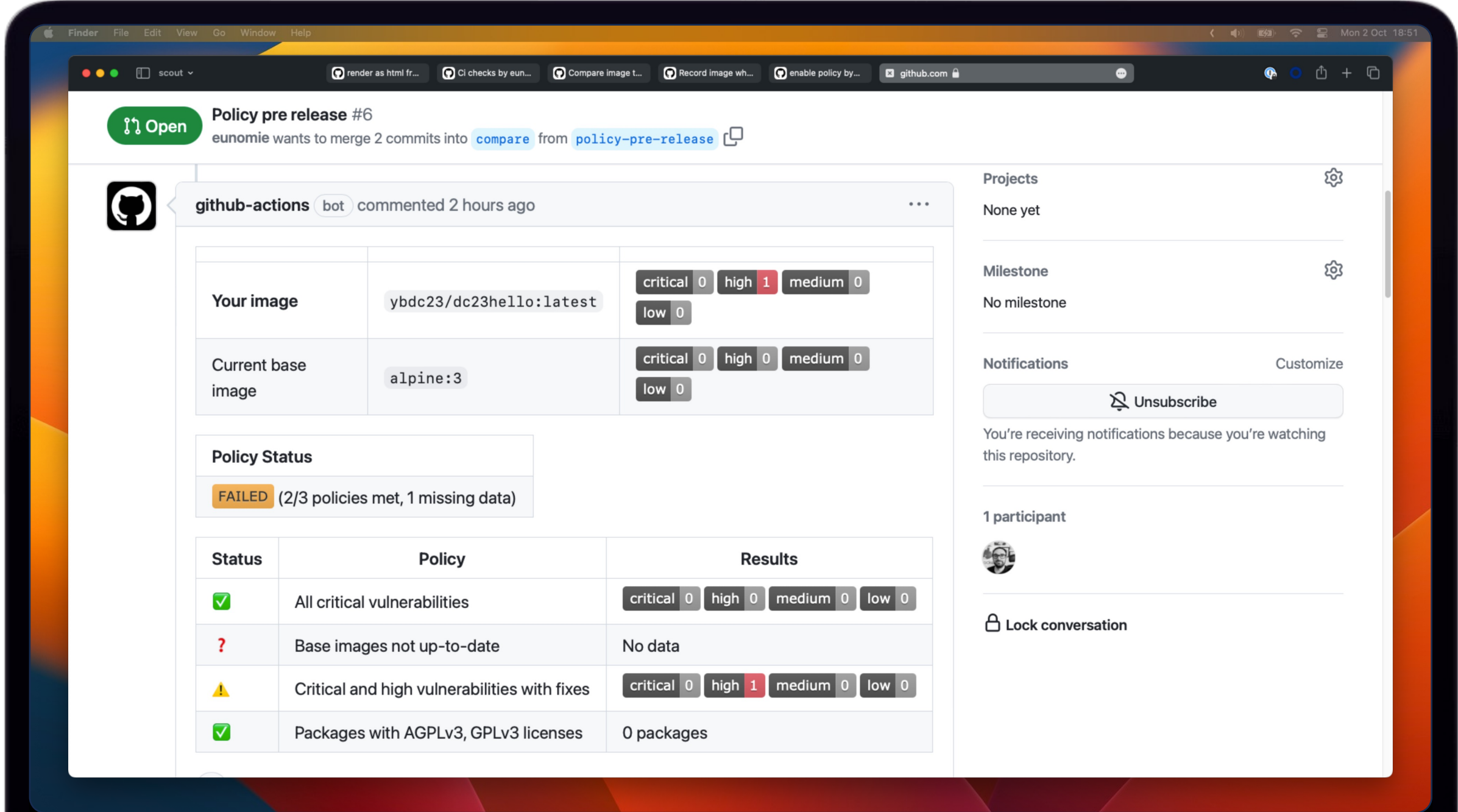
## Packages and Vulnerabilities

+ 6 packages added
  16 packages unchanged

[dc23-scou|1:main|

```

Docker Scout GitHub Action



The screenshot shows a GitHub pull request comment from the `github-actions` bot. The comment displays the results of a Docker Scout policy check for the image `ybdc23/dc23hello:latest` against the base image `alpine:3`. The overall policy status is **FAILED** because 2 out of 3 policies were met, with 1 missing data point.

Image	critical	high	medium	low
Your image: <code>ybdc23/dc23hello:latest</code>	0	1	0	0
Current base image: <code>alpine:3</code>	0	0	0	0

Policy Status
FAILED (2/3 policies met, 1 missing data)

Status	Policy	Results
✓	All critical vulnerabilities	critical 0 high 0 medium 0 low 0
?	Base images not up-to-date	No data
⚠	Critical and high vulnerabilities with fixes	critical 0 high 1 medium 0 low 0
✓	Packages with AGPLv3, GPLv3 licenses	0 packages

The right sidebar of the GitHub interface shows repository settings: Projects (None yet), Milestone (No milestone), Notifications (Unsubscribe), and 1 participant.

07

Summary



Docker Scout CLI

Quick overview of an image

List of all vulnerabilities of an image
with details

Compare two images

Record image to environment

Compare image to environment

Details about policies

Local only images

Registry only images

Local then registry if not found

Local file system

```
docker scout quickview IMAGE
```

```
docker scout cves IMAGE
```

```
docker scout cves --details IMAGE
```

```
docker scout compare IMAGE --to IMAGE
```

```
docker scout environment ENV IMAGE
```

```
docker scout compare IMAGE --to-env ENV
```

```
docker scout policy IMAGE
```

```
local://
```

```
registry://
```

```
image://
```

```
fs://
```



Docker Scout GitHub Action

Quick overview of an image

List of all vulnerabilities of an image

Compare two images

uses: docker/scout-action@main

with:

command: **quickview**

command: **cves**

command: **compare**



Resources

<https://docs.docker.com/scout/>

<https://docs.docker.com/engine/reference/commandline/scout/>

<https://github.com/docker/scout-cli>

<https://github.com/docker/scout-action>

 dockercon.23

THANK YOU



dockercon. 23