

Going secure on GitHub

at ironPeak services



1. \$ whoami



Niels Hofmans

role Independent Cybersecurity Consultant

work Code, App & System Security

interest Go, Docker, Cloud, Media

contact hello@ironpeak.be

github github.com/hazcod

* not affiliated with GitHub

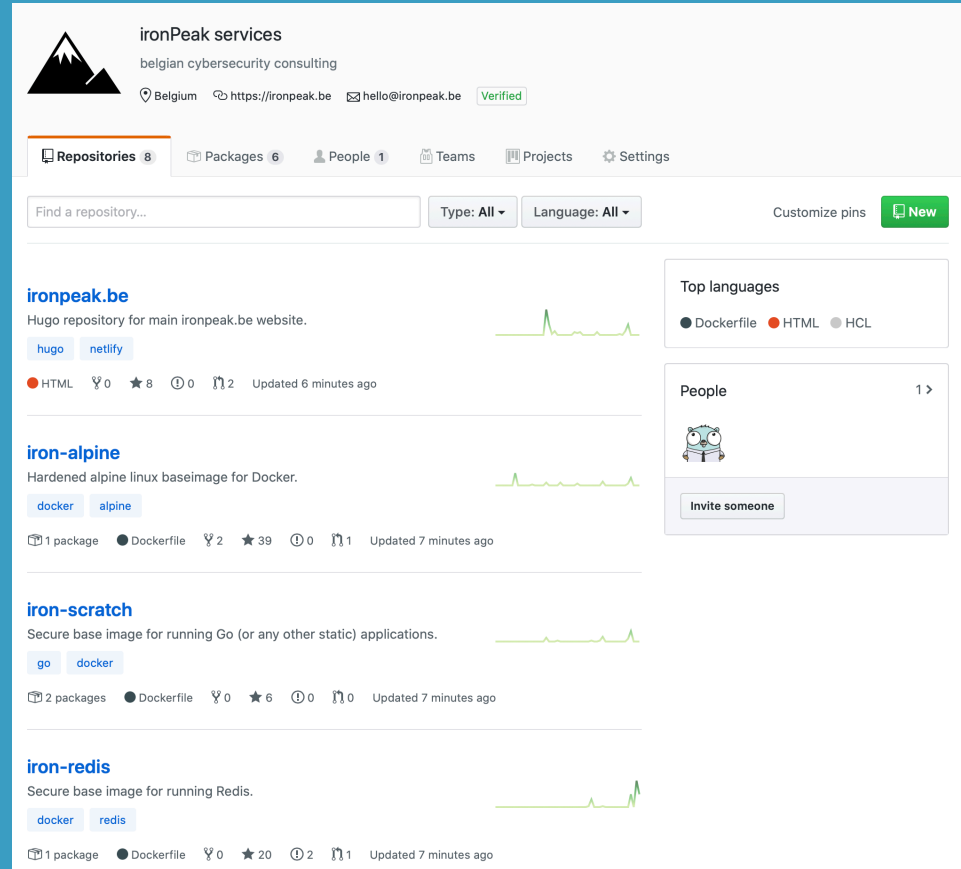
2. \$ why go

- Simple
- Statically typed
- Modern
- Performant
- Batteries included

4. \$ dev requirements

Cybersecurity Startup

- Open Source
- Repository
 - GitHub Enterprise (\$9/user)
 - Private repositories
 - Package registry
 - Github Action CI/CD
 - SSO with google suite
- Infrastructure
 - IaaS
 - Container microservices
 - zero trust



The screenshot shows the GitHub profile of 'ironPeak services', a Belgian cybersecurity consulting firm. The profile includes a verified badge and links to their website, GitHub, and contact information. The main section displays a list of repositories:

- ironpeak.be**: Hugo repository for main ironpeak.be website. Languages: hugo, netlify. 8 stars, 0 forks, 0 issues, 2 pull requests. Updated 6 minutes ago.
- iron-alpine**: Hardened alpine linux baseimage for Docker. Languages: docker, alpine. 1 package, 0 Dockerfiles, 2 stars, 39 forks, 0 issues, 1 pull request. Updated 7 minutes ago.
- iron-scratch**: Secure base image for running Go (or any other static) applications. Languages: go, docker. 2 packages, 0 Dockerfiles, 6 stars, 0 forks, 0 issues, 0 pull requests. Updated 7 minutes ago.
- iron-redis**: Secure base image for running Redis. Languages: docker, redis. 1 package, 0 Dockerfiles, 20 stars, 2 forks, 1 issue, 1 pull request. Updated 7 minutes ago.

On the right side, there are sections for 'Top languages' (Dockerfile, HTML, HCL) and 'People' (1 person, with an 'Invite someone' button).

5. \$ repo

Org Config

- Require 2FA + SSO
- Groups authz
- Local actions + github.com/wei/pull

Repo config

- Protect master branch: PR, Status
- One-way Secrets

App Integrations

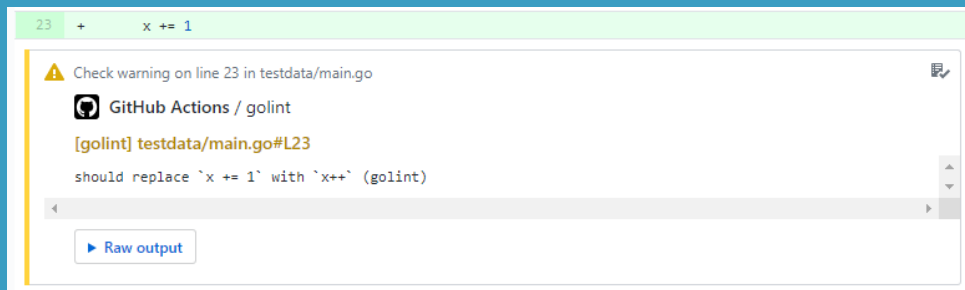
- dependabot (free)
- whitesource bolt (free)



5. \$ repo


Action configuration

- github.com/9sako6/imgcmp
 - .dependabot/
 - .github/workflows/
pr.yaml
 - github.com/9sako6/imgcmp
 - linting (reviewdog golang, docker, ...)
 - build (golang, docker, ...)
 - testing (golang, docker, ...)
 - vulnerability scan (docker)
- deploy.yaml
- create github release
 - publish package (docker)



23 + x += 1

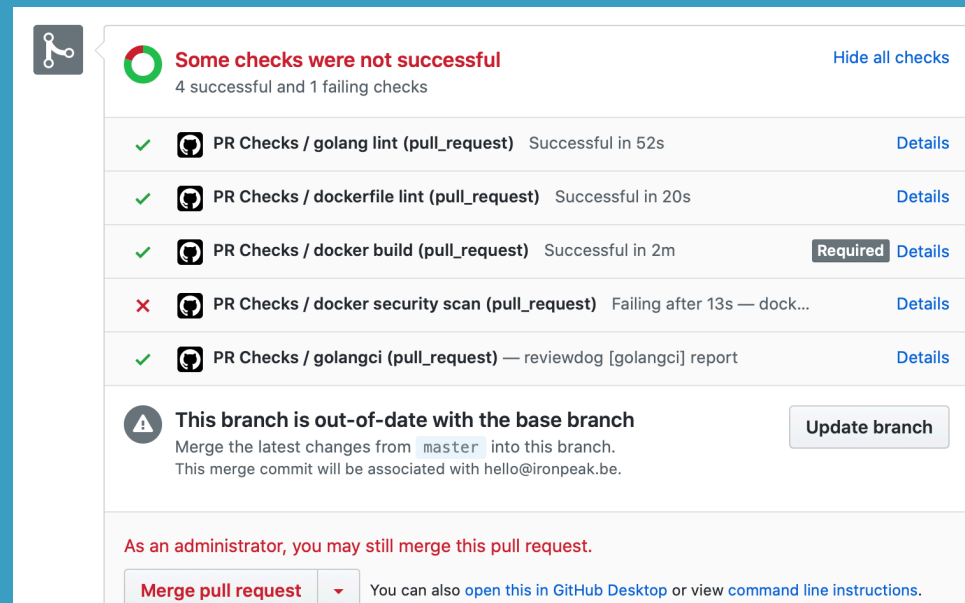
⚠ Check warning on line 23 in testdata/main.go



 GitHub Actions / golint

[golint] testdata/main.go#L23






should replace `x += 1` with `x++` (golint)


[Raw output](#)



  **Some checks were not successful** [Hide all checks](#)


4 successful and 1 failing checks

✓	 PR Checks / golang lint (pull_request)	Successful in 52s	Details
✓	 PR Checks / dockerfile lint (pull_request)	Successful in 20s	Details
✓	 PR Checks / docker build (pull_request)	Successful in 2m	Required Details
✗	 PR Checks / docker security scan (pull_request)	Failing after 13s — dock...	Details
✓	 PR Checks / golangci (pull_request)	— reviewdog [golangci] report	Details

 **This branch is out-of-date with the base branch** [Update branch](#)

Merge the latest changes from `master` into this branch.
This merge commit will be associated with hello@ironpeak.be.

As an administrator, you may still merge this pull request.

[Merge pull request](#)  You can also [open this in GitHub Desktop](#) or view [command line instructions](#).

6. \$ code

- standard library
- go tests & examples -> go doc
- IDE linting (vs code, goland)
- hazcod/gherror: send errors to github
- scratch containers
- healthcheck probes
- oauth2/oidc(pkce)
- api gateway
- paseto
- grpc/flatbuffers
- uber/cadence

```
$ go test -v
=== RUN TestReverse
--- PASS: TestReverse (0.00s)
=== RUN: ExampleReverse
--- PASS: ExampleReverse (0.00s)
PASS
ok      github.com/golang/example/stringutil  0.009s
```

7. \$ what's next

github.com/ironPeakServices

- more iron docker images
- swarm -> kubernetes
- opentracing
- volume clustering
- code fuzzing
- integration testing / TDD

...



7. \$ exit



<https://ironpeak.be/slides/261109-going-secure-on-github.pdf>