C🍪🍪KIE-APP

Convergent Capstone Design 1
9th Week Progress Report

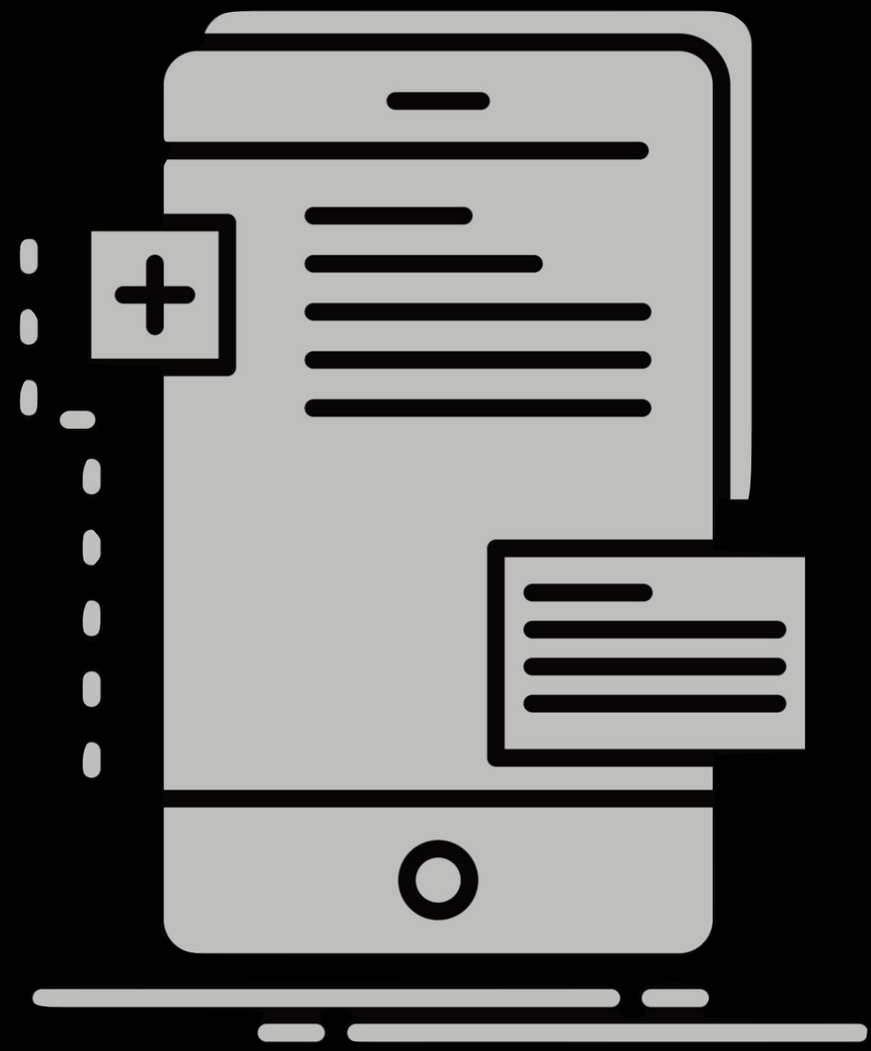
Group 5 Park JongBeum & Baek SeungHeon, April 25th 2023

Recall

Front End

What we did last week

- Add App Icon
- Create Sign-In Page
- Create Sign-Up Page
- Request Device Permission
- Improve UI



iPhone 14 Pro Max
iOS 16.4

3:01

iPhone 14 Pro Max
iOS 16.4

12:43

DEBUG

아이디

testtest

8/30

비밀번호

.....

11/30

로그인

회원가입

iPhone 14 Pro Max
iOS 16.4

12:43

DEBUG

No Images

Select Image

아이디

최소 6자 이상 입력해주세요. 0/30

비밀번호

최소 10자 이상 입력해주세요. 0/30

비밀번호 확인

비밀번호가 일치합니다. 0/30

이름

최소 1자 이상 입력해주세요. 0/10

생년월일

전화번호 ('-' 없이 입력)

0/11

Sign up

iPhone 14 Pro Max
iOS 16.4

12:51

COOKIE

Connected

김채원 안녕

김채원 ㅎㅇ

김채원 ㅎㅇㅎㅇ

김채원 ㅋㅋㅋㅋㅋ

김채원 😀😀😀😃😃😄😄😄😄

김채원 🍪🍪🍪🍪🍪

Type your message...

I | The | I'm

q w e r t y u i o p

a s d f g h j k l

z x c v b n m

123 space done

iPhone 14 Pro Max
iOS 16.4

12:43

COOKIE

DEBUG

박종범 백승헌 Jane

JB cw1 cw2

cw3 cw4 cw5

Friends

iPhone 14 Pro Max
iOS 16.4

12:45

COOKIE

Carmel Park Apartments

웨스트 홈스태드 로드

Safeway 식료품점

노스포인트 Northpoint

쿠퍼티노 호텔 The Cupertino

Appliance Express Repair

주니페로 세라 프리웨이

블릭 스토리지 Public Storage

Apple

IL2

Apple Infinite Loop 전자제품 판매점

De Anza 12

Mariani Three 주차장

Sam H. Lawson Middle School 중학교

데 안자 3 De Anza 3 (DA3)

Lawson Middle School Tennis Courts 테니스장

Track

Dance Studio 댄스학원

Donut Wheel 도넛 전문점

Google

Location

Back End

What we did last week

- Launch Test Server
- Account API & DB
    - Sign-In
    - Sign-Up
    - Existence of Account

Account API & DB

/account/signup
/account/signin
/account/exists

cookie_server - test_account

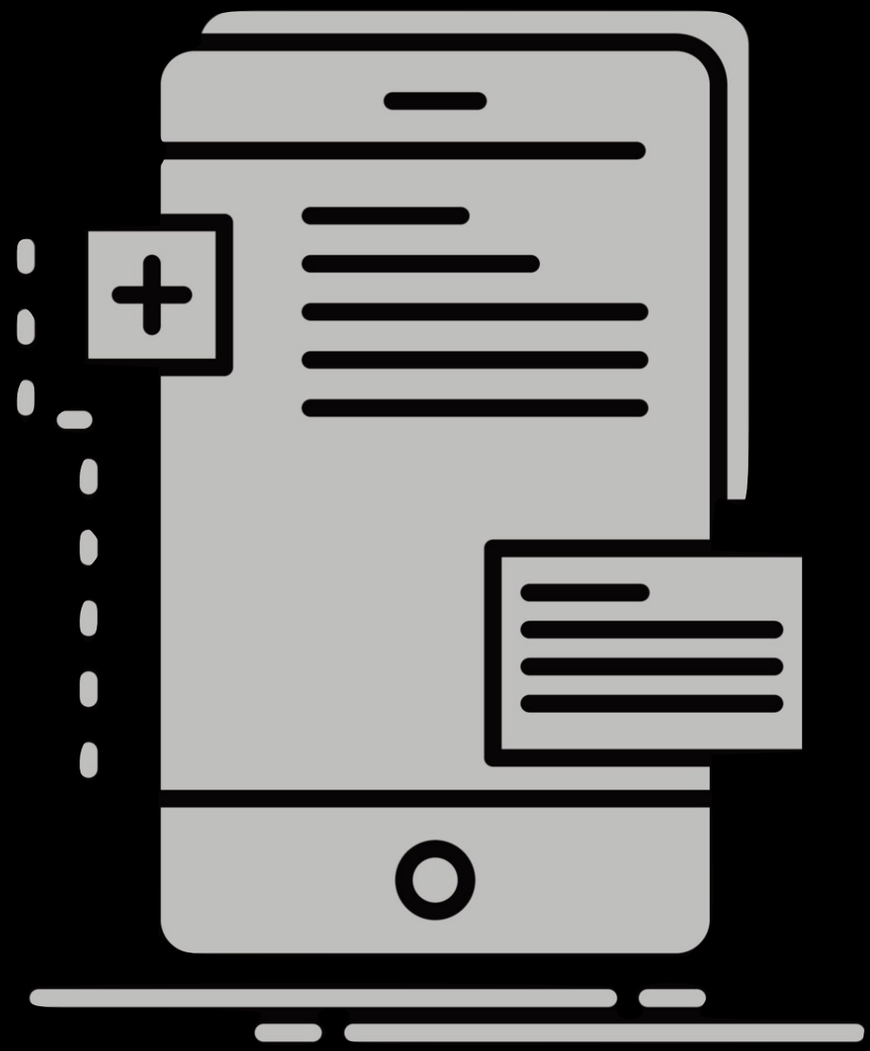

```
{
  "_id": {
    "$oid": "6432463eb9cf0924039d4777"
  },
  "userid": "testtest",
  "password": "8d9124b80290dfd92a1ececb45c7d6555c5fe06c3913a7edb4666ed1a50af6c5",
  "username": "안녕",
  "birthday": {
    "$date": "2022-02-02T00:00:00.000Z"
  },
  "phone": "01000000000",
  "profile": {
    "image": "https://i.imgur.com/1Q9ZQ9r.png",
    "message": "Hello, I'm new here!"
  },
  "friendList": [],
  "chatList": [],
  "createdAt": {
    "$date": "2023-04-09T04:59:42.920Z"
  },
  "updatedAt": {
    "$date": "2023-04-09T04:59:42.920Z"
  },
  "__v": 0
}
```

Frontend

Front End

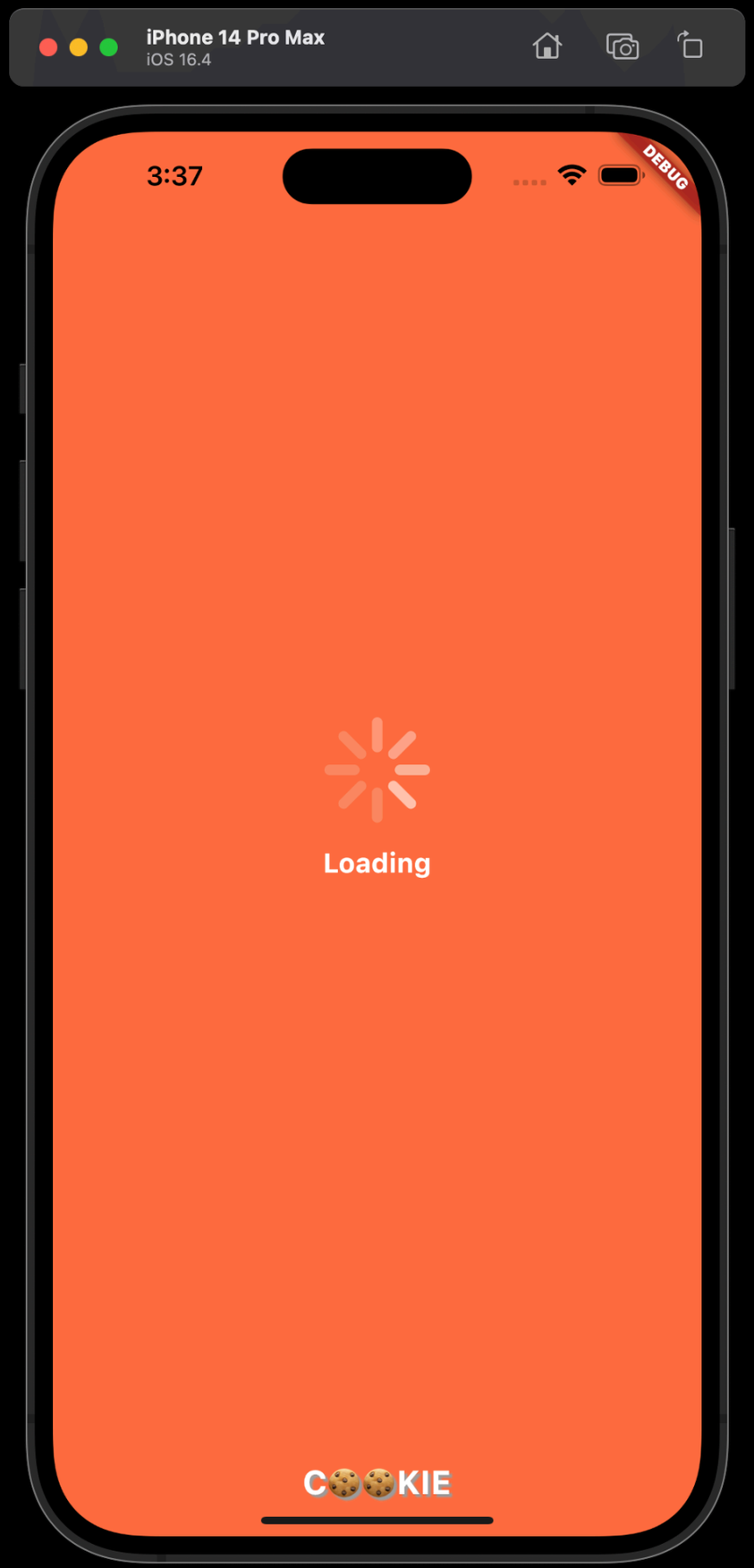
What Our Team Have Done

- Auto login
- Chat history tab
- Settings tab
- Improve UI



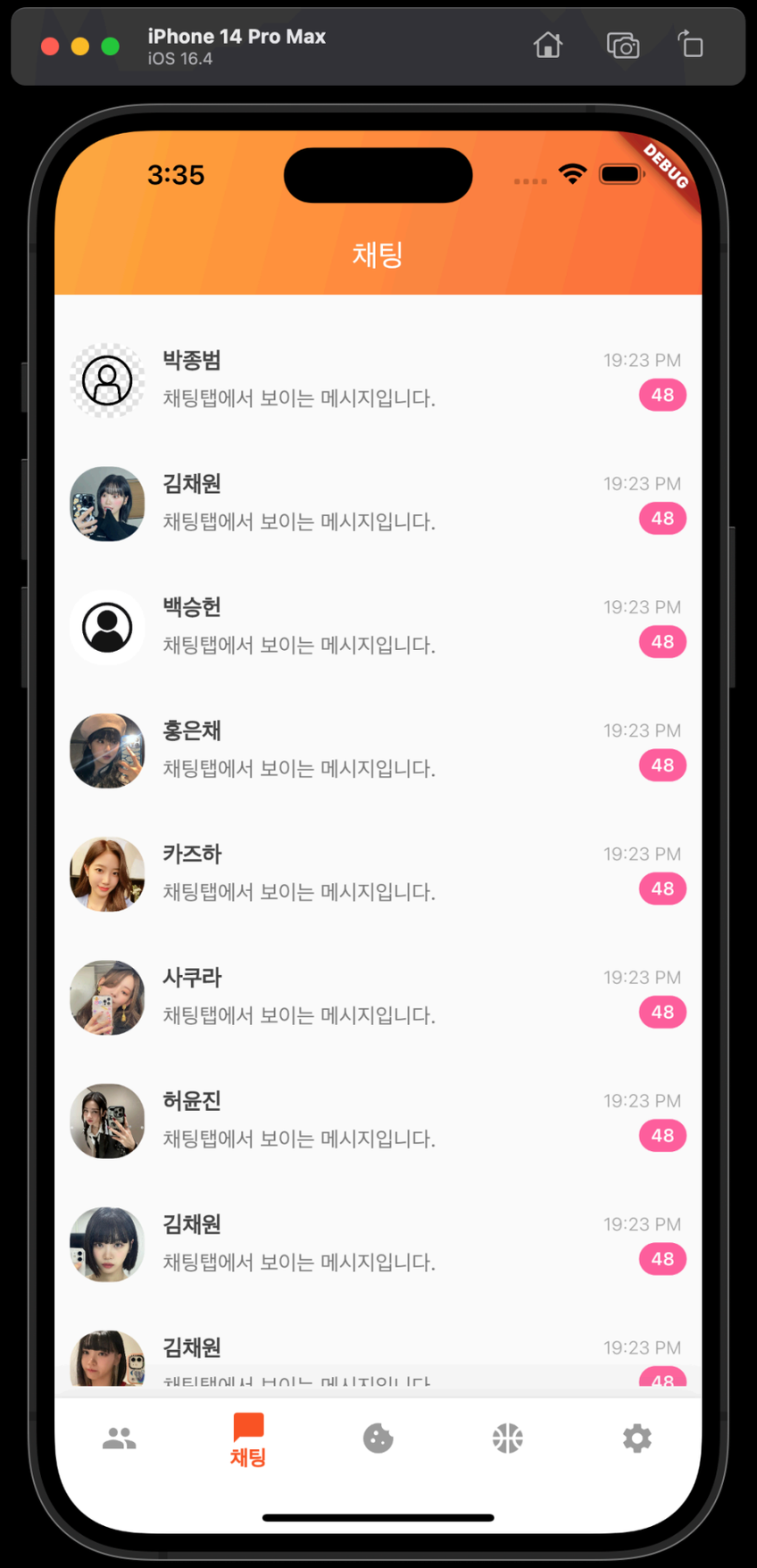
Auto login

- Flutter secure storage
  - Encrypts data
  - Very simple
- Adding a loading screen
  - Check your login information



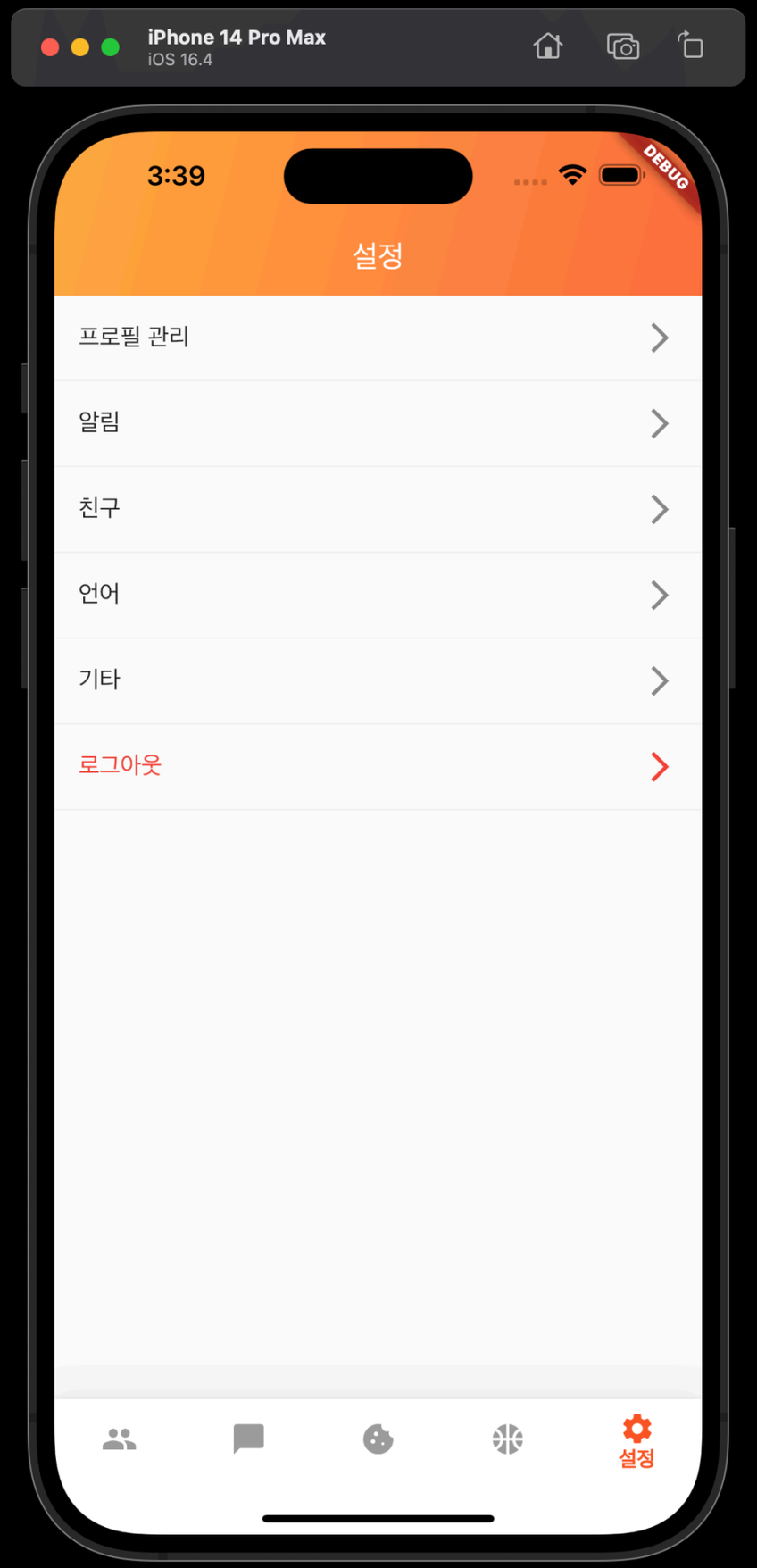
Chat history tab

- Show a record of a conversation with friends
  - Use the ListView
  - Last conversation history
  - Number of unread messages
  - etc.



Setting tab

- Various functional controls
  - Personal profile settings
  - Logout function
  - More to come



iPhone 14 Pro Max
iOS 16.4

3:35

DEBUG

설정

프로필 관리

알림

친구

언어

기타

로그아웃

로그아웃

정말로 로그아웃 하시겠습니까?

아니오 예

설정

iPhone 14 Pro Max
iOS 16.4

2:46

DEBUG

프로필 관리

이름
홍길동

상태메시지
안녕하세요. 홍길동입니다.

전화번호
profiles['phonenumber']

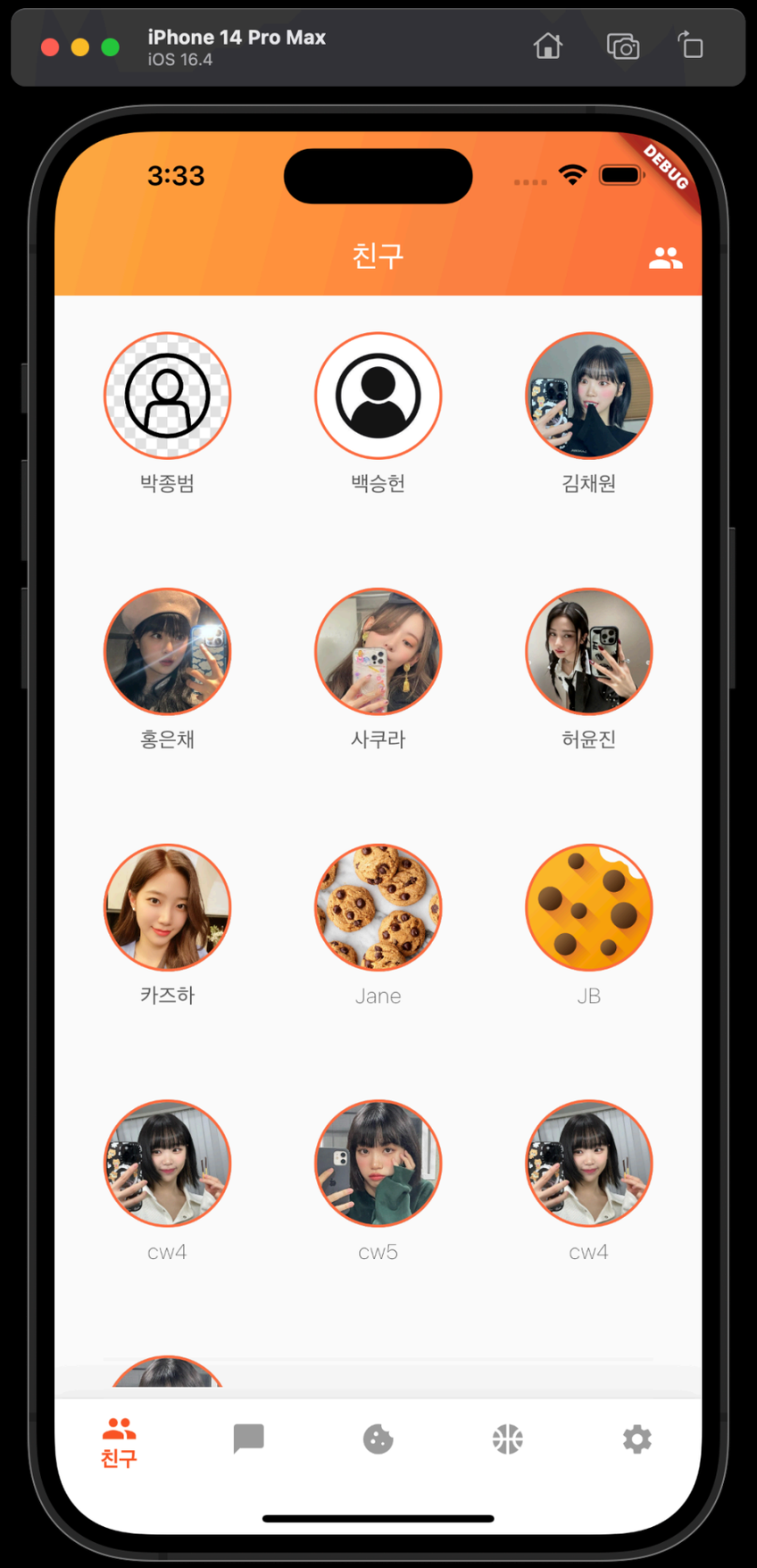
이름
홍길동

이름
홍길동

이름
홍길동

UI Improvements

- Continue to develop
  - Friend tab
    - Friend profile
    - Bottom sheet
  - Navigation bar
  - Chat bubble

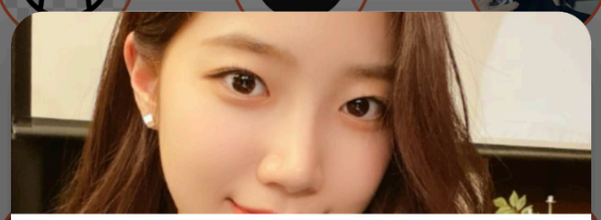


iPhone 14 Pro Max
iOS 16.4

3:33

DEBUG

친구



user.status_message

이름
카즈하

생일
user.birthday

거주지
user.address

나이
user.age

확인

친구

iPhone 14 Pro Max
iOS 16.4

3:35

DEBUG

친구

박종범

백승헌

김채원

홍은채

사쿠라

허윤진

친구관리

알림

개인정보

도움말

도움말

도움말

iPhone 14 Pro Max
iOS 16.4

2:47

DEBUG

카즈하

연결 안됨

카즈하
안녕하세요

카즈하
채팅 페이지 테스트입니다

카즈하
대화를 원할 경우 마침표로 대화를 마무리하세요

Type your message...

Backend

Back End

What Our Team Have Done

- HTTPS
- JSON Web Token
- socket.io changes..
  - Session
  - Rooms
  - More events
  - Admin Page

HTTPS & SSL/TLS

개인정보 보호법 시행령
제30조(개인정보의 안전성 확보 조치)
① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.
3. 개인정보를 안전하게 저장 · 전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치

Application Layer

HTTP

FTP

NNTP

XMPP

Handshake Layer

SSL / TLS

Record Layer

HandShake

HandShake

HandShake

Record

Transport Layer

TCP/IP

https://www.lesstif.com/ws/ssl-tls-https-43843962.html

Let’s Encrypt

- Certificate Authority (CA)
- Auto renew (every 90 days) via certbot
- *.parkjb.com wildcard subdomain support
- **Free!**

ssllabs.com

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > parkjb.com

SSL Report: parkjb.com (211.243.126.115)

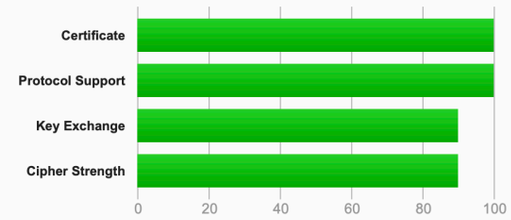
Assessed on: Mon, 24 Apr 2023 15:44:20 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A+



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.3.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

DNS Certification Authority Authorization (CAA) Policy found for this domain. MORE INFO »

Certificate #1: EC 256 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	parkjb.com Fingerprint SHA256: e34db6046f3f363c2c6d75b6e573aca571ece8a361dc9e8d6ea4e41aacccf3cf Pin SHA256: Y59oWURf7lrd6moqDurcp9Snrn3+jYZwj4VUo3ygM5k=
Common names	parkjb.com
Alternative names	*.parkjb.com parkjb.com
Serial Number	046c3e58924af4b46995444ed5042eeebc98
Valid from	Sun, 16 Apr 2023 15:19:40 UTC
Valid until	Sat, 15 Jul 2023 15:19:39 UTC (expires in 2 months and 20 days)
Key	EC 256 bits
Weak key (Debian)	No
Issuer	R3 AIA: http://r3.i.lencr.org/
Signature algorithm	SHA256withRSA

Qualys SSL Labs A+ Rated

ssllabs.com

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > test.parkjb.com

SSL Report: test.parkjb.com (211.243.126.115)

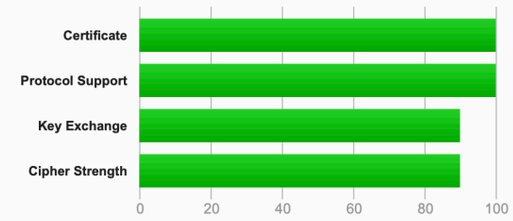
Assessed on: Mon, 24 Apr 2023 18:22:07 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A+



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.3.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

DNS Certification Authority Authorization (CAA) Policy found for this domain. MORE INFO »

Certificate #1: EC 256 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	parkjb.com Fingerprint SHA256: e34db6046f3f363c2c6d75b6e573aca571ece8a361dc9e8d6ea4e41aacccf3cf Pin SHA256: Y59oWURf7lrd6moqDurcp9Snrn3+jYZwj4VUo3ygM5k=
Common names	parkjb.com
Alternative names	*.parkjb.com parkjb.com
Serial Number	046c3e58924af4b46995444ed5042eeebc98
Valid from	Sun, 16 Apr 2023 15:19:40 UTC
Valid until	Sat, 15 Jul 2023 15:19:39 UTC (expires in 2 months and 20 days)
Key	EC 256 bits
Weak key (Debian)	No
Issuer	R3 AIA: http://r3.i.lencr.org/
Signature algorithm	SHA256withRSA

Qualys SSL Labs A+ Rated

ssllabs.com

JSON WEB TOKEN

Authentication

Are you the real “testtest” user?

Authorization

Is this operation (read, write, send message etc.) permitted to “testtest” user?


```
{
    "success": true,
    "account": {
        "_id": "6432463eb9cf0924039d4777",
        "userid": "testtest",
        "phone": "01000000000"
    }
}
```


{
"success": true,
"account": {
"_id": "6432463eb9cf0924039d4777",
"userid": "testtest",
"phone": "01000000000"
},
"token":
Header
Payload
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiI2N
DMyNDYzZWI5Y2YwOTI0MDM5ZDQ3NzciLCJ1c2VyaWQiOiJ0ZXN0
dGVzdCIsInVzZXJuYW1lIjoi7JWI64WVIiwiaWF0IjoxNjgyMzU
xNjMzLCJleHAiOjE2ODI5NTY0MzMsImlzcyI6InRlc3QucGFya2
piLmNvbSIsInN1YiI6InVzZXJJbmZvIn0.r3-o6R-
1f8vSvZnENA-gOF0eFbgyj7Q140u7uNk7RhM"
Signature
}

Algorithm HS256

Encoded PASTE A TOKEN HERE

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiI2NDMyNDYzZWI5Y2YwOTI0MDM5ZDQ3NzciLCJ1c2VyaWQiOiJ0ZXN0dGVzdCIsInVzZXJuYW1lIjoi7JWI64WVIiwiaWF0IjoxNjgyMzUxNjMzLCJleHAiOjE2ODI5NTY0MzMsImlzcyI6InRlc3QucGFya2piLmNvbSIsInN1YiI6InVzZXJJbmZvIn0.r3-o6R-1f8vSvZnENA-gOF0eFbgyj7Q140u7uNk7RhM

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE


```
{
  "alg": "HS256",
  "typ": "JWT"
}
```


PAYLOAD: DATA


```
{
  "_id": "6432463eb9cf0924039d4777",
  "userid": "testtest",
  "username": "안녕",
  "iat": 1682351633,
  "exp": 1682956433,
  "iss": "test.parkjb.com",
  "sub": "userInfo"
}
```


VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  256bit SECRET KEY
) secret base64 encoded
```

⊗ Invalid Signature

SHARE JWT

JWT

Header

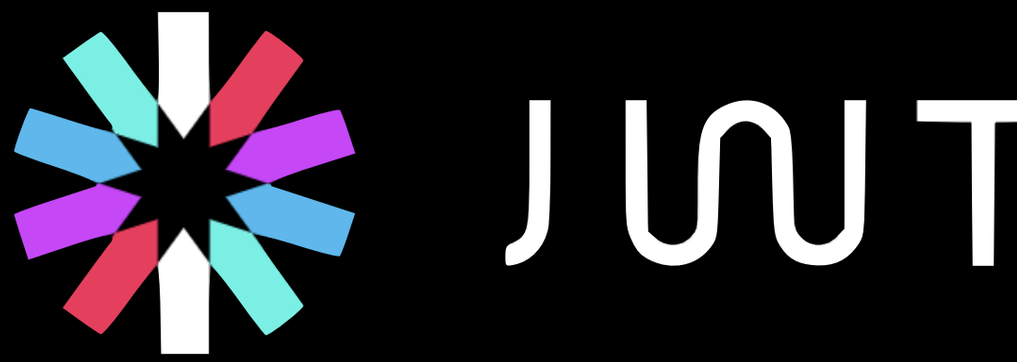
- alg: signature or encryption algorithm
- typ: type of token

JOLT

JWT

Payload

- Any payloads needed (ex. User info)
- sub: whom the token refers to
- iat: Issued at
- exp: expired at
- iss: Issuer (who created and signed)
- And more… (ex. aud, nbf, jtl)



JWT
Signature

- HMACSHA256(

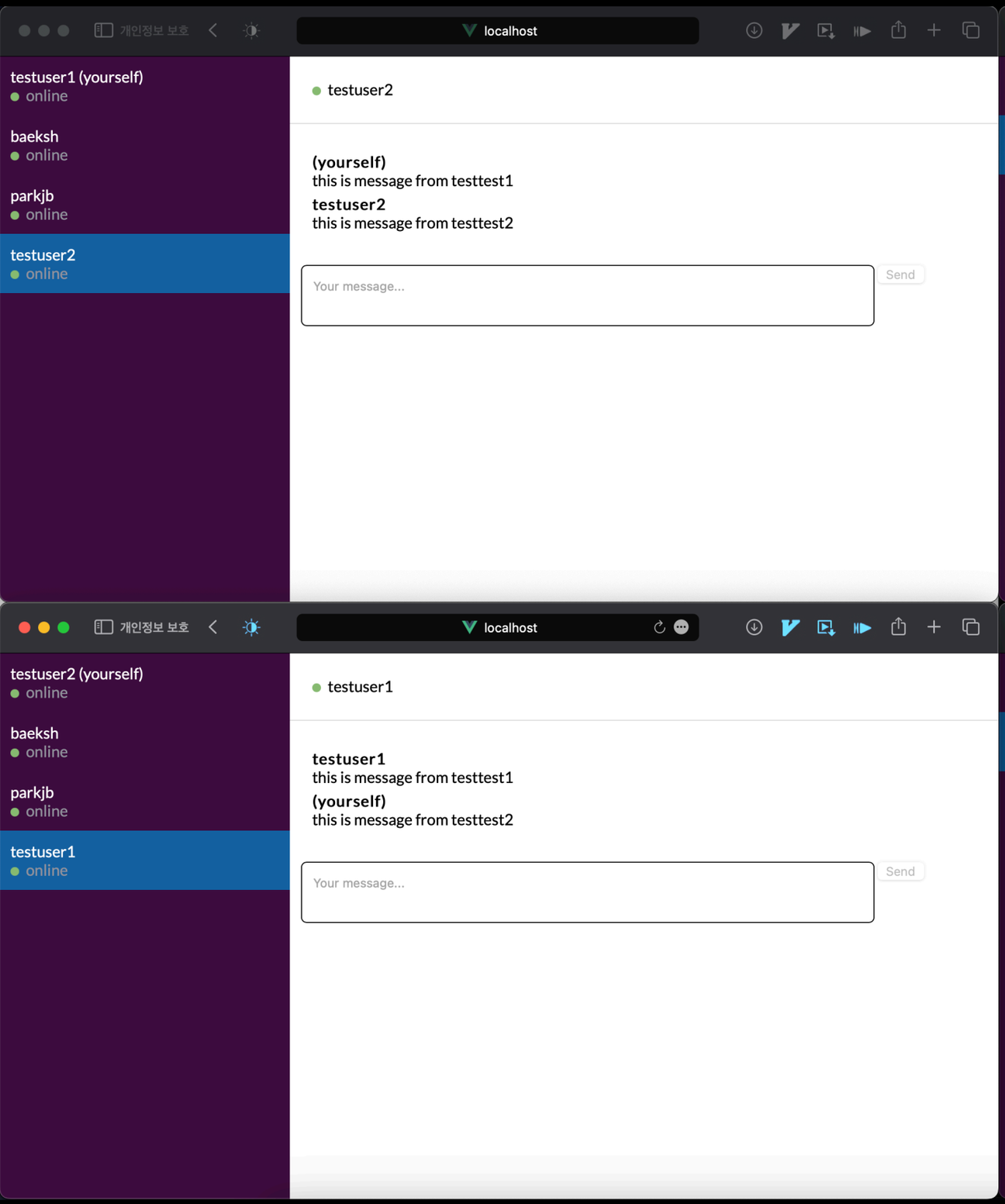
  <header>.<payload>,

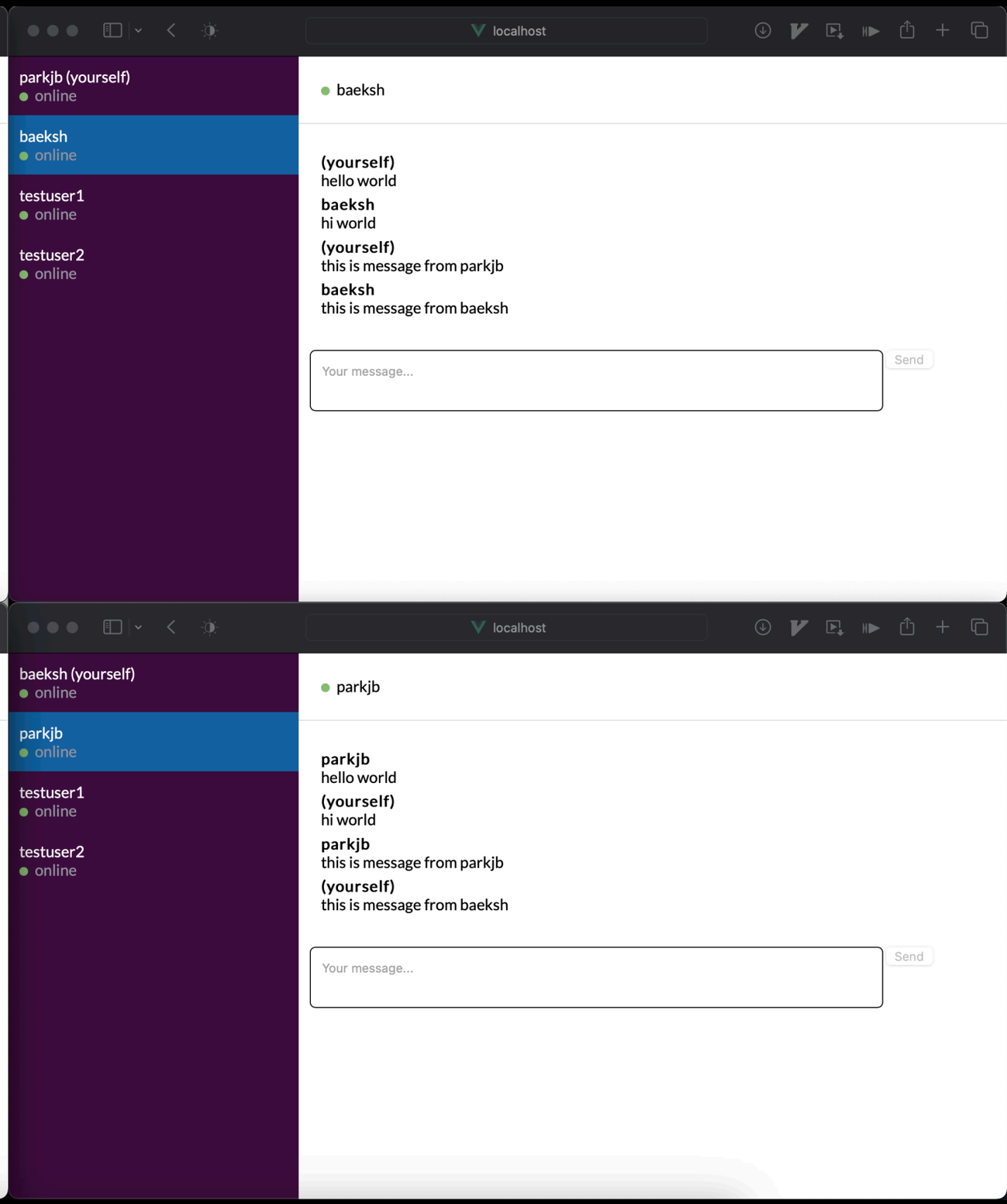
  <secret key>

)

JOLT

socket.io


localhost
testuser1 (yourself)
online
baeksh
online
parkjb
online
testuser2
online
testuser2
(yourself)
this is message from testtest1
testuser2
this is message from testtest2
Your message...
Send


localhost
parkjb (yourself)
online
baeksh
online
testuser1
online
testuser2
online
baeksh
(yourself)
hello world
baeksh
hi world
(yourself)
this is message from parkjb
baeksh
this is message from baeksh
Your message...
Send

localhost
testuser2 (yourself)
online
baeksh
online
parkjb
online
testuser1
online
testuser1
testuser1
this is message from testtest1
(yourself)
this is message from testtest2
Your message...
Send

localhost
baeksh (yourself)
online
parkjb
online
testuser1
online
testuser2
online
parkjb
parkjb
hello world
(yourself)
hi world
parkjb
this is message from parkjb
(yourself)
this is message from baeksh
Your message...
Send

admin.socket.io

Socket.IO Admin UI 0.5.1

Server URL: test.parkjb.com
Status: CONNECTED

UPDATE

- Dashboard
- Sockets
- Rooms
- Clients
- Events
- Servers

Language: English

Dark theme?

Read-only?

Dashboard

Clients

Transport	#
WebSocket	2 100.0 %
HTTP long-polling	0 0.0 %

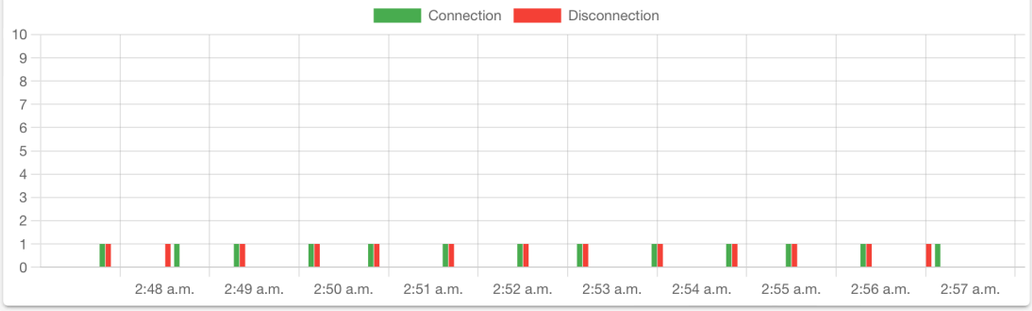
Servers

Status	#
HEALTHY	1 100.0 %
UNHEALTHY	0 0.0 %

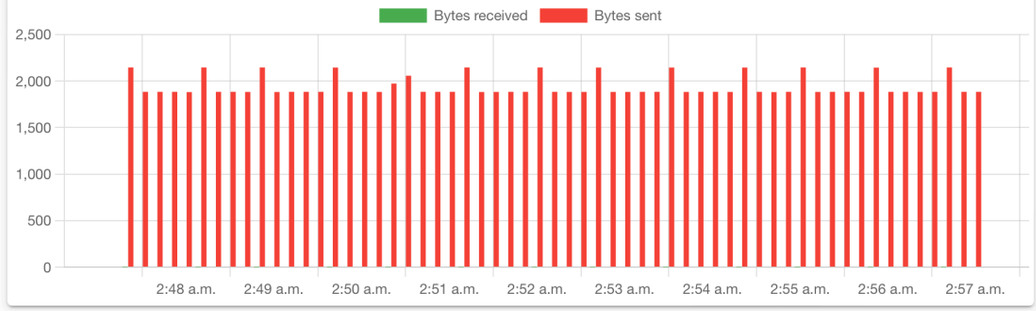
Namespaces

Name	# of sockets
/	0
/admin	1

Connection and disconnection events



Bytes received and sent



socket.io admin page

Thank You

Questions are welcome