

차량 업데이트 파일의 안전한 관리

다양한 Go 의 활용

이호민 / 42dot



Speaker



이호민

42dot / Connected Car Platform

“Go 언어의 실용성, 속도, 그리고 생산성에 매료되어 10년 이상 사용해 왔으며, 42dot에서는 SDV(Software Defined Vehicle)의 안전한 업데이트를 지원하는 서버를 작성하고 운영하고 있습니다.

시스템 아키텍처와 보안에 관심이 많으며 Go를 사용해 안정성과 효율성을 극대화하는 데 주력하고 있습니다.”



GopherCon Korea 2024

여러분이 얻어가실 내용

- 보안 기본 개념 탑재
- 다양한 용도로 **Go**를 사용한 사례
 - **UI**가 있는 앱을 만드는데 **Go**를 활용하는 방법






SDV



Software Defined Vehicle



“SDV (Software Defined Vehicle)는 소프트웨어로 하드웨어를 제어하고 관리하는 자동차를 뜻한다. 소프트웨어를 수시로 업데이트해 성능을 개선하고 앱을 설치해 새로운 기능도 추가하는 스마트폰과 유사한 모습이다.”

https://ko.wikipedia.org/wiki/Software_Defined_Vehicle



Software OTA update 왜 함?

- Seamless 한 사용자 경험
- 몇만 대 ~ 몇백만 대의 리콜 비용 절약
 - 안전과 보안에 관련된 **SW** 수정 필요한 경우
- OTA 시스템이 완벽(**bullet proof**) 해야 함





CIA Triad



보안의 3 요소 (CIA triad)

- **Confidentiality:** 업데이트 파일의 암호화
- **Integrity:** 업데이트 파일의 무결성 보장
- **Availability:** 업데이트 파일에 접근할 수 있어야 함





업데이트 파일의 암호화



ChatGPT에게 시키기



“파일을 암호화 하는 코드를 Go 로 작성해줘”



// encryptFile 함수는 주어진 파일을 AES-256-GCM으로 암호화하여 ".enc" 확장자로 저장합니다.

```
func encryptFile(filename string, dataKey []byte) error {  
    plaintext, _ := os.ReadFile(filename)  
    // AES 암호화 블록을 생성합니다.  
    block, _ := aes.NewCipher(dataKey)  
    // GCM(Galois/Counter Mode) 암호화 모드를 초기화합니다.  
    gcm, _ := cipher.NewGCM(block)  
    // Nonce(암호화에 사용될 초기화 벡터)를 생성합니다.  
    nonce := make([]byte, gcm.NonceSize())  
    io.ReadFull(rand.Reader, nonce)  
    // nonce를 포함한 최종 암호문을 생성합니다.  
    ciphertext := gcm.Seal(nonce, nonce, plaintext, nil)  
    return os.WriteFile(filename+".enc", ciphertext, 0644)  
}
```



손 본 내역



- `io.Reader`, `io.Writer` 로 입출력 인자 받기
 - 정해진 크기의 버퍼를 사용해 메모리 절약
- **Enveloped Encryption**



외부 패키지

- 파일의 암호화는 **CLI** 툴로 로컬에서 미리 진행
 - cobra
- 암호화된 파일과, 데이터키를 **CRUD** 하는 **REST API** 서버 작성
 - gin 또는 echo 등등등...





Envelope Encryption



대칭키 암호화

- 하나의 키로 암호화와 복호화 모두 수행
- 대량 데이터 암호화, 실시간 통신 등에 주로 사용
- 대표 알고리즘: **AES, DES**
- 장점: 처리 속도가 빠르고 효율적
- 단점: 키 유출 시 보안 위협



/42dot

```
|— 1.root.yaml
|— root.yaml
|— vehicle1
    |— ecu1
        |— eb29f6ab7affd899a.ecu1_v1.0.4.img.enc
        |— aeb29f6ab7affd899.ecu1_v1.0.4.img.ekey
    |— ecu2
        |— 9dcaeaa36ec161d6c.ecu2_v1.0.0.img.enc
        |— 9dcaeaa36ec161d6c.ecu2_v1.0.0.img.ekey
    |— metadata
        |— 3.targets.yaml
        |— 6.snapshot.yaml
        |— 9.timestamp.yaml
        |— targets.yaml
        |— snapshot.yaml
        |— timestamp.yaml
```






비대칭키 암호화

- 공개키로 암호화, 개인키로 복호화
- 키 교환, 디지털 서명, 인증 등에 주로 사용
- 대표 알고리즘: **RSA, ECC**
- 장점: 키 분배와 관리가 더 안전함 (공개키는 노출 가능)
- 단점: 속도가 느리고 복잡함



Envelope Encryption

- 대칭키로 암호화 한 바이너리를 스토리지(**CDN**)에 저장
- 암호화된 대칭키(**KMS**)를 스토리지에 저장
- 클라이언트가 공개키와 함께 업데이트 파일을 서버에 요청
- 데이터키를 클라이언트의 공개키로 암호화    하여 전송
- 클라이언트에서 데이터키를 복호화해 바이너리를 복호화
- 암호화 되지 않은 데이터키는 사용자에게 유출되지 않게 관리





업데이트 파일의 무결성 보장



Uptane

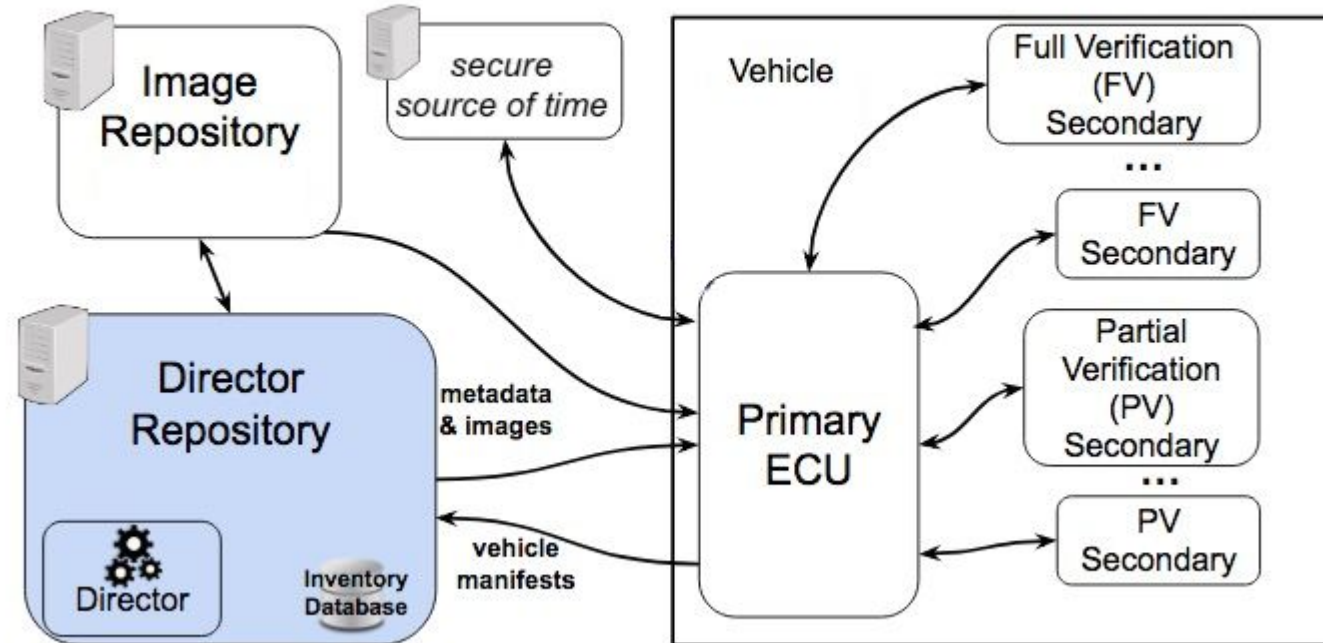
Uptane is an open-source framework that ensures the security of software updates for vehicles.

- <https://uptane.org/>






How Uptane Works

How Uptane Works



Uptane 의 무결성을 보장

- 바이너리와 메타데이터를 미리 생성하여 저장  **Image Repo.**
- 요청에 따라 메타데이터를 동적 생성  **Director Repo.**
- 메타데이터를 서명하여 작성자 보장  **Image/Director Repo.**
- **Image** 메타와 **Director** 의 메타 비교하여 공격받았는지 감지.



/42dot

```
| 1.root.yaml ←
| root.yaml
| vehicle1
|   | ecu1
|   |   | eb29f6ab7affd899a.ecu1_v1.0.4.img.enc
|   |   | aeb29f6ab7affd899.ecu1_v1.0.4.img.ekey
|   |   |
|   |   | ecu2
|   |   |   | 9dcaea36ec161d6c.ecu2_v1.0.0.img.enc
|   |   |   | 9dcaea36ec161d6c.ecu2_v1.0.0.img.ekey
|   |   |   |
|   |   |   | metadata
|   |   |   |   | 3.targets.yaml ←
|   |   |   |   | 6.snapshot.yaml
|   |   |   |   | 9.timestamp.yaml
|   |   |   |   | targets.yaml
|   |   |   |   | snapshot.yaml
|   |   |   |   | timestamp.yaml
```





앱 작성 (with Svelte)



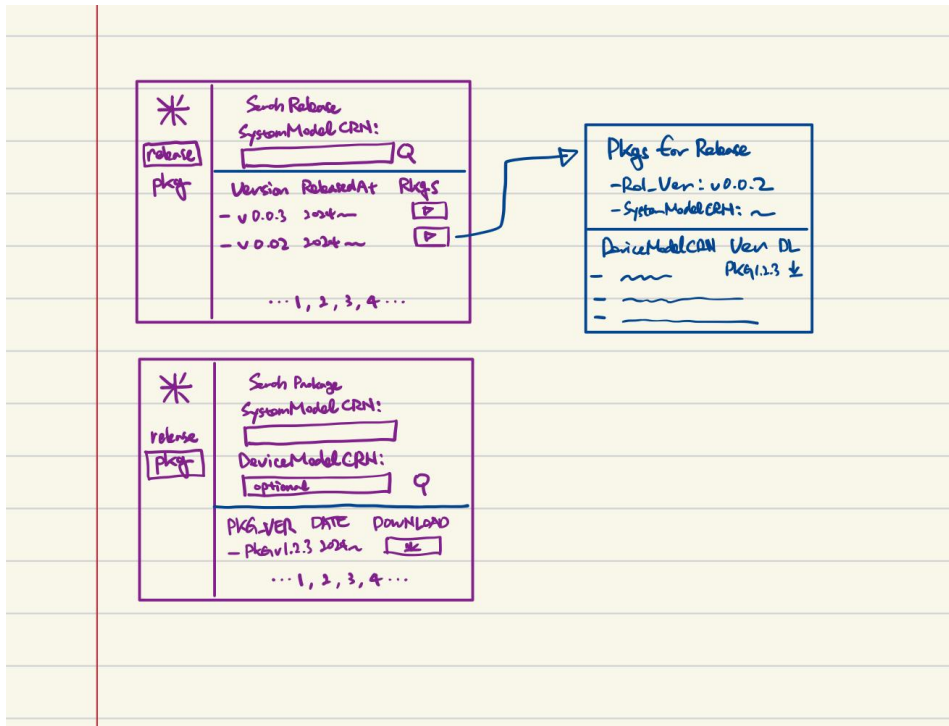
SvelteKit 특징

- <https://svelte.dev/>

SvelteKit은 컴파일 중심의 빠른 성능과 서버 사이드 렌더링 (SSR), 정적 사이트 생성(SSG) 등 다양한 렌더링 방식을 지원합니다. 간결한 문법과 파일 기반 라우팅으로 개발자 경험이 뛰어나며, 다양한 배포 옵션과 유연한 상태 관리를 제공합니다. 결과적으로 빠른 로딩, 간편한 개발, 다양한 배포 방식을 통해 효율적인 풀스택 애플리케이션 개발이 가능합니다.



ChatGPT에게 시키기



“Svelte로 이 사진의 사이트를 만들고 싶어 코드를 작성해줘”

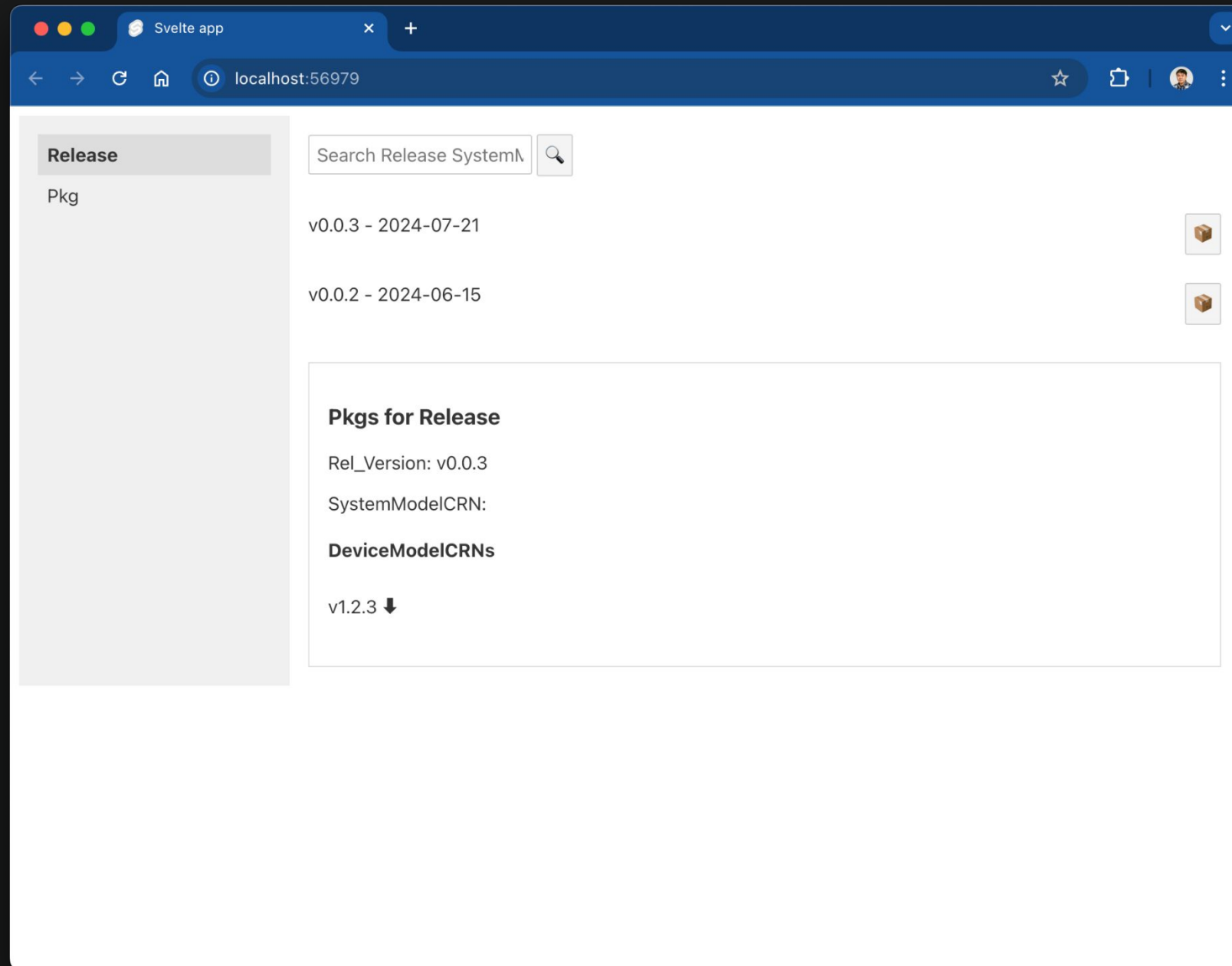


1. **Set Up the Project:** If you haven't set up a Svelte project yet, you can do so by running:

복사

Directory Structure

복사



A FEW MOMENTS LATER



OTA Explorer

intstagereal

Releases

about

System Model CRN to search OTA release...

Search

10 Items

1-10 of 10

CCP-Test-Shuttle-Only.v1.0.0-240809083800

SNAPSHOT

CCP-Test.AKit-McCoy.v0.0.0-240521

ID

117

System Model CRN

did:dm:42dot:system:mccoy::

Release Version

CCP-Test.AKit-McCoy.v0.0.0-240521

Packages

Device Model CRN: cid:dm:42dot:device:mccoy-ak7::

Package Version: CCP-Test.AKit-McCoy.v0.0.0-240521

ID

74

Path

binary/did:dm:42dot:system:mccoy::/cid:dm:42dot:device:mccoy-ak7::/42dot-image-shuttle-galactic-42dot-ak7_delta_20240521_CCP-Test.AKit-McCoy.v0.0.0-240521.tar.enc

Size

391833632 bytes

SHA256 Hash

47604668ddd884f38a33b1e90e18286f5b73ea4c8206871da62d05a465fbe90d

Download JSON

Download Package

Device Model CRN: cid:dm:42dot:device:mccoy-ak7rec::

Package Version: CCP-Test.AKit-McCoy.v0.0.0-240521

Release Note

No release note

Release date

2024-05-21T07:20:36.493609Z

CCP-Test.AKit-McCoy.v0.0.0-240520000002


CCP-Test.AKit-McCoy.v0.0.0-240520000001



CORS

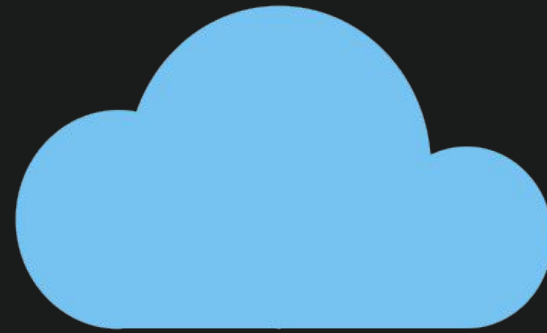
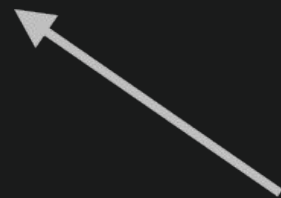
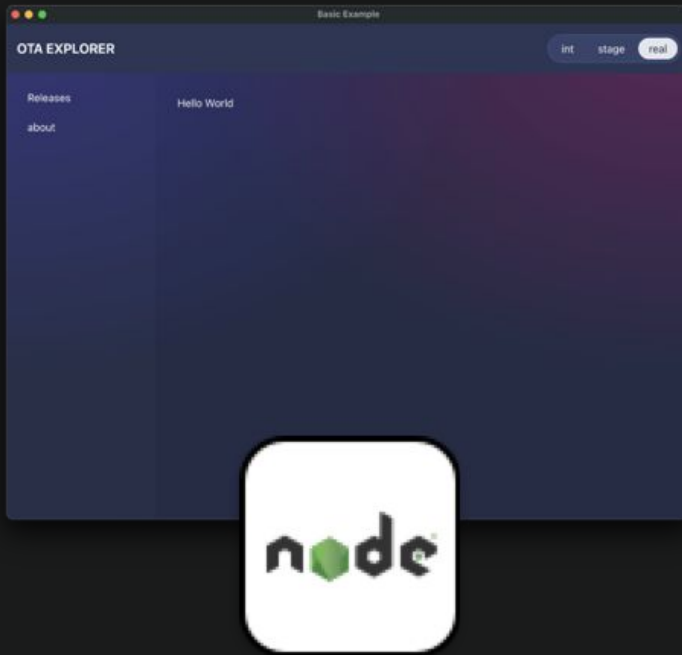


Cross-Origin Resource Sharing



CORS 에러는 브라우저가 서로 다른 도메인 간의 리소스 요청을 허용하지 않아서 발생하는 문제입니다. 이 에러는 주로 웹 애플리케이션이 다른 도메인, 프로토콜 또는 포트에서 리소스를 요청할 때 발생합니다.





임시방편 - 모든 도메인에서 요청을 허용


- pkg.go.dev
 - cors 검색



cors - Search Results - Go Pa x

pkg.go.dev/search?q=cors&m=

☆🔒🐈📦⬇️👤⋮

Why Go ▾LearnDocs ▾**Packages**Community ▾

cors

/ 🔍

Packages

Symbols

Showing 25 modules with matching packages. [Search help](#)

[cors](#) (github.com/rs/cors)

Package cors is net/http handler to handle CORS related requests as defined by <http://www.w3.org/TR/cors/>
Imported by [7,646](#) | v1.11.0 published on Apr 24, 2024 | [MIT](#)

[cors](#) (github.com/gin-contrib/cors)

Imported by [5,074](#) | v1.7.2 published on May 1, 2024 | [MIT](#)

[cors](#) (github.com/go-chi/cors)

cors package is net/http handler to handle CORS related requests as defined by <http://www.w3.org/TR/cors/> You can configure it by passing an option struct to cors.New: `c := cors.New(cors.Options{ AllowedOrigins: []string{"foo.com"}, AllowedMethods: []string{"GET", "POST", "DELETE"}, AllowCredentials: true, })` Then insert the handler in the chain: `handler = c.Handler(handler)` See [Options documentation](#) for more options.
Imported by [2,306](#) | v1.2.1 published on Apr 19, 2022 | [MIT](#)

[cors](#) (github.com/astaxie/beego/plugins/cors)

Package cors provides handlers to enable CORS support.
Imported by [466](#) | v1.12.3 published on Nov 3, 2020 | [Apache-2.0](#)

[cors](#) (github.com/gofiber/fiber/v3/middleware/cors)

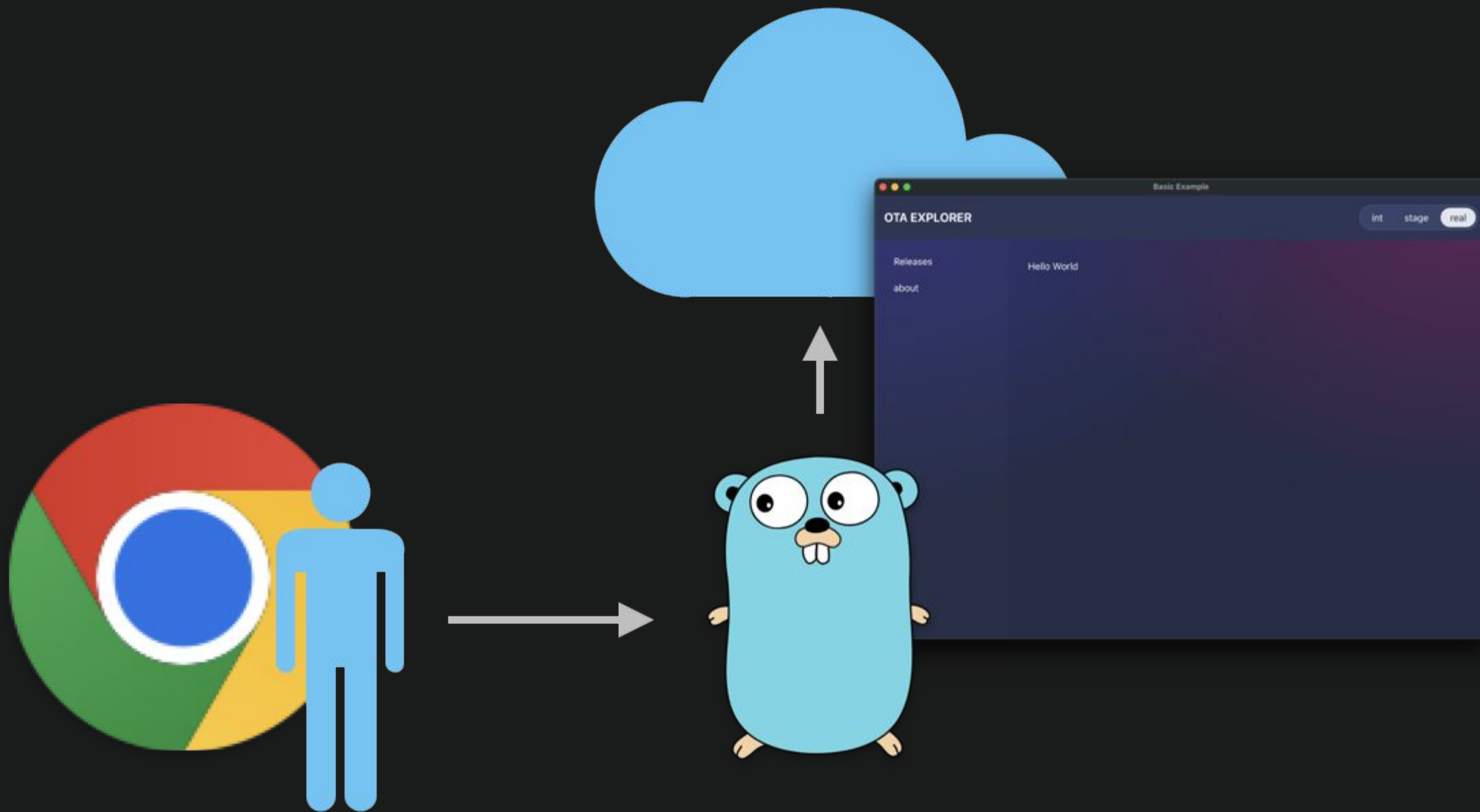
Imported by [22](#) | v3.0.0-beta.3 published on Jun 30, 2024 | [MIT](#)
Other major versions: [v2](#)

[gin](#) (github.com/rs/cors/wrapper/gin)



embed





```
//go:embed all:fe_build
```

```
var feBuild embed.FS
```

```
...
```

```
fe, err := fs.Sub(feBuild, "fe_build")
```

```
...
```

```
mux.Handle("/", http.FileServer(http.FS(fe)))
```

```
...
```





webview



```
import webview "github.com/webview/webview_go"

...

go func() {
    http.ListenAndServe(fmt.Sprintf(":%d", port), handler)
}()

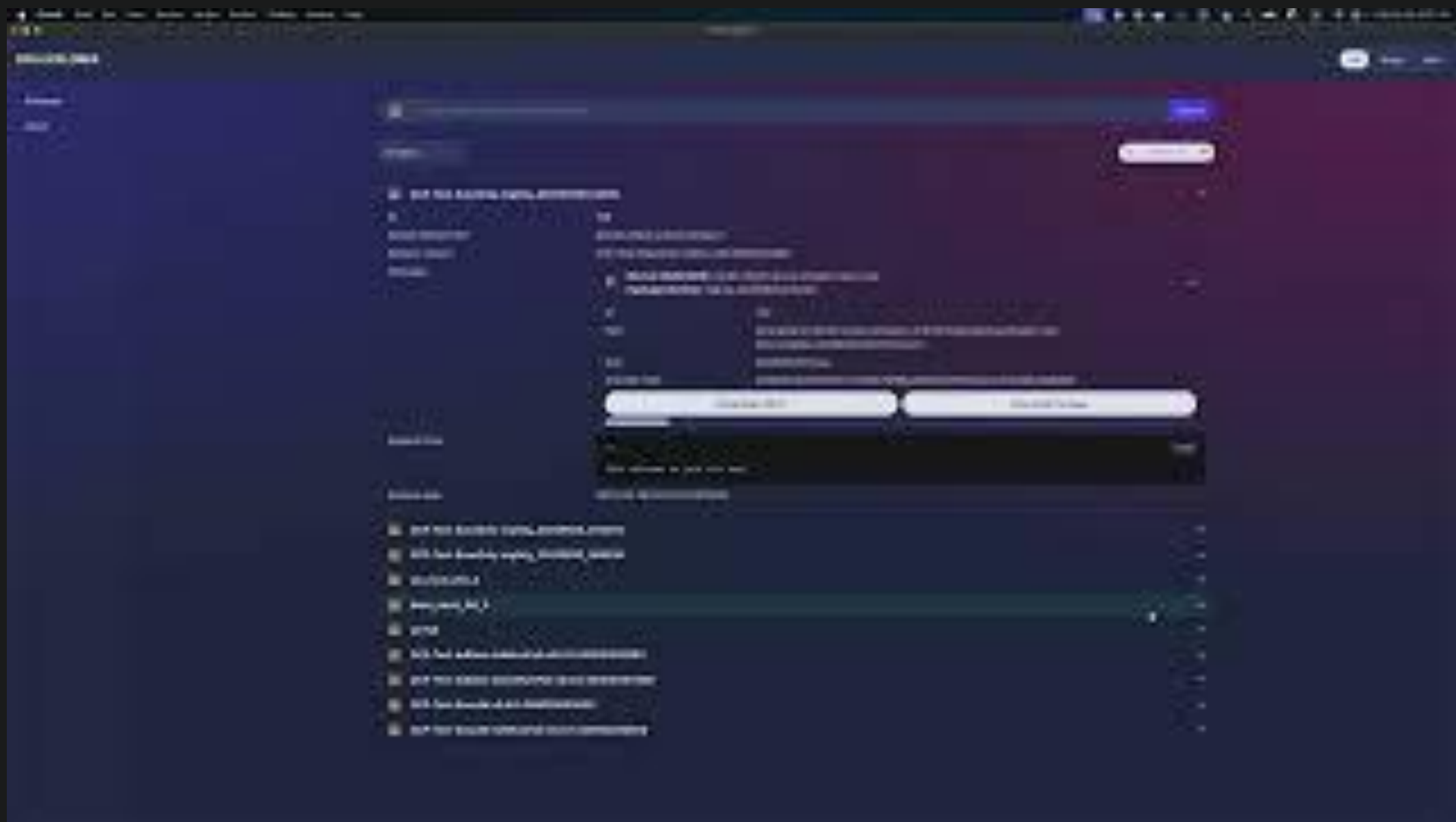
w := webview.New(false)
defer w.Destroy()
w.SetTitle("OTA Explorer")
w.SetSize(1024, 768, webview.HintNone)
w.Navigate(fmt.Sprintf("http://127.0.0.1:%d", port))
w.Run()
```





Live Demo







WAILS



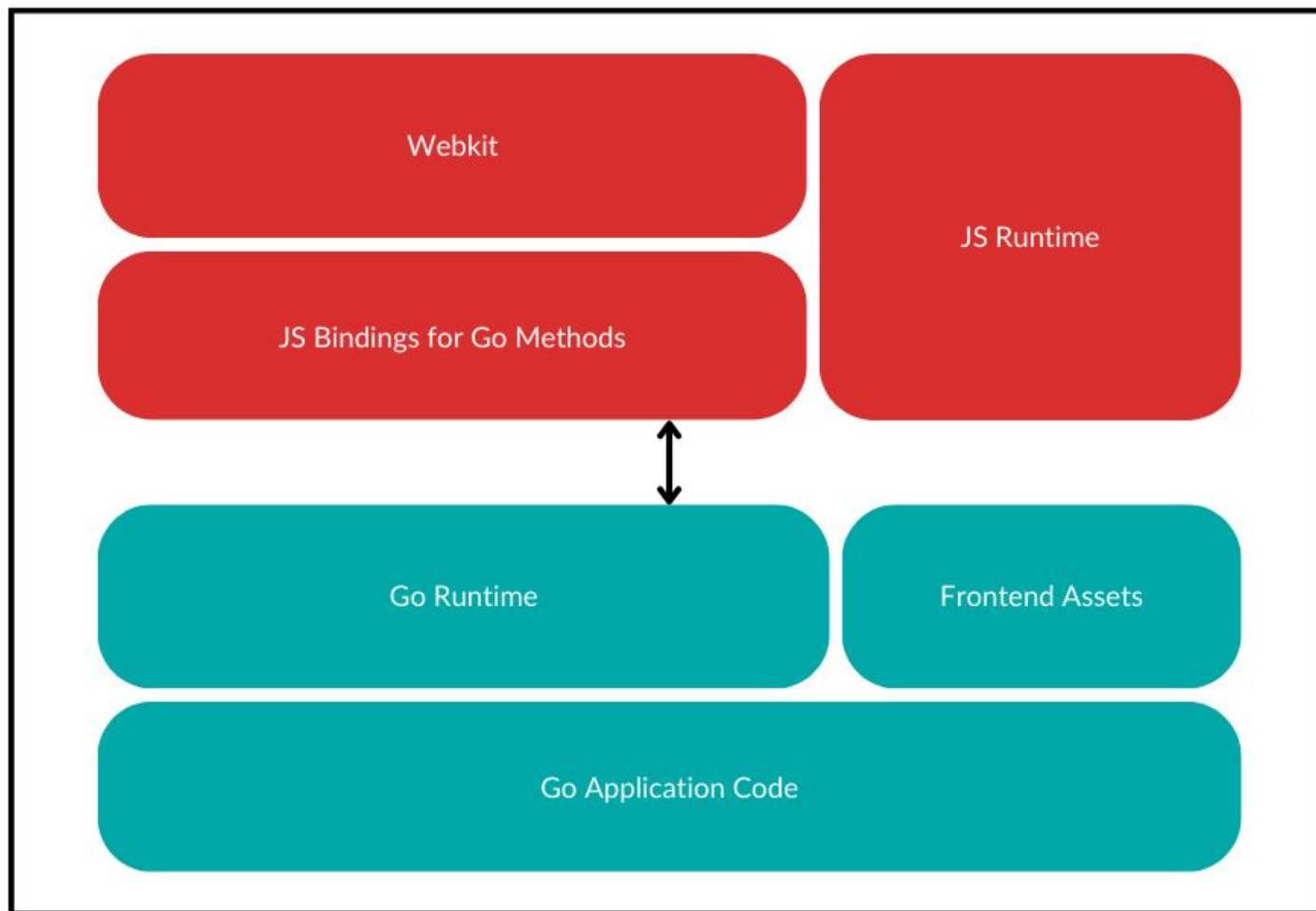
WAILS

Build beautiful cross-platform applications using Go

- <https://wails.io/>



Components of a Wails App



```
go install github.com/wailsapp/wails/v2/cmd/wails@latest
```

```
wails init \
```

```
-g -ide vscode -q \
```

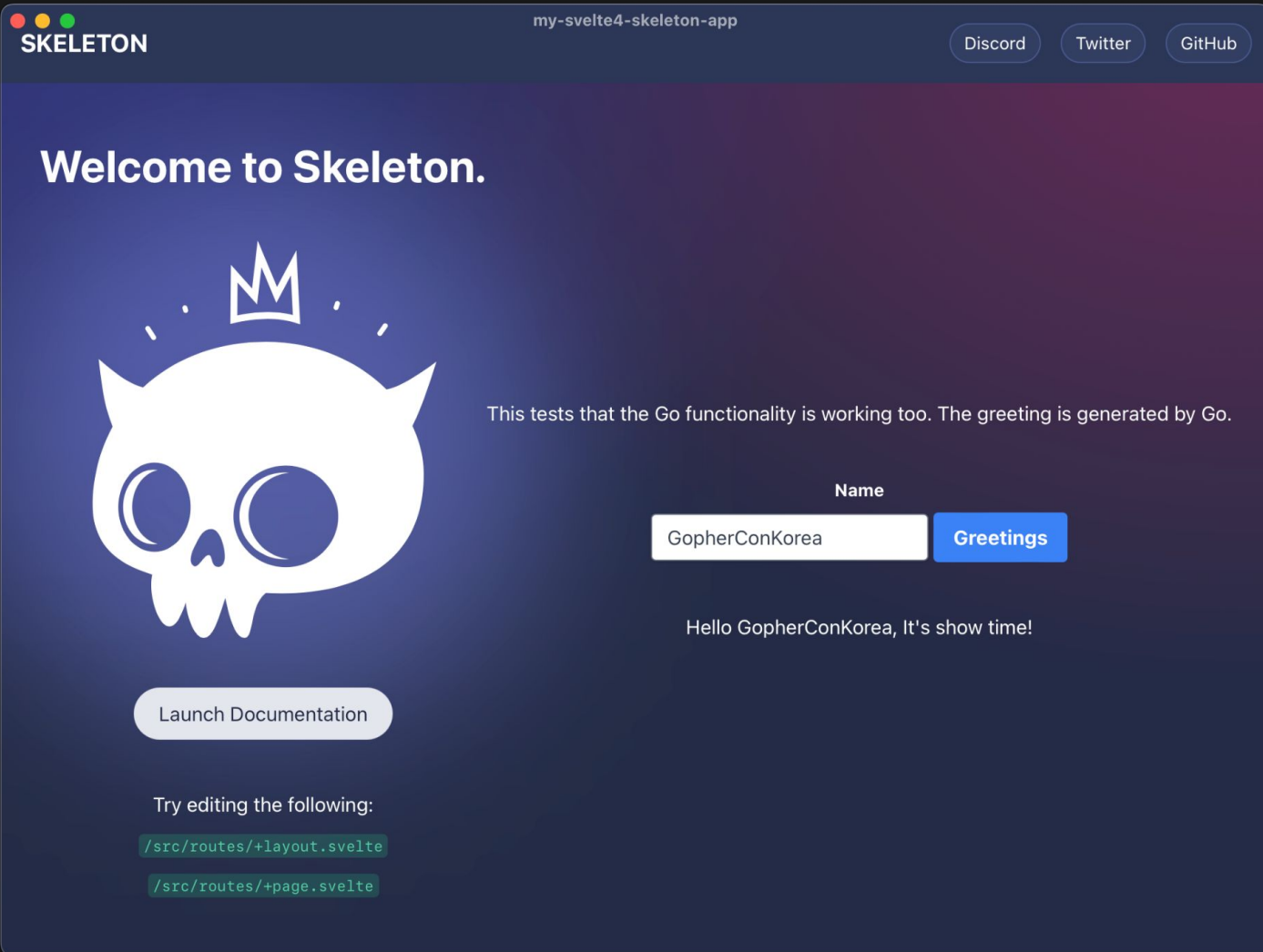
```
-n myproject \
```

```
-t https://github.com/suapapa/wails-svelte4-skeleton-template
```

```
cd myproject
```

```
wails dev
```







회고



Go 사용 회고

- 높은 생산성으로 안전한 프로그램을 두루 개발 할 수 있음.
- 기본 패키지로 암호화 패키지가 있음.
- 단일 파일로 빌드 되서 좋음.
- 새 버전에 추가되는 기능들은 잘 안 쓰게 됨.



Q&A



Thank you!

