@GoWayFest
#GoWayFest

Going Secure With Go

Natalie Pistunovich

@NataliePis

@GoWayFest
#GoWayFest

Going Secure With Go

Natalie Pistunovich

@NataliePis


@NataliePis

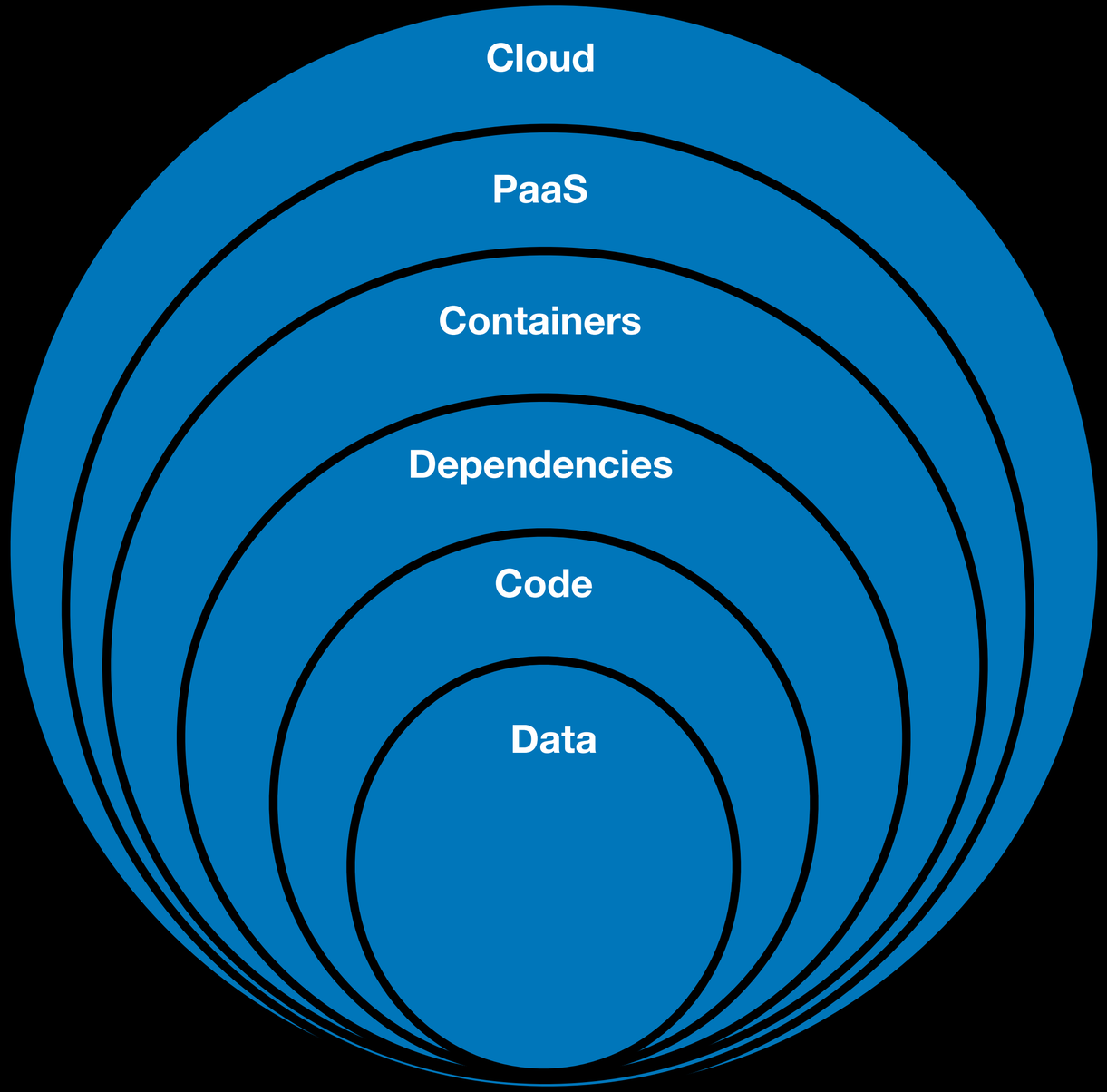

@NataliePis

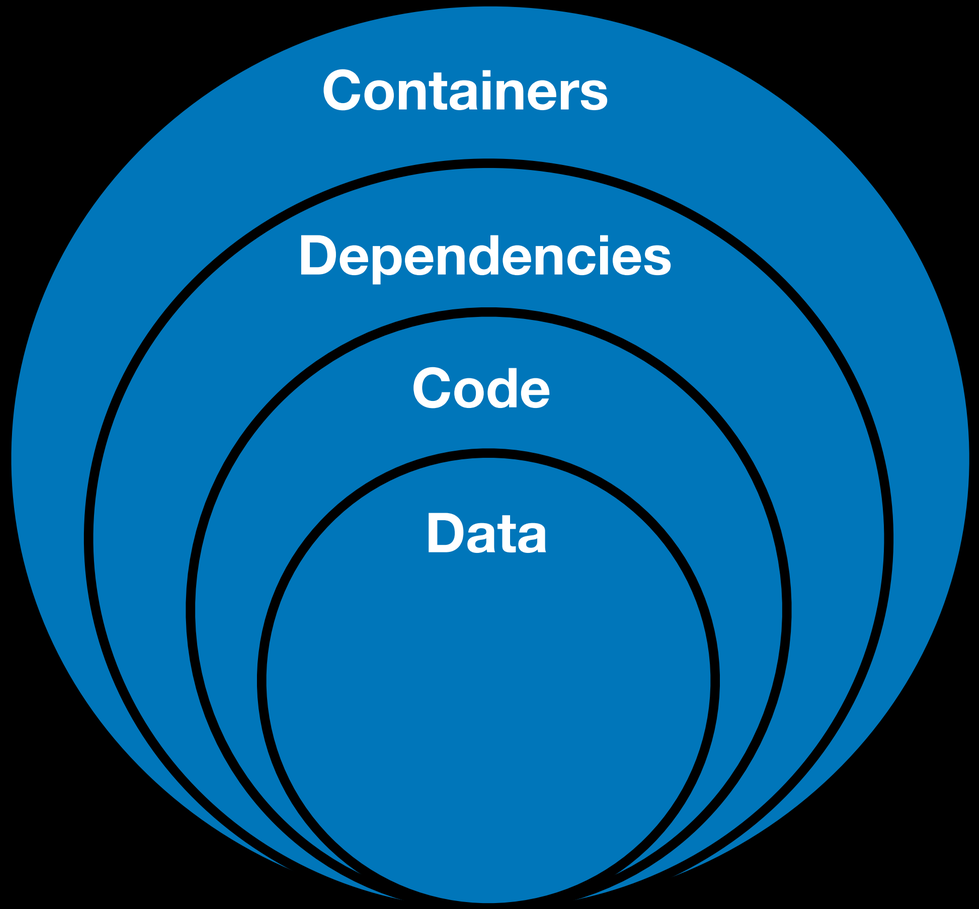

@NataliePis

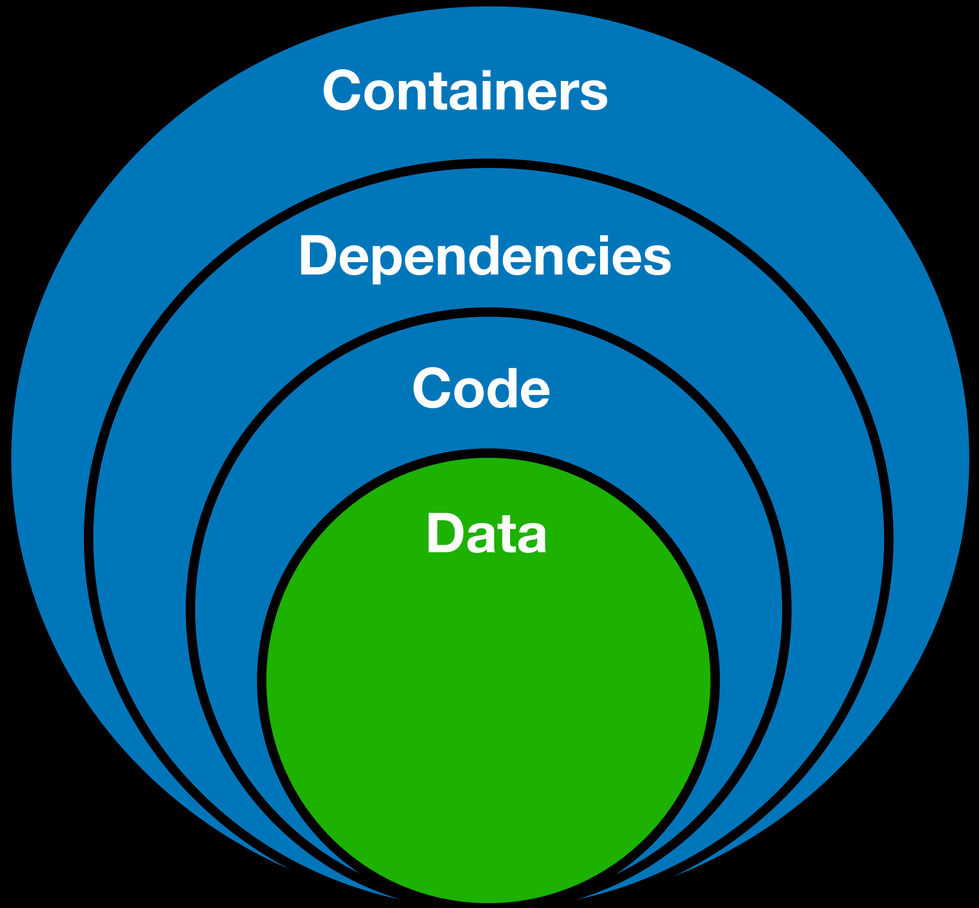
Special Thanks

@webdeva

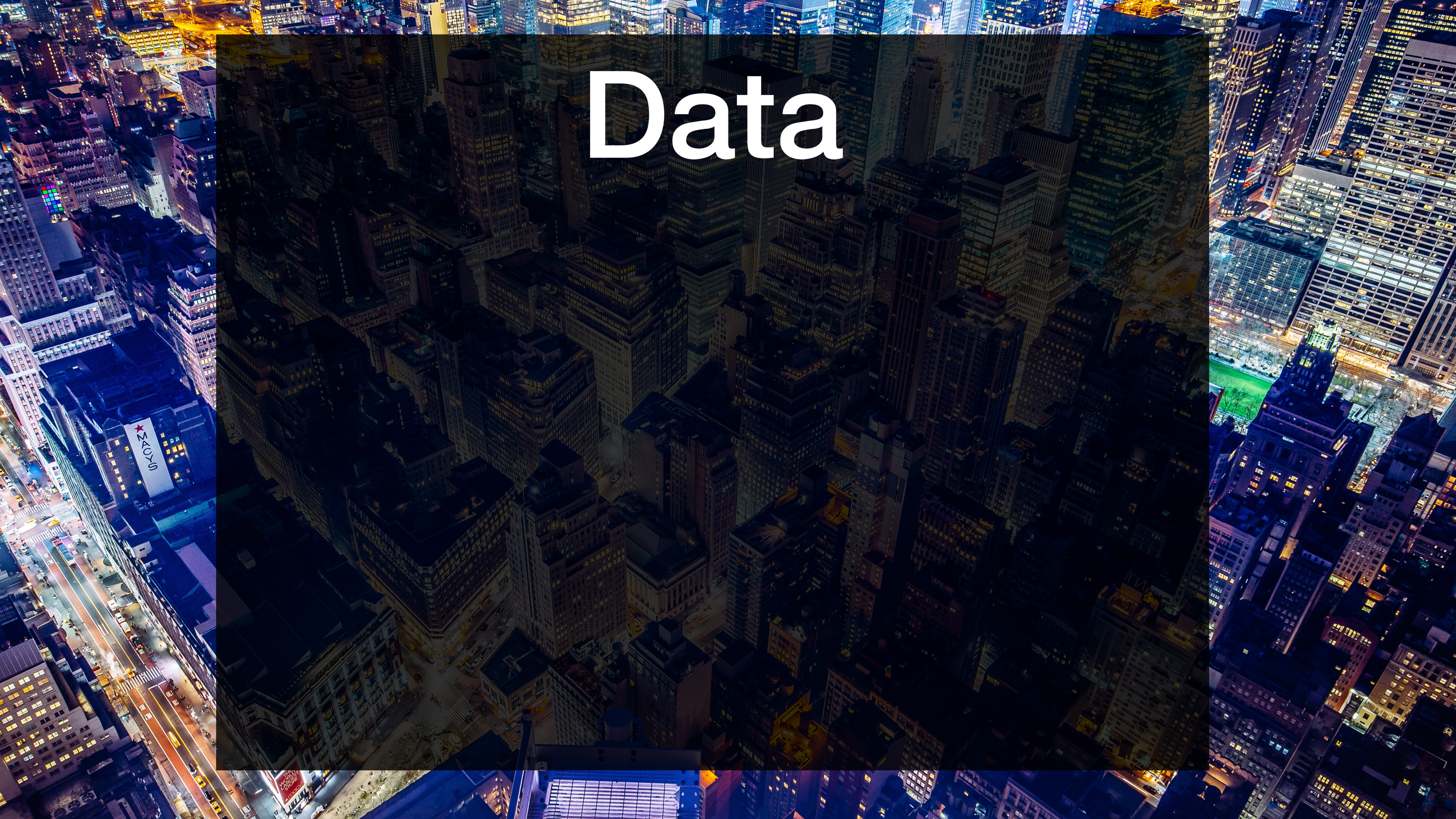
& @jbaruch


Cloud
PaaS
Containers
Dependencies
Code
Data


Containers
Dependencies
Code
Data


Containers
Dependencies
Code
Data

Data



Data

- Passwords

```
-- PostgreSQL

UPDATE credentials
    SET password = crypt('new-password', gen_salt('bf'));
~
~
~
~
~
~
~
~
~
-- INSERT --
```

```
import (
        "fmt"
        "math/rand"
)

func main() {
        rand.Seed(1)

        b := make([]byte, 4)
        _, err := rand.Read(b) // HL
        if err != nil {
                fmt.Println("error: ", err)
                return
        }
        fmt.Println(b)
}
```

~
~

```
➜  Public-Speaking git:(go-security-sg) ✗ go run main.go
[82 253 252 7]
➜  Public-Speaking git:(go-security-sg) ✗ go run main.go
[82 253 252 7]
➜  Public-Speaking git:(go-security-sg) ✗ go run main.go
[82 253 252 7]
➜  Public-Speaking git:(go-security-sg) ✗ go run main.go
[82 253 252 7]
➜  Public-Speaking git:(go-security-sg) ✗
```

```
import (
        "fmt"
        "math/rand"
)

func main() {
        rand.Seed(1)

        b := make([]byte, 4)
        _, err := rand.Read(b) // HL
        if err != nil {
                fmt.Println("error: ", err)
                return
        }
        fmt.Println(b)
}
```

~
~

```
import (
        "fmt"
        "math/rand"
        "time"
)

func main() {
        rand.Seed(time.Now().Unix())

        b := make([]byte, 4)
        _, err := rand.Read(b) // HL
        if err != nil {
                fmt.Println("error: ", err)
                return
        }
        fmt.Println(b)
}
```

~

```
➜  Public-Speaking git:(go-security-sg) ✗ go run main.go
[17 40 42 48]
➜  Public-Speaking git:(go-security-sg) ✗ go run main.go
[231 108 255 28]
➜  Public-Speaking git:(go-security-sg) ✗ go run main.go
[34 43 154 67]
➜  Public-Speaking git:(go-security-sg) ✗ go run main.go
[34 43 154 67]
➜  Public-Speaking git:(go-security-sg) ✗ go run main.go
[24 179 223 232]
➜  Public-Speaking git:(go-security-sg) ✗ go run main.go
^[[A[118 116 85 178]
➜  Public-Speaking git:(go-security-sg) ✗ go run main.go
^[[A[118 116 85 178]
➜  Public-Speaking git:(go-security-sg) ✗ go run main.go
^[[A[203 33 91 251]
➜  Public-Speaking git:(go-security-sg) ✗ go run main.go
[203 33 91 251]
➜  Public-Speaking git:(go-security-sg) ✗ go run main.go
[203 33 91 251]
➜  Public-Speaking git:(go-security-sg) ✗ go run main.go
[169 166 192 123]
➜  Public-Speaking git:(go-security-sg) ✗
```

```
import (
        "fmt"
        "crypto/rand"
)

func main() {
        rand.Seed(1)

        b := make([]byte, 4)
        _, err := rand.Read(b) // HL
        if err != nil {
                fmt.Println("error: ", err)
                return
        }
        fmt.Println(b)
}
```
~

```
➜ Public-Speaking git:(go-security-sg) ✗ go run main.go
[110 9 104 30]
➜ Public-Speaking git:(go-security-sg) ✗ go run main.go
[248 125 59 179]
➜ Public-Speaking git:(go-security-sg) ✗ go run main.go
[156 66 239 128]
➜ Public-Speaking git:(go-security-sg) ✗ go run main.go
[178 251 100 64]
➜ Public-Speaking git:(go-security-sg) ✗ go run main.go
[172 34 104 225]
➜ Public-Speaking git:(go-security-sg) ✗ go run main.go
[65 34 225 230]
➜ Public-Speaking git:(go-security-sg) ✗ go run main.go
[208 170 189 227]
➜ Public-Speaking git:(go-security-sg) ✗ go run main.go
[85 150 168 43]
➜ Public-Speaking git:(go-security-sg) ✗ go run main.go
[2 44 57 70]
➜ Public-Speaking git:(go-security-sg) ✗ go run main.go
[96 156 9 13]
➜ Public-Speaking git:(go-security-sg) ✗ go run main.go
[10 31 115 37]
➜ Public-Speaking git:(go-security-sg) ✗ go run main.go
[154 78 9 170]
```

```
import (
        "fmt"
        "crypto/rand"
)

func main() {
        rand.Seed(1)

        b := make([]byte, 4)
        _, err := rand.Read(b) // HL
        if err != nil {
                fmt.Println("error: ", err)
                return
        }
        fmt.Println(b)
}
```
~

Data

- Passwords
- User Personal Data

Mask Rules

Last updated: Feb 18, 2019

A mask rule is a type of processing rule that hides irrelevant or sensitive information from logs before ingestion. When you create a mask rule, whatever expression you choose to mask will be replaced with a mask string before it is sent to Sumo Logic. You can provide a mask string, or use the default, "#."

Ingestion volume is calculated after applying the mask filter. If the mask reduces the size of the log, the smaller size will be measured against ingestion limits. Masking is a good method for reducing overall ingestion volume.

The mask string does not support the use of colon : characters.

For example, to mask the email address `dan@demo.com` from this log:

```
2018-05-16 09:43:39,607 -0700 DEBUG [hostId=prod-cass-raw-8]
[module=RAW] [logger=scala.raw.InboundRawProtocolHandler] [auth=User:dan@demo.com] [remote_ip=98.248
[web_session=19zefhqy...] [session=80F1BD83AEBDF4FB] [customer=0000000000000005] [call=InboundRawPro
```

You could use the following filter expression:

```
auth=User\:(.*\.com)\]\s
```

With a mask string of `AAA` would provide the following result:

Mask Rules

Last updated: Feb 18, 2019

A mask rule is a type of processing rule that hides irrelevant or sensitive information from logs before ingestion. When you create a mask rule, whatever expression you choose to mask will be replaced with a mask string before it is sent to Sumo Logic. You can provide a mask string, or use the default, "#."

Ingestion volume is calculated after applying the mask filter. If the mask reduces the size of the log, the smaller size will be measured against ingestion limits. Masking is a good method for reducing overall ingestion volume.

The mask string does not support the use of colon : characters.

For example, to mask the email address `dan@demo.com` from this log:

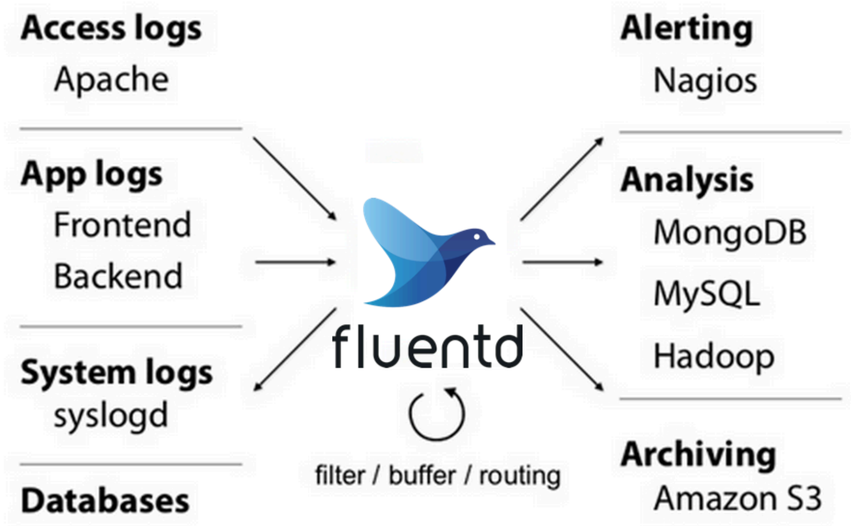
```
2018-05-16 09:43:39,607 -0700 DEBUG [hostId=prod-cass-raw-8]
[module=RAW] [logger=scala.raw.InboundRawProtocolHandler] [auth=User:dan@demo.com] [remote_ip=98.248
[web_session=19zefhqy...] [session=80F1BD83AEBDF4FB] [customer=0000000000000005] [call=InboundRawPro
```

You could use the following filter expression:

```
auth=User\:(.*\.com)\]\s
```

With a mask string of `AAA` would provide the following result:

splunk>



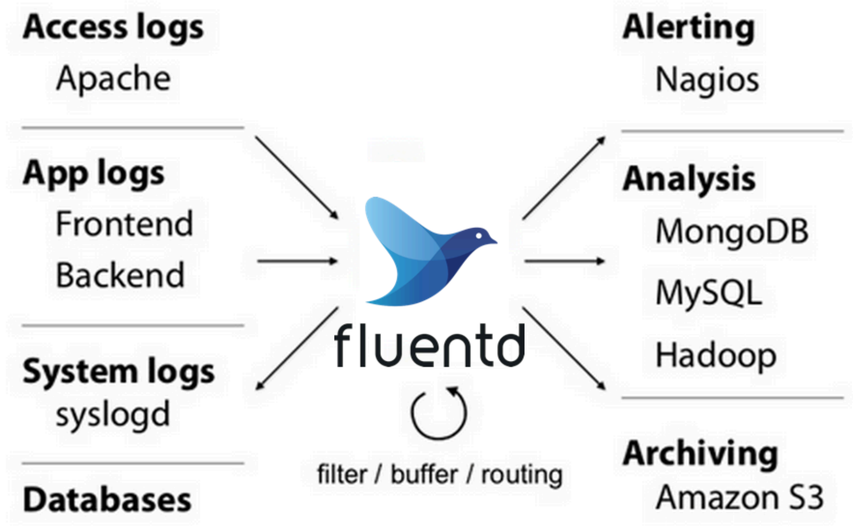
For example, to mask the email address `dan@demo.com` from this log:

```
2018-05-16 09:43:39,607 -0700 DEBUG [hostId=prod-cass-raw-8]
[module=RAW] [logger=scala.raw.InboundRawProtocolHandler] [auth=User:dan@demo.com] [remote_ip=98.248
[web_session=19zefhqy...] [session=80F1BD83AEBDF4FB] [customer=0000000000000005] [call=InboundRawPro
```

You could use the following filter expression:

```
auth=User\:(.*\.com)\]\s
```

With a mask string of `AAA` would provide the following result:



For example, to mask the email address `dan@demo.com` from this log:

```
2018-05-16 09:43:39,607 -0700 DEBUG [hostId=prod-cass-raw-8]
[module=RAW] [logger=scala.raw.InboundRawProtocolHandler] [auth=User:dan@demo.com] [remote_ip=98.248
[web_session=19zefhqy...] [session=80F1BD83AEBDF4FB] [customer=0000000000000005] [call=InboundRawPro
```

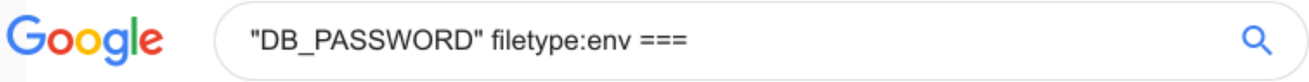
You could use the following filter expression:

```
auth=User\:(.*\.com)\]\s
```

With a mask string of `AAA` would provide the following result:

Data

- Passwords
- User Personal Data
- Secrets Management



All Maps Shopping News Videos More Settings Tools

About 1,990 results (0.37 seconds)

APP_NAME=Laravel APP_ENV=local APP_KEY=base64 ...
www.safeairtravels.com/.env
... DB_CONNECTION=mysql DB_HOST=127.0.0.1 DB_PORT=3306 DB_DATABASE=safeairt_db DB_USERNAME=safeairt_user **DB_PASSWORD**=pass1234!

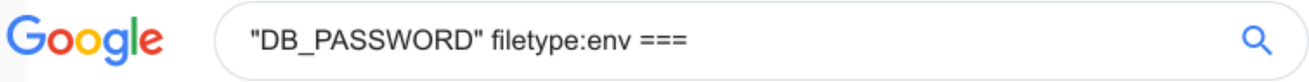
APP_ENV=local APP_DEBUG=true APP_KEY ...
idcc.com.my/.env
... DB_DATABASE=shlim999_idcc2 DB_USERNAME=shlim999_idcc2 **DB_PASSWORD**=abc120303 CACHE_DRIVER=file SESSION_DRIVER=file.

env - Onix Jr.
onixjr.com/portal/.env
HpCgWAn$_/HvcCf|^+`VCXx[pzr8z1xAU3s' DB_HOST='localhost' DB_NAME='onixj015_portal' **DB_PASSWORD**='p742S1d[T]' DB_USER='onixj015_wp344' ...

env - Professorvirtual.org
https://professorvirtual.org/educadataorg/.env
... DB_DATABASE=apren814_laravel DB_USERNAME=apren814 **DB_PASSWORD**=mY0tV8g9u0 BROADCAST_DRIVER=log CACHE_DRIVER=file ...

APP_ENV=local APP_DEBUG=true APP_KEY=base64 ...
www.oaksnorthaddison.com/.env
... DB_HOST=127.0.0.1 DB_PORT=3306 DB_DATABASE=yijsbcug_oaksnorth_designpro DB_USERNAME=yijsbcug_oaksU **DB_PASSWORD**=^2}Bq8f]_4.

APP_ENV=local APP_DEBUG=false APP_KEY=base64 ...
https://ihusigroup.com/hotels/.env
... DB_DATABASE=ihusigro_hotel DB_USERNAME=ihusigro_hotel **DB_PASSWORD**=% [U9raGX+GgF CACHE_DRIVER=file SESSION_DRIVER=file ...



All Maps Shopping News Videos More Settings Tools

About 1,990 results (0.37 seconds)

APP_NAME=Laravel APP_ENV=local APP_KEY=base64 ...
www.safeairtravels.com/.env
... DB_CONNECTION=mysql DB_HOST=127.0.0.1 DB_PORT=3306 DB_DATABASE=safeairt_db DB_USERNAME=safeairt_user **DB_PASSWORD**=pass1234!

APP_ENV=local APP_DEBUG=true APP_KEY ...
idcc.com.my/.env
... DB_DATABASE=shlim999_idcc2 DB_USERNAME=shlim999_idcc2 **DB_PASSWORD**=abc120303 CACHE_DRIVER=file SESSION_DRIVER=file.

env - Onix Jr.
onixjr.com/portal/.env
HpCgWAn$_/HvcCf|^+`VCXx[pzr8z1xAU3s' DB_HOST='localhost' DB_NAME='onixj015_portal' **DB_PASSWORD**='p742S1d[T]' DB_USER='onixj015_wp344' ...

env - Professorvirtual.org
https://professorvirtual.org/educadataorg/.env
... DB_DATABASE=apren814_laravel DB_USERNAME=apren814 **DB_PASSWORD**=mY0tV8g9u0 BROADCAST_DRIVER=log CACHE_DRIVER=file ...

APP_ENV=local APP_DEBUG=true APP_KEY=base64 ...
www.oaksnorthaddison.com/.env
... DB_HOST=127.0.0.1 DB_PORT=3306 DB_DATABASE=yijsbcug_oaksnorth_designpro DB_USERNAME=yijsbcug_oaksU **DB_PASSWORD**=^2}Bq8f]_4.

APP_ENV=local APP_DEBUG=false APP_KEY=base64 ...
https://ihusigroup.com/hotels/.env
... DB_DATABASE=ihusigro_hotel DB_USERNAME=ihusigro_hotel **DB_PASSWORD**=% [U9raGX+GgF CACHE_DRIVER=file SESSION_DRIVER=file ...

- Repositories 29
- Code 80K+
- **Commits** 30K+
- Issues 35K
- Packages
- Marketplace
- Topics
- Wikis 2K
- Users

Advanced search Cheat sheet

Showing 28,161 available commit results

Sort: Best match

remove password

Syarif Hidayat authored and Syarif Hidayat committed to syarbeats/spring-jdbc 12 hours ago

`6507ddf`

Removed Passwords

sjcswank committed to sjcswank/stash-web 4 days ago ✓

`58473c5`

remove password

simbo1905 committed to ocd-scm/ocd-tagger 7 days ago

`aca2016`

remove password pattern

mikegikas committed to teamProjectAfdemp/teamProject 6 days ago

`eeda806`

Remove password from deployments

Fredi Bach committed to FrediBach/FakeQL 7 days ago ✓

1

`ac29877`

rtyley.github.io/bfg-repo-cleaner/

Secrets

Kubernetes `secret` objects let you store and manage sensitive information, such as passwords, OAuth tokens, and ssh keys. Putting this information in a `secret` is safer and more flexible than putting it verbatim in a Pod Lifecycle definition or in a container image. See Secrets design document for more information.

Overview of Secrets

A Secret is an object that contains a small amount of sensitive data such as a password, a token, or a key. Such information might otherwise be put in a Pod specification or in an image; putting it in a Secret object allows for more control over how it is used, and reduces the risk of accidental exposure.

Users can create secrets, and the system also creates some secrets.

To use a secret, a pod needs to reference the secret. A secret can be used with a pod in two ways: as files in a volume mounted on one or more of its containers, or used by kubelet when pulling images for the pod.

Secrets

Kubernetes `secret` objects let you store and manage sensitive information, such as passwords, OAuth tokens, and ssh keys. Putting this information in a `secret` is safer and more flexible than putting it verbatim in a Pod Lifecycle definition or in a container image. See Secrets design document for more information.

Overview of Secrets

A Secret is an object that contains a small amount of sensitive data such as a password, a token, or a key. Such information might otherwise be put in a Pod specification or in an image; putting it in a Secret object allows for more control over how it is used, and reduces the risk of accidental exposure.

Users can create secrets, and the system also creates some secrets.

To use a secret, a pod needs to reference the secret. A secret can be used with a pod in two ways: as files in a volume mounted on one or more of its containers, or used by kubelet when pulling images for the pod.

Using Secrets as Environment Variables

To use a secret in an environment variable in a pod:

1. Create a secret or use an existing one. Multiple pods can reference the same secret.
2. Modify your Pod definition in each container that you wish to consume the value of a secret key to add an environment variable for each secret key you wish to consume. The environment variable that consumes the secret key should populate the secret's name and key in `env[].valueFrom.secretKeyRef`.
3. Modify your image and/or command line so that the program looks for values in the specified environment variables

This is an example of a pod that uses secrets from environment variables:

```
apiVersion: v1
kind: Pod
metadata:
  name: secret-env-pod
spec:
  containers:
  - name: mycontainer
    image: redis
    env:
      - name: SECRET_USERNAME
        valueFrom:
          secretKeyRef:
            name: mysecret
            key: username
      - name: SECRET_PASSWORD
        valueFrom:
          secretKeyRef:
            name: mysecret
            key: password
```

Understanding Process Namespace Sharing

Pods share many resources so it makes sense they would also share a process namespace. Some container images may expect to be isolated from other containers, though, so it's important to understand these differences:

1. **The container process no longer has PID 1.** Some container images refuse to start without PID 1 (for example, containers using `systemd`) or run commands like `kill -HUP 1` to signal the container process. In pods with a shared process namespace, `kill -HUP 1` will signal the pod sandbox. (`/pause` in the above example.)
2. **Processes are visible to other containers in the pod.** This includes all information visible in `/proc`, such as passwords that were passed as arguments or environment variables. These are protected only by regular Unix permissions.
3. **Container filesystems are visible to other containers in the pod through the `/proc/$pid/root` link.** This makes debugging easier, but it also means that filesystem secrets are protected only by filesystem permissions.

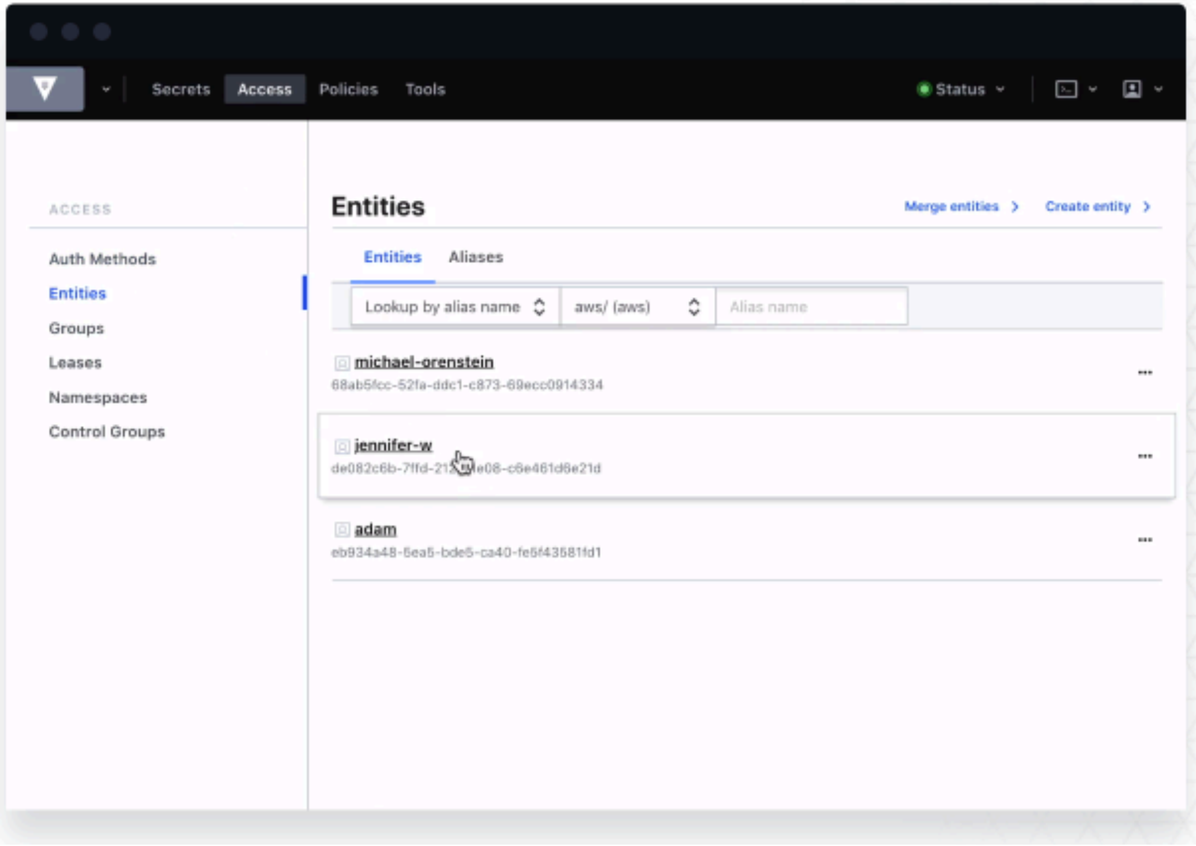
cat /proc/<PID>/environ

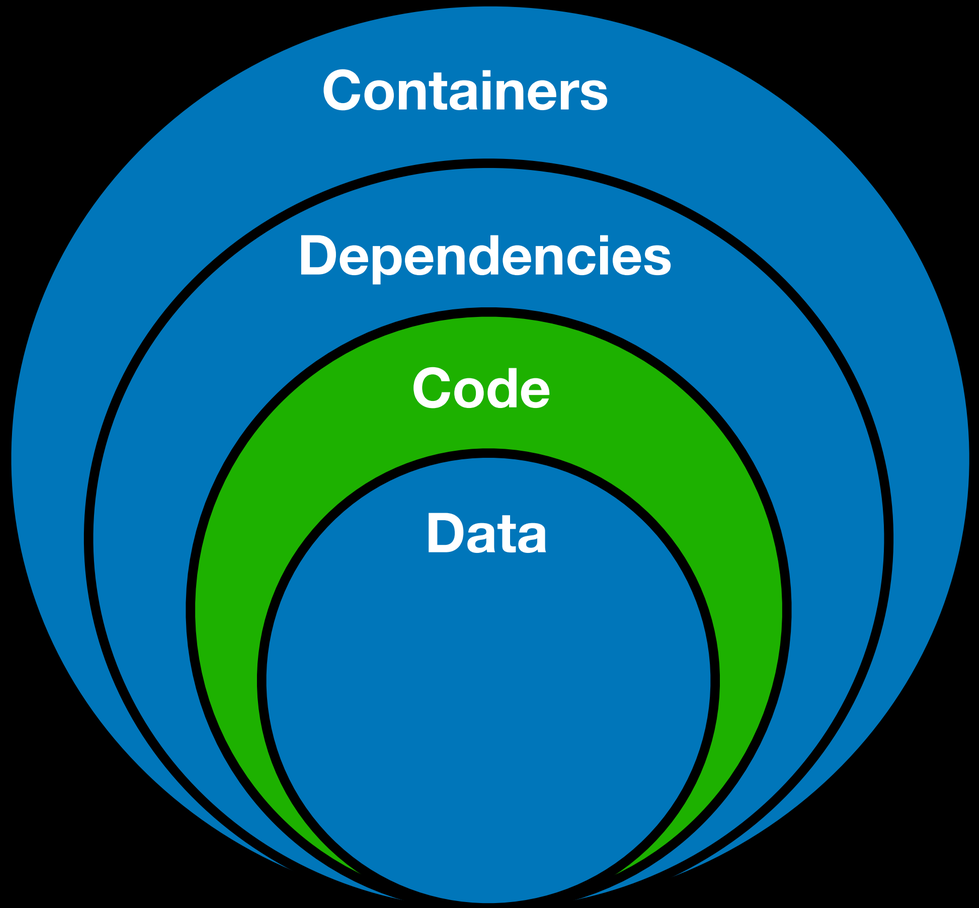
Manage Secrets and Protect Sensitive Data

Secure, store and tightly control access to tokens, passwords, certificates, encryption keys for protecting secrets and other sensitive data using a UI, CLI, or HTTP API.

Download

Get Started with Vault




Containers
Dependencies
Code
Data

Code

- Input Validation

Code

- Input Validation

Code

- Input Validation

Code

- Input Validation
- SQL Injection

```
package injection

import (
    "database/sql"
    "fmt"
)

func findUser(db *sql.DB, name string) {
    query := fmt.Sprintf("SELECT * FROM users WHERE name = '%s'", na
me)
    db.Query(query)
}
```

-- INSERT --

```
package injection

import (
    "database/sql"
    "fmt"
)

func findUser(db *sql.DB, name string) {
    query := fmt.Sprintf("SELECT * FROM users WHERE name = '%s'", na
me)
    db.Query(query)
}
```

-- INSERT --

```
package injection

import (
    "database/sql"
    "fmt"
)

func findUser(db *sql.DB, name string) {
    query := fmt.Sprintf("SELECT * FROM users WHERE name = '%s'", na
me)
    db.Query(query)
}

func findUserSafe(db *sql.DB, name string) {
    query := "SELECT * FROM users WHERE name = $1"
    db.Query(query, name)
}
```

-- INSERT --

```go
package injection

import (
    "database/sql"
    "fmt"
    "strings"
)

func insertUsers(db *sql.DB, names []string) {
    var values []string
    for _, name := range names {
        values = append(values, fmt.Sprintf("('%s')", name))
    }
    query := fmt.Sprintf(
        "INSERT INTO users (name) VALUES %s",
        strings.Join(values, ","),
    )
    db.Query(query)
}
```

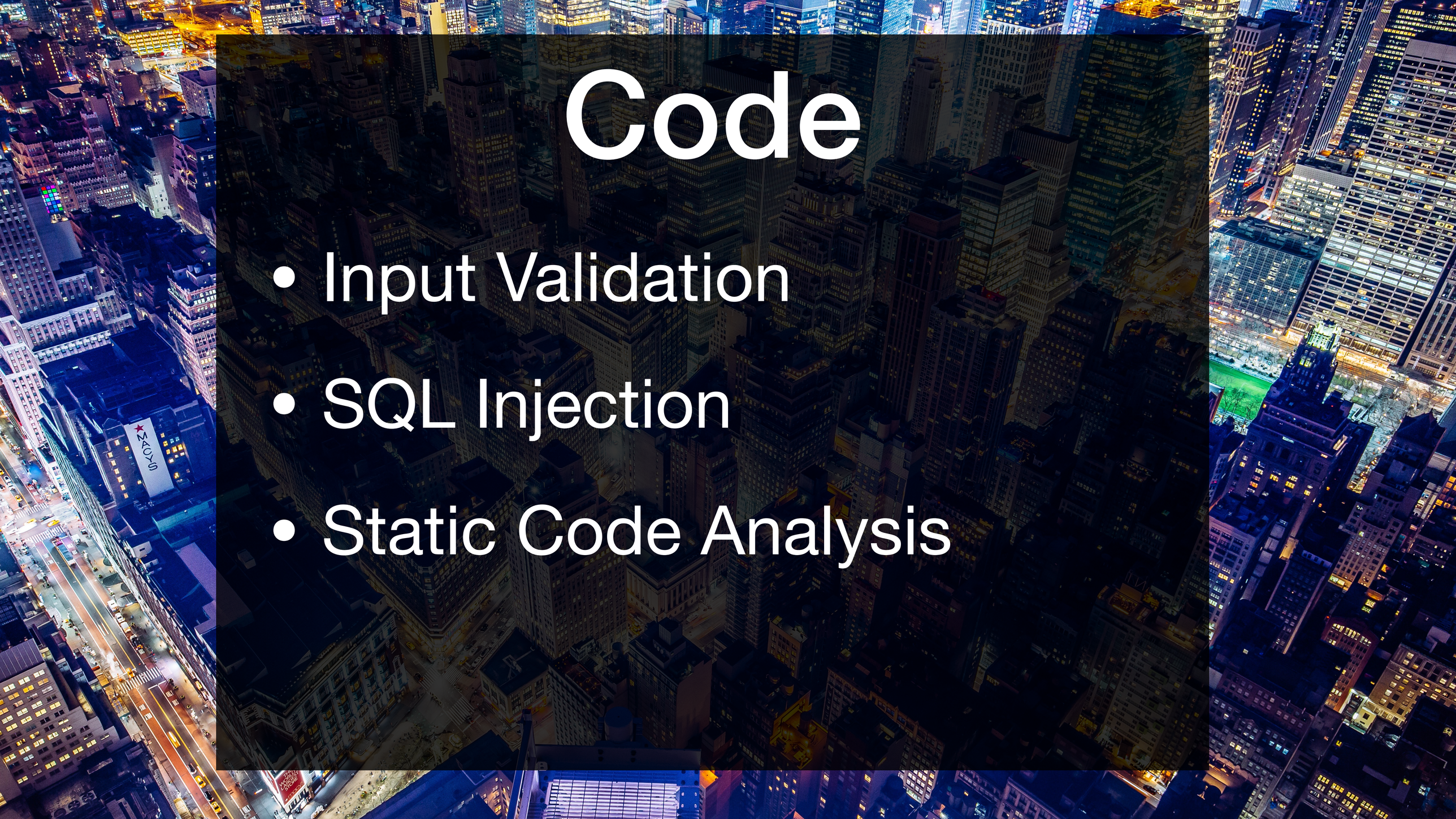
~
~
-- INSERT --

```go
package injection

import (
    "database/sql"
    "fmt"
    "strings"
)

func insertUsers(db *sql.DB, names []string) {
    var values []string
    for _, name := range names {
        values = append(values, fmt.Sprintf("('%s')", name))
    }
    query := fmt.Sprintf(
        "INSERT INTO users (name) VALUES %s",
        strings.Join(values, ","),
    )
    db.Query(query)
}

func insertUsersSafe(db *sql.DB, names []string) {
    // How would you write it? ;)
}
~
~
-- INSERT --
```



Code

- Input Validation
- SQL Injection
- Static Code Analysis

```
Results:

[going-secure/examples/random/math-seed-time/main.go:13] - G404: Use of weak random number
generator (math/rand instead of crypto/rand) (Confidence: MEDIUM, Severity: HIGH)
  > rand.Read(b)

[going-secure/examples/sql-injection/bulk.go:14-17]
- G201: SQL string formatting (Confidence: HIGH, Severity: MEDIUM)
  > fmt.Sprintf(
                "INSERT INTO users (name) VALUES %s",
                strings.Join(values, ","),
        )

[going-secure/examples/sql-injection/single.go:9]
- G201: SQL string formatting(Confidence: HIGH, Severity: MEDIUM)
  > fmt.Sprintf("SELECT * FROM users WHERE name = '%s'", name)

Summary:
   Files: 10
   Lines: 181
  Issues: 11
```

```
Results:

[going-secure/examples/random/math-seed-time/main.go:13] - G404: Use of weak random number
generator (math/rand instead of crypto/rand) (Confidence: MEDIUM, Severity: HIGH)
  > rand.Read(b)

[going-secure/examples/sql-injection/bulk.go:14-17]
- G201: SQL string formatting (Confidence: HIGH, Severity: MEDIUM)
  > fmt.Sprintf(
                "INSERT INTO users (name) VALUES %s",
                strings.Join(values, ","),
        )

[going-secure/examples/sql-injection/single.go:9]
- G201: SQL string formatting(Confidence: HIGH, Severity: MEDIUM)
  > fmt.Sprintf("SELECT * FROM users WHERE name = '%s'", name)

Summary:
   Files: 10
   Lines: 181
  Issues: 11
```

Go linter that checks if package imports are in a list of acceptable packages.

10 commits | 1 branch | 0 releases | 1 contributor | GPL-3.0

Branch: master | New pull request | Create new file | Upload files | Find File | Clone or download

bbrodriges and dixonwille allow to check packages only for test files — Latest commit 1f388ab on 19 Dec 2018

cmd/depguard	allow to check packages only for test files	4 months ago
vendor	Add support for glob matching	9 months ago
.gitignore	Initial commit	11 months ago
Gopkg.lock	Add support for glob matching	9 months ago
Gopkg.toml	Add support for glob matching	9 months ago
LICENSE	Initial commit	11 months ago
README.md	allow to check packages only for test files	4 months ago
depguard.go	allow to check packages only for test files	4 months ago

README.md

Depguard

Go linter that checks package imports are in a list of acceptable packages. It supports a white list and black list option and can do prefix or glob matching. This allows you to allow imports from a whole organization or only allow specific packages within a repository. It is recommended to use prefix matching as it is faster than glob matching. The fewer glob matches the better.

> If a pattern is matched by prefix it does not try to match via glob.

golangci / golangci-lint

Watch 36 | Star 2,352 | Fork 150

Code | Issues 109 | Pull requests 3 | Projects 0 | Wiki | Insights

Linters Runner for Go. 5x faster than gometalinter. Nice colored output. Can report only new issues. Fewer false-positives. Yaml/toml config. https://golangci.com

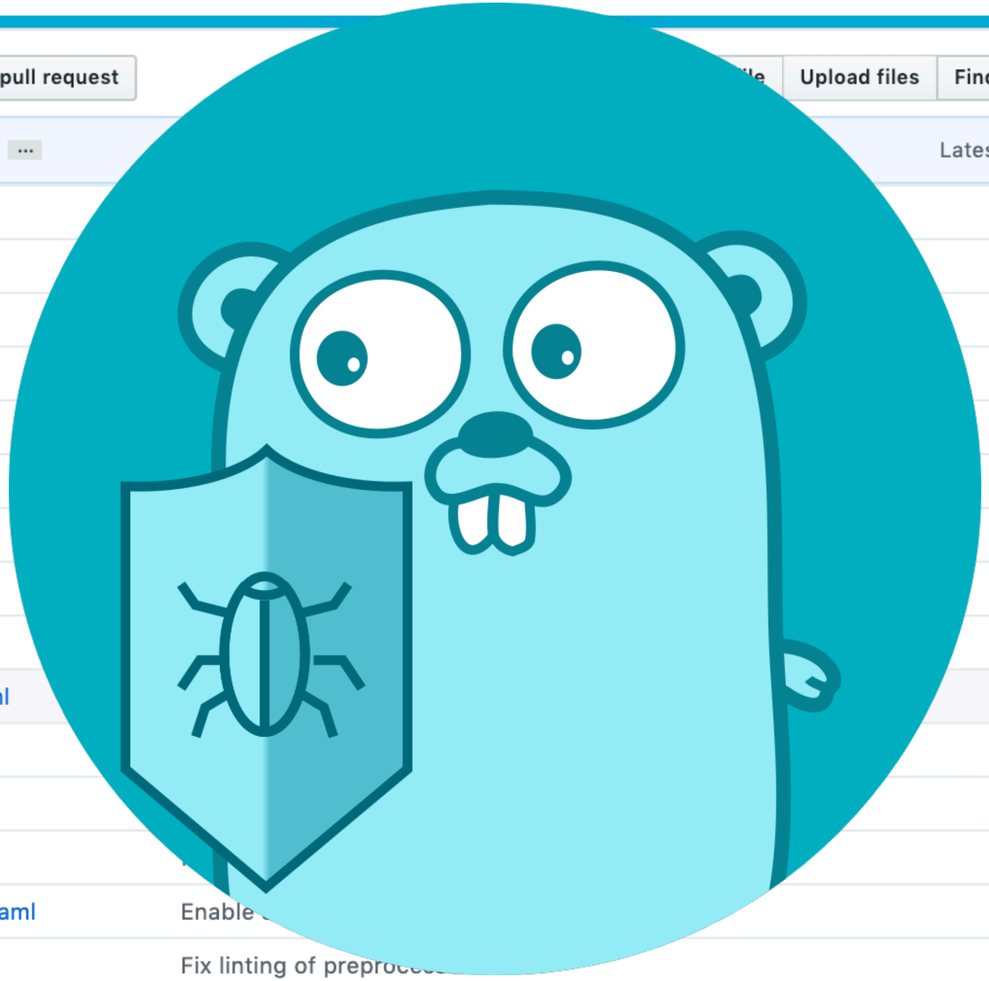
go golang linter ci

411 commits | 12 branches | 46 releases | 56 contributors | GPL-3.0

Branch: master | New pull request | Upload files | Find File | Clone or download

jirfag Update go-critic ... Latest commit 692dacb 3 days ago

.github		6 months ago
cmd/golangci-lint		2 months ago
docs		11 months ago
pkg		7 days ago
scripts		a month ago
test		7 days ago
third_party		a month ago
vendor		2 days ago
.gitignore		27 days ago
.golangci.example.yml		8 days ago
.golangci.yml		2 days ago
.goreleaser.yml		3 months ago
.markdownlint.yaml		6 months ago
.pre-commit-hooks.yaml	Enable	7 days ago
.travis.yml	Fix linting of preproce	7 days ago



golangci / golangci-lint

Watch 36 | Star 2,352 | Fork 150

Code | Issues 109 | Pull requests 3 | Projects 0 | Wiki | Insights

Linters Runner for Go. 5x faster than gometalinter. Nice colored output. Can report only new issues. Fewer false-positives. Yaml/toml config. https://golangci.com

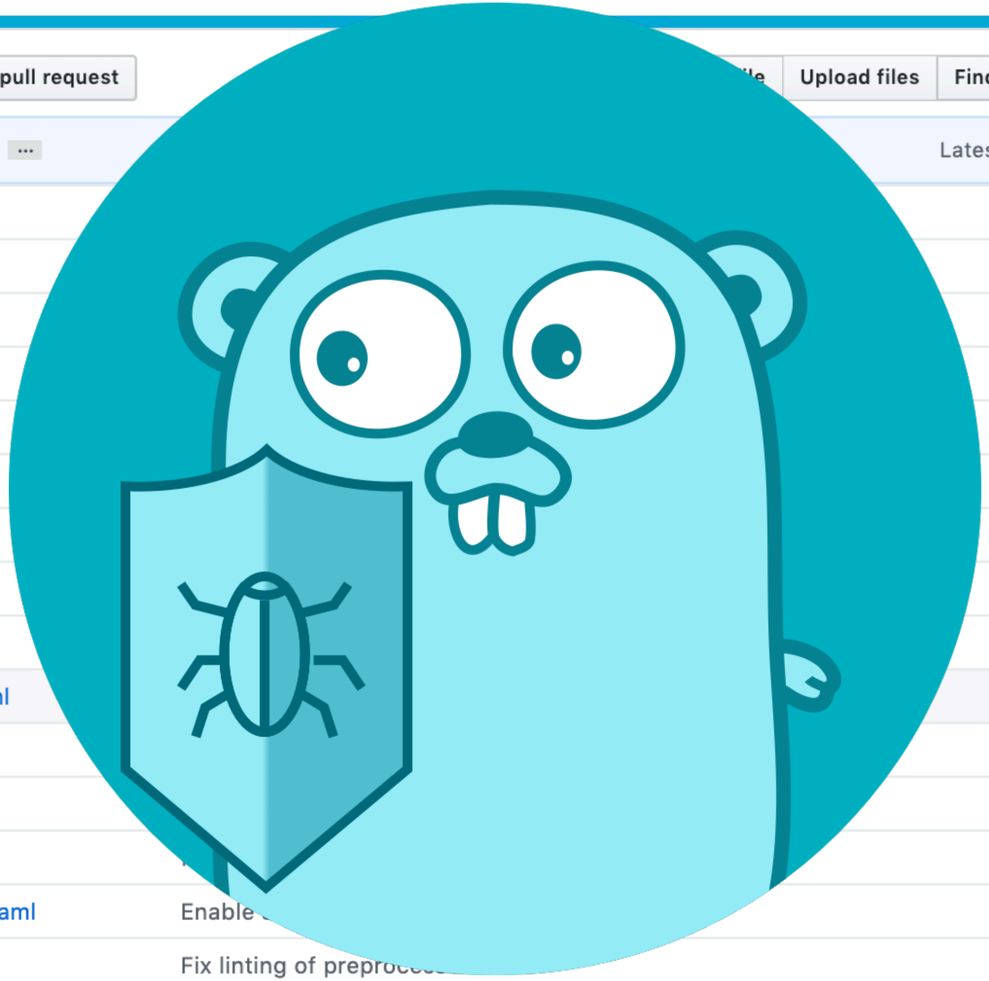
go golang linter ci

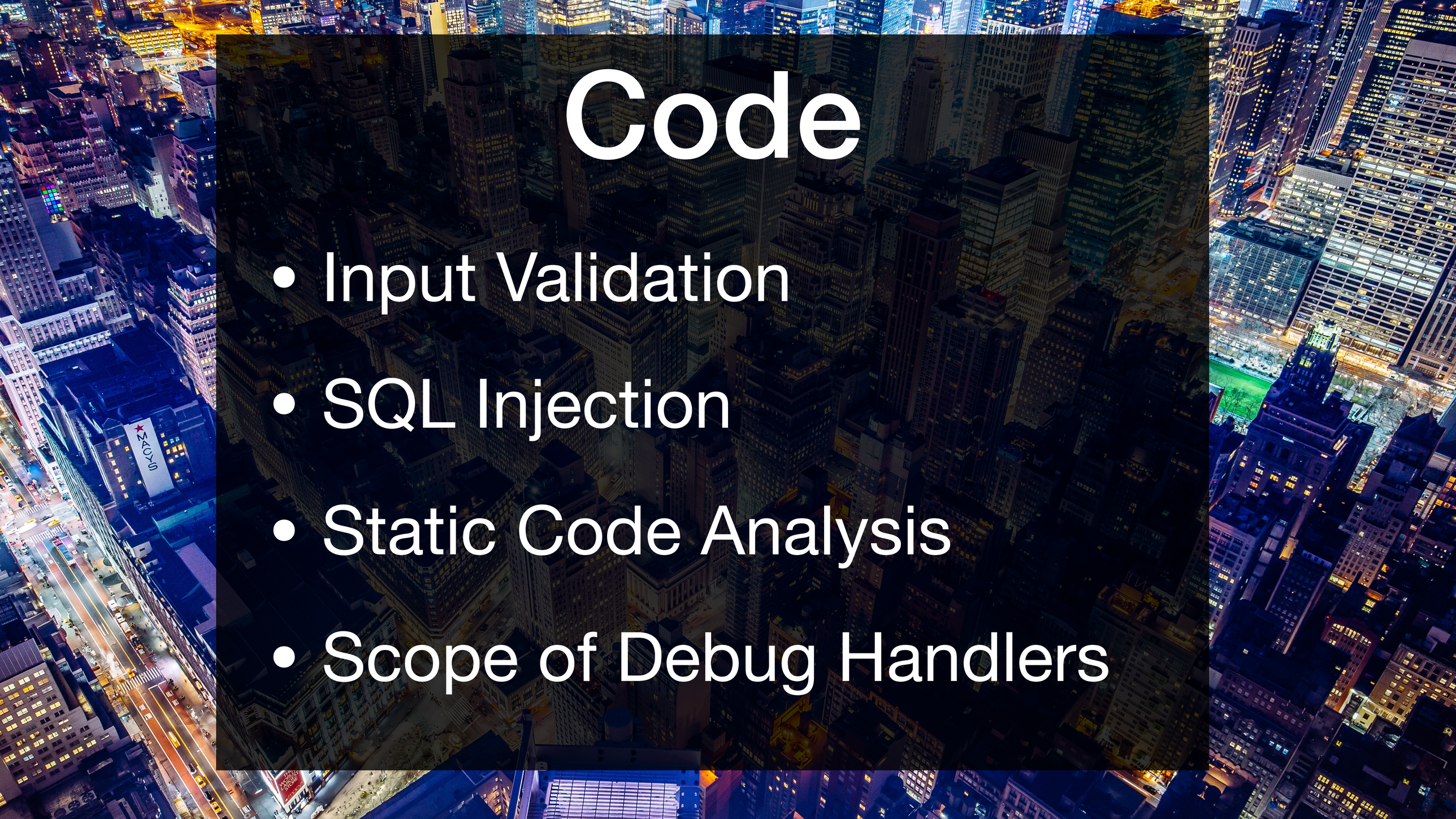
411 commits | 12 branches | 46 releases | 56 contributors | GPL-3.0

Branch: master | New pull request | Upload files | Find File | Clone or download

jirfag Update go-critic ... Latest commit 692dacb 3 days ago

.github		6 months ago
cmd/golangci-lint		2 months ago
docs		11 months ago
pkg		7 days ago
scripts		a month ago
test		7 days ago
third_party		a month ago
vendor		2 days ago
.gitignore		27 days ago
.golangci.example.yml		8 days ago
.golangci.yml		2 days ago
.goreleaser.yml		3 months ago
.markdownlint.yaml		6 months ago
.pre-commit-hooks.yaml	Enable	7 days ago
.travis.yml	Fix linting of preproce	7 days ago





Code

- Input Validation
- SQL Injection
- Static Code Analysis
- Scope of Debug Handlers

```
package pprofed

import (
    "net/http"
    _ "net/http/pprof" // add pprof handlers
)

func serve(addr string) {
    http.HandleFunc("/", func(w http.ResponseWriter, r *http.Request) {
        // provide some business logic
    })

    http.ListenAndServe(addr, nil)
}
~
~
~
~
~
~
~
~
~
~
-- INSERT --
```

```go
package pprofed

import (
    "net/http"
    "net/http/pprof"

    "github.com/gorilla/mux"
)

func diagnostics(addr string) error {
    r := mux.NewRouter()

    r.HandleFunc("/diag/pprof", pprof.Index)
    r.HandleFunc("/diag/cmdline", pprof.Cmdline)
    r.HandleFunc("/diag/profile", pprof.Profile)
    r.HandleFunc("/diag/symbol", pprof.Symbol)
    r.HandleFunc("/diag/trace", pprof.Trace)
    r.Handle("/diag/goroutine", pprof.Handler("goroutine"))
    r.Handle("/diag/heap", pprof.Handler("heap"))
    r.Handle("/diag/threadcreate", pprof.Handler("threadcreate"))
    r.Handle("/diag/block", pprof.Handler("block"))

    return http.ListenAndServe(addr, r)
}
```

-- INSERT --

```
func external(addr string) error {
    r := mux.NewRouter()

    r.HandleFunc("/", func(w http.ResponseWriter, r *http.Request) {
        // provide some business logic
    })

    return http.ListenAndServe(addr, r)
}
```

~
~
~
~
~
~
~
~
~
~
~
~
~
~
~

-- INSERT --

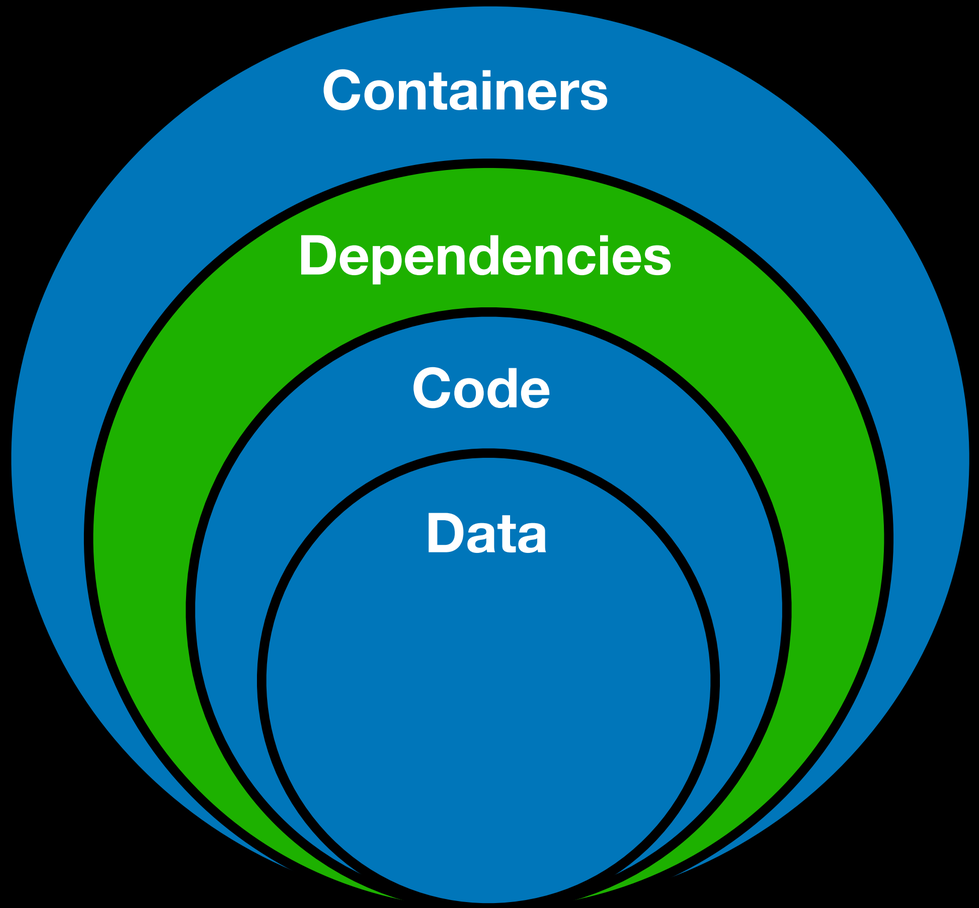
Bill Sempf
@sempf

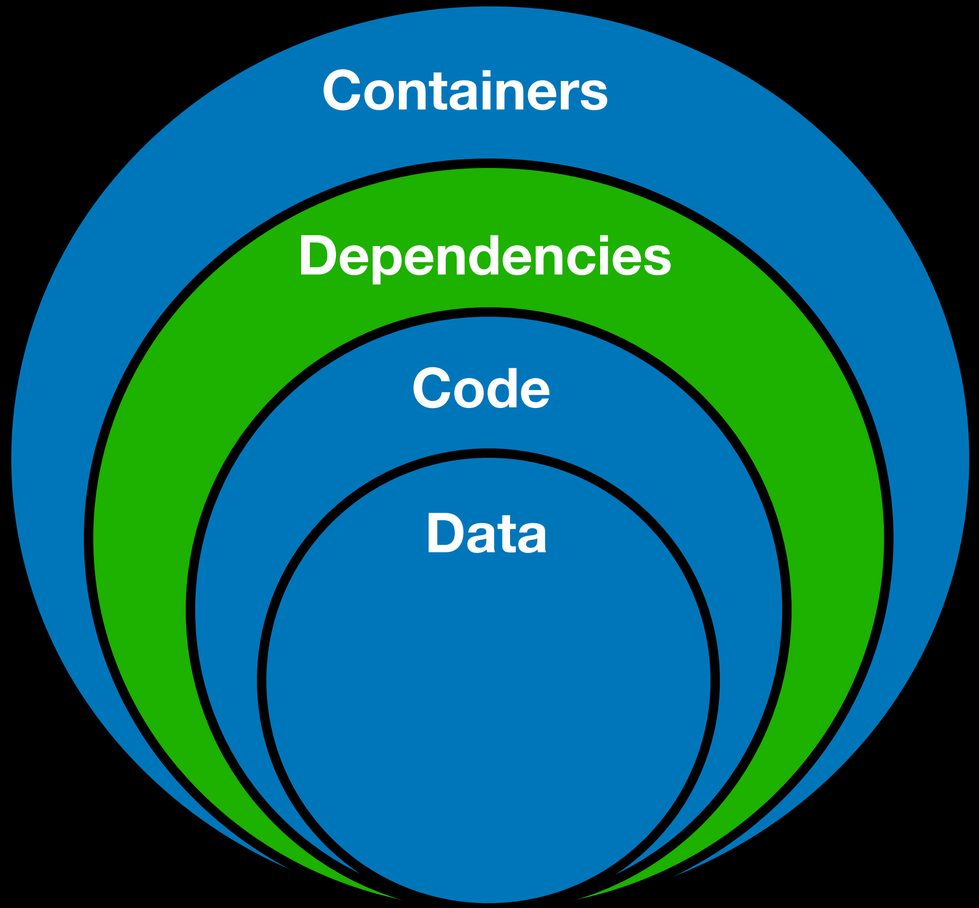
Follow

QA Engineer walks into a bar. Orders a beer. Orders 0 beers. Orders 999999999 beers. Orders a lizard. Orders -1 beers. Orders a sfdeljknesv.

10:56 AM - 23 Sep 2014

29,050 Retweets **21,155** Likes


Containers
Dependencies
Code
Data


Containers
Dependencies
Code
Data

Natalie
@NataliePis

Follow

“Are you absolutely sure this doesn’t exist in your codebase with all the dependencies?”

@davecheney at @dotGoEu

6:29 AM - 25 Mar 2019

41 Retweets **105** Likes

2 41 105

Dependencies

- Dependencies Checklist

Dependencies

- Dependencies Checklist
- Checklist

Dependencies Checklist

- Code Quality

Dependencies Checklist

- Code Quality
- Test Coverage

Dependencies Checklist

- Code Quality
- Test Coverage
- Activity

Dependencies Checklist

- Code Quality
- Test Coverage
- Activity
- Maintainers

Dependencies Checklist

- Code Quality
- Test Coverage
- Activity
- Maintainers
- Security

Dependencies Checklist

- Code Quality
- Test Coverage
- Activity
- Maintainers
- Security
- Licenses

Dependencies Checklist

- Code Quality
- Test Coverage
- Activity
- Maintainers
- Security
- Licenses

research.swtch.com/deps

Dependencies

- Dependencies Checklist
  - Checklist
  - Examples

Example 1

During the briefing, Equifax representatives informed Oversight Committee staff that:

- the company failed to heed a March 8, 2017, alert from US-CERT explicitly warning about a specific vulnerability through a web-application known as "Apache Struts";
- the company's failure allowed cyber attackers to exploit this vulnerability to gain access to hundreds of millions of sensitive consumer files and documents from May 13, 2017, to July 29, 2017—the date that Equifax finally detected the breach;
- the company's General Counsel did not inform the FBI about the breach until the following Wednesday, August 2, 2017;

Takeaways

- Picking "safe" dependencies is not enough

Example 1

Takeaways

- Picking "safe" dependencies is not enough
- Know what transitive dependencies you use

Example 1

Takeaways

- Picking "safe" dependencies is not enough
- Know what transitive dependencies you use
- Continuously monitor new discoveries

Example 1

Example 1

Dependabot

Report abuse

Automated dependency updates

London https://dependabot.com support@dependabot.... Verified

Repositories 17 People 4 Projects 0

Pinned repositories

feedback
Feedback, feature requests, and bug reports for Dependabot 🤖
★ 36 7

dependabot-core
🤖 The core logic behind Dependabot's update PR creation
Ruby ★ 424 72

api-docs
Documentation for Dependabot's API
★ 8 4

Find a repository... Type: All Language: All

dependabot-core
🤖 The core logic behind Dependabot's update PR creation

javascript ruby python java go docker rust

Ruby ★ 424 72 Updated 6 hours ago

dependabot-script
A simple script that demonstrates how to use Dependabot Core

Ruby ★ 34 17 MIT Updated a day ago

api-docs
Documentation for Dependabot's API

★ 8 4 Updated 18 days ago

dockerfiles
Dockerfile Updated 27 days ago

yarn-lib
A build of yarn that provides access to its internals

Top languages
Ruby PHP Go
Jupyter Notebook Dockerfile

People 4 >

Developer Program Member

Supported languages

Ruby
JavaScript
Python
PHP
Elixir
Rust
Java - Maven BETA
Java - Gradle BETA
.NET BETA
Go ALPHA
Elm ALPHA
Submodules
Docker
Terraform ALPHA

Takeaways

- Picking "safe" dependencies is not enough
- Know what transitive dependencies you use
- Continuously monitor new discoveries
- Upgrade swiftly

Example 1

Example 2

The Register®
Biting the hand that feeds IT

Security

Check your repos... Crypto-coin-stealing code sneaks into fairly popular NPM lib (2m downloads per week)

Node.js package tried to plunder Bitcoin wallets

By Thomas Claburn in San Francisco 26 Nov 2018 at 20:58 49 SHARE ▼

Takeaways

- Multiple maintainers > a single maintainer

Example 2

Takeaways

- Multiple maintainers > a single maintainer
- Automatic upgrades can have risks

Example 2

Takeaways

- Multiple maintainers > a single maintainer
- Automatic upgrades can have risks
- Lock your dependencies versions

Example 2

Example 3

The Register®
Biting the hand that feeds IT

Software

How one developer just broke Node, Babel and thousands of projects in 11 lines of JavaScript

Code pulled from NPM – which everyone was using

By Chris Williams, Editor in Chief 23 Mar 2016 at 01:24 168 SHARE ▼

Careful, careful ... Don't fumble this like the JS world (Credit: Claus Rebler)

Updated Programmers were left staring at broken builds and failed installations on Tuesday after someone toppled the Jenga tower of JavaScript.

Example 3

The Register®
Biting the hand that feeds IT

Software

How one developer just broke Node, Babel and thousands of projects in 11 lines of JavaScript

Code pulled from NPM – which everyone was using

By Chris Williams, Editor in Chief 23 Mar 2016 at 01:24 168 SHARE ▼

Careful, careful ... Don't fumble this like the JS world (Credit: Claus Rebler)

Updated Programmers were left staring at broken builds and failed installations on Tuesday after someone toppled the Jenga tower of JavaScript.

Takeaways

- Immutable dependencies are a must

Example 3

Takeaways

- Immutable dependencies are a must
- Central repositories can be risky

Example 3

Example 4

lerna / lerna

Watch 201 | Star 14,511 | Fork 931

Code | Issues 147 | Pull requests 6 | Projects 0 | Wiki | Insights

Add text to MIT License banning ICE collaborators #1616

Merged **jamiebuilds** merged 2 commits into `master` from `new-license` on Aug 29, 2018

Conversation 11 | Commits 2 | Checks 0 | Files changed 1 | +22 −1

jamiebuilds commented on Aug 29, 2018 • edited by TheLarkInn | Contributor

In this PR, the following text has been added to the existing MIT license:

```
The following license shall not be granted to the following entities or any
subsidiary thereof due to their collaboration with US Immigration and Customs
Enforcement ("ICE"):

- "Microsoft Corporation"
- "Palantir Technologies"
- "Amazon.com, Inc."
- ...
```

I have already spoken to **@kittens** and **@evocateur** about this privately, but I do need **@kittens** to give us permission to make this change.

18 | 9 | 10 | 1 | 15

Reviewers

evocateur ✓

kittens ✓

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

Example 4

lerna / lerna

Watch 201 | Star 14,511 | Fork 931

Code | Issues 147 | Pull requests 6 | Projects 0 | Wiki | Insights

Add text to MIT License banning ICE collaborators #1616

Merged **jamiebuilds** merged 2 commits into `master` from `new-license` on Aug 29, 2018

Conversation 11 | Commits 2 | Checks 0 | Files changed 1 | +22 −1

jamiebuilds commented on Aug 29, 2018 • edited by TheLarkInn | Contributor

In this PR, the following text has been added to the existing MIT license:

```
The following license shall not be granted to the following entities or any
subsidiary thereof due to their collaboration with US Immigration and Customs
Enforcement ("ICE"):

- "Microsoft Corporation"
- "Palantir Technologies"
- "Amazon.com, Inc."
- ...
```

I have already spoken to **@kittens** and **@evocateur** about this privately, but I do need **@kittens** to give us permission to make this change.

18 | 9 | 10 | 1 | 15

Reviewers

evocateur ✓

kittens ✓

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

Example 4

lerna / lerna

Watch 201 | Star 14,511 | Fork 931

Code | Issues 147 | Pull requests 6 | Projects 0 | Wiki | Insights

Add text to MIT License banning ICE collaborators #1616

Merged **jamiebuilds** merged 2 commits into `master` from `new-license` on Aug 29, 2018

Conversation 11 | Commits 2 | Checks 0 | Files changed 1 | +22 −1

jamiebuilds commented on Aug 29, 2018 • edited by TheLarkInn | Contributor

In this PR, the following text has been added to the existing MIT license:

```
The following license shall not be granted to the following entities or any
subsidiary thereof due to their collaboration with US Immigration and Customs
Enforcement ("ICE"):

- "Microsoft Corporation"
- "Palantir Technologies"
- "Amazon.com, Inc."
- ...
```

I have already spoken to **@kittens** and **@evocateur** about this privately, but I do need **@kittens** to give us permission to make this change.

18 | 9 | 10 | 1 | 15

Reviewers

evocateur ✓

kittens ✓

Assignees

No one assigned

Labels

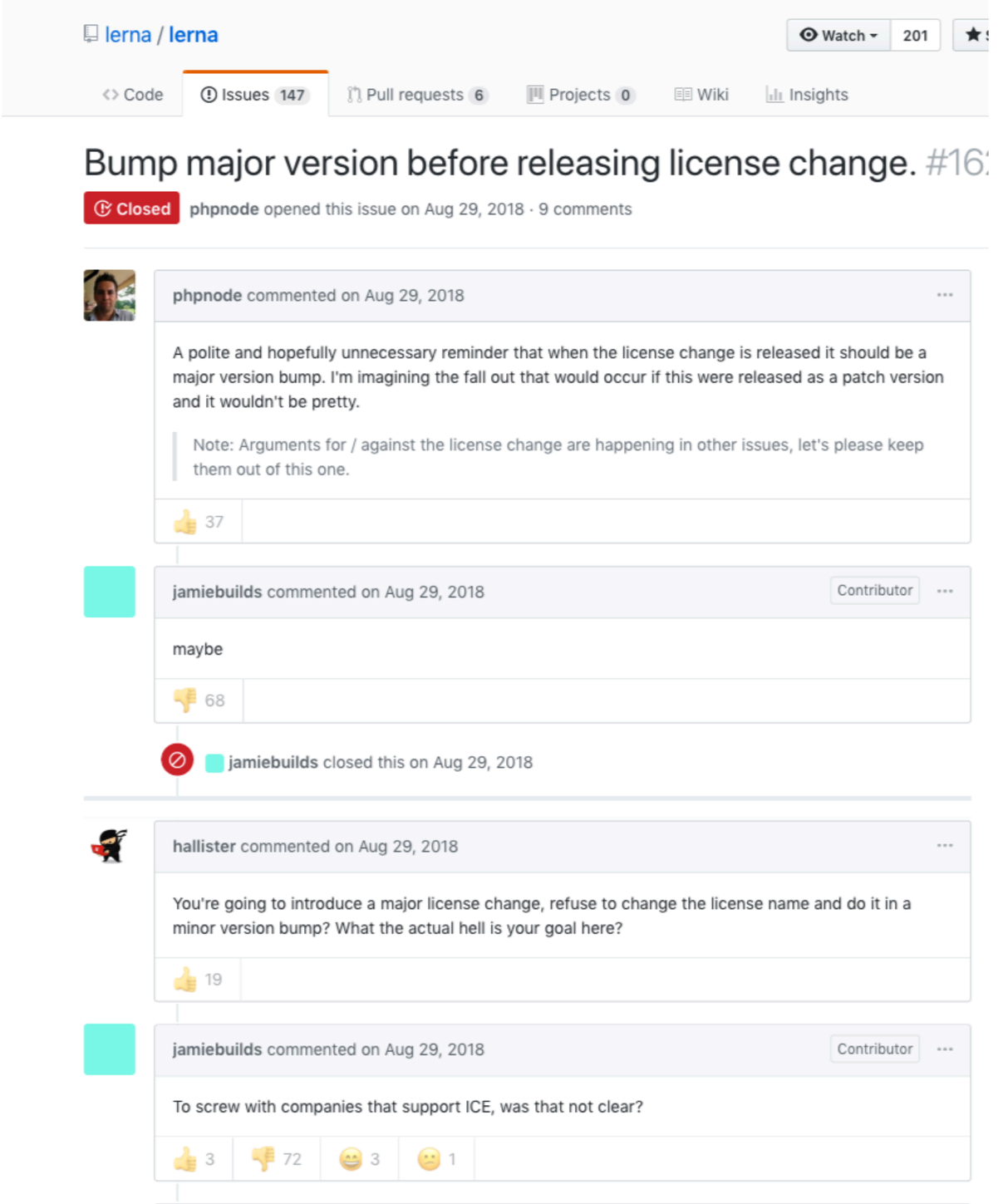
None yet

Projects

None yet

Milestone

Example 4



lerna / lerna

Watch 201

Code | Issues 147 | Pull requests 6 | Projects 0 | Wiki | Insights

Bump major version before releasing license change. #16

Closed **phpnode** opened this issue on Aug 29, 2018 · 9 comments

phpnode commented on Aug 29, 2018

A polite and hopefully unnecessary reminder that when the license change is released it should be a major version bump. I'm imagining the fall out that would occur if this were released as a patch version and it wouldn't be pretty.

> Note: Arguments for / against the license change are happening in other issues, let's please keep them out of this one.

37

jamiebuilds commented on Aug 29, 2018 Contributor

maybe

68

jamiebuilds closed this on Aug 29, 2018

hallister commented on Aug 29, 2018

You're going to introduce a major license change, refuse to change the license name and do it in a minor version bump? What the actual hell is your goal here?

19

jamiebuilds commented on Aug 29, 2018 Contributor

To screw with companies that support ICE, was that not clear?

3 72 3 1

Takeaways

- Licenses can be as a complex as security issues

Example 4

Takeaways

- Licenses can be as a complex as security issues
- Even minor upgrades need attention

Example 4

To Summarize

To Summarize

To Summarize

- Control your dependency tree

To Summarize

- Control your dependency tree
- Add dependencies consciously

To Summarize

- Control your dependency tree
- Add dependencies consciously
- Continuously verify the dependencies

To Summarize

- Control your dependency tree
- Add dependencies consciously
- Continuously verify the dependencies
- Always have a reproducible build

To Summarize

- Control your dependency tree
- Add dependencies consciously
- Continuously verify the dependencies
- Always have a reproducible build
- Upgrade dependencies frequently

Dependencies

- Dependencies Checklist
- Solutions in Go

Solutions

- Unused imports are errors

Solutions

- Unused imports are errors
- Regularly check and update your *go.mod*

Solutions

- Unused imports are errors
- Regularly check and update your *go.mod*
  - Unused packages deleted from *go.mod*

Solutions

- Unused imports are errors
- Regularly check and update your *go.mod*
  - Unused packages deleted from *go.mod*
  - Transitive dependencies are added to *go.mod*

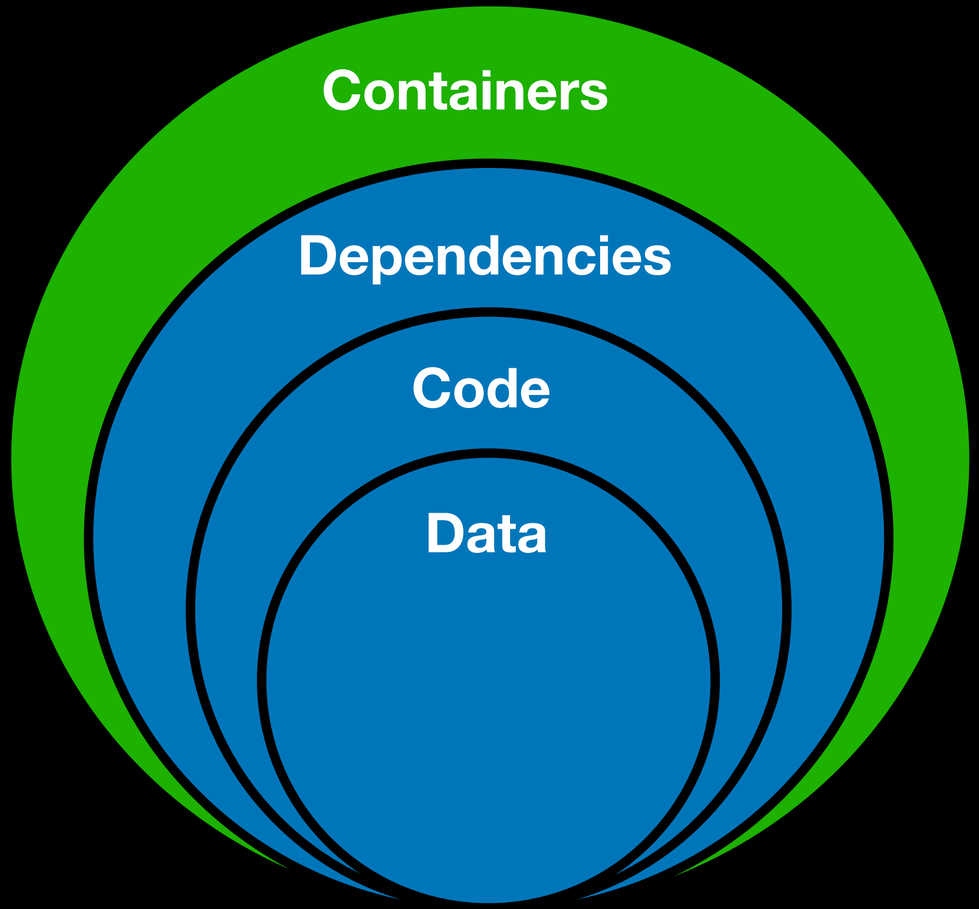
Solutions

- Unused imports are errors
- Regularly check and update your *go.mod*
  - Unused packages deleted from *go.mod*
  - Transitive dependencies are added to *go.mod*
- Use vulnerabilities and licenses databases (e.g. NVD, JFrog Xray)

Solutions

- Unused imports are errors
- Regularly check and update your *go.mod*
  - Unused packages deleted from *go.mod*
  - Transitive dependencies are added to *go.mod*
- Use vulnerabilities and licenses databases (e.g. NVD, JFrog Xray)
- Minimal sanity check: *goreportcard*

goreportcard.com


Containers
Dependencies
Code
Data

Containers

- Multi-Stage Build

```
# Stage 0. Build the binary
FROM artifactory/golang:1.11

# add a non-privileged user
RUN useradd -u 10001 myapp

RUN mkdir -p /go/src/github.com/rumyantseva/myapp
ADD . /go/src/github.com/rumyantseva/myapp
WORKDIR /go/src/github.com/rumyantseva/myapp

# Build the binary with go build

# Important! Here we consider the "old way" when the vendor
# directory is commited and pushed to the repo
# and might be considered as immutable.
# If you use go mod and GOPROXY,
# this part should be handled a little bit differentely!
RUN CGO_ENABLED=0 go build \
    -o bin/myapp github.com/rumyantseva/myapp/cmd/myapp

# Stage 1. Run the binary
~
~
~
```

```
# Stage 1. Run the binary
FROM scratch

ENV PORT 8080

# certificates to interact with other services
COPY --from=0 /etc/ssl/certs/ca-certificates.crt /etc/ssl/certs/

# don't forget /etc/passwd from previous stage
COPY --from=0 /etc/passwd /etc/passwd
USER myapp

# and finally the binary
COPY --from=0 /go/src/github.com/rumyantseva/myapp/bin/myapp /myapp
EXPOSE $PORT

CMD ["myapp"]
~
~
~
~
~
~
~
~
```

```
FROM artifactory/golang:1.11

# Change here to update
ENV VERSION 1.12.3
ENV CHECKSUM c531688661b500d4c0c500fcf57f829388a4a9ba79697c2e134302aedef0cd46

# Make sure we have a fixed golangci-lint script with a chekcsum check
RUN echo "${CHECKSUM}  golangci-lint-${VERSION}-linux-amd64.tar.gz" > CHECKSUM

# Download from Github the specified release and extract into the go/bin folder
RUN curl -L "https://github.com/golangci/golangci-lint/releases/download/v${VERSION}/golangci-l
int-${VERSION}-linux-amd64.tar.gz" \
    -o golangci-lint-${VERSION}-linux-amd64.tar.gz \
    && shasum -a 256 -c CHECKSUM \
    && tar xvzf golangci-lint-${VERSION}-linux-amd64.tar.gz \
        --strip-components=1 \
        -C ./bin \
        golangci-lint-${VERSION}-linux-amd64/golangci-lint

# Clean up
RUN rm -rf CHECKSUM "golangci-lint-${VERSION}-linux-amd64.tar.gz"
~
~
~
```

```
FROM artifactory/golang-linters

RUN mkdir -p /go/src/github.com/rumyantseva/myapp
ADD . /go/src/github.com/rumyantseva/myapp
WORKDIR /go/src/github.com/rumyantseva/myapp

# Run linters
RUN golangci-lint run \
    --no-config --issues-exit-code=1 \
    --deadline=10m --exclude-use-default=false \
    --enable-all \
    ./...

# Run tests
RUN go test -timeout=600s -v --race ./...
```

Containers

- Multi-Stage Build
- Policies

Policies

- Pod Security Policies, e.g.
  - Disallow containers in privileged containers
  - Disallow containers that require root access
  - Disallow containers that access a specific host port

kubernetes.io/docs/concepts/policy/pod-security-policy

Policies

- Pod Security Policies
- Network Policies
  - Pod ingress/egress traffic shaping

kubernetes.io/docs/concepts/extend-kubernetes/compute-storage-net/network-plugins

Policies

- Pod Security Policies
- Network Policies
- Kritis

github.com/grafeas/kritis

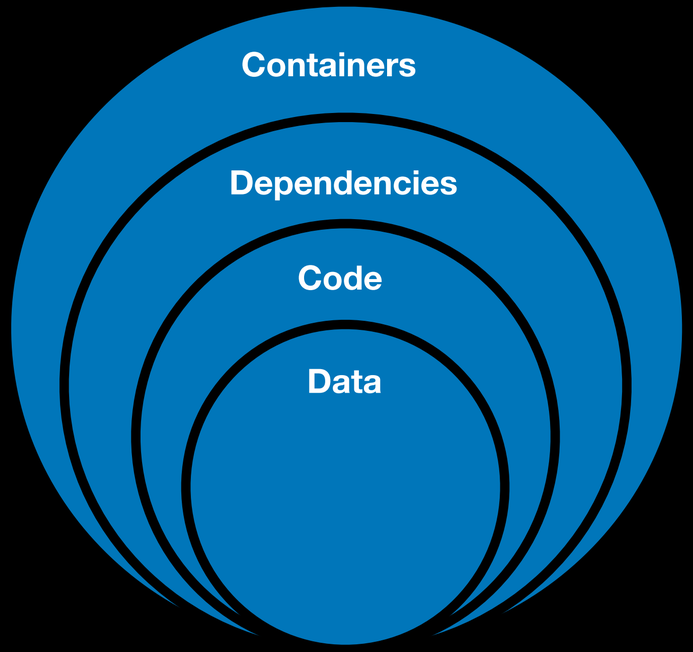

Overwhelmed?


Automate!

DevSecOps

"The philosophy of integrating security practices within the DevOps process."

- Data
  - Passwords
  - User Personal Data
  - Secrets Management
- Code
  - Input Validation
  - SQL Injection
  - Static Code Analysis
  - Scope of Debug Handles
- Dependencies
  - Dependencies Checklist
    - Checklist
    - Examples
  - Solutions in Go
- Containers
  - Multi-Stage Build
  - Policies



Thank You!

@NataliePis