

# Full Stack Development at KaJi Inc.



FULL-STACK DEVELOPMENT



## Challenges

- Minimal experience with C#, .NET and MongoDB
- First time creating HTTP responses, requests and REST APIs
- Learning HTML, JavaScript, CSS and the Vue framework
- No documentation for existing code
- Most of existing code written by interns who are no longer at KaJi Inc.
- Working in isolation, limited availability for help

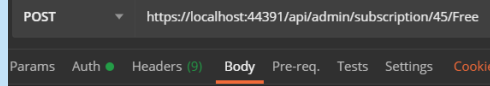
## Conclusion

- Achieved skills in building REST APIs
- Gained an understanding of programming with HTTP
- Learned frontend development in depth
- Experienced identifying and patching authorization vulnerabilities
- Practiced working with other peoples' code
- Conquered a long self-learning and self-discipline challenge
- Overall programming skills and analysis skills sharpened

## Features and Implementation

Tour company creates a subscription

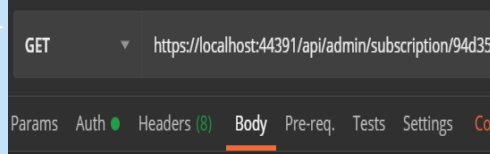
Calls POST API with company ID and subscription type in route parameters



Returns ID of new subscription

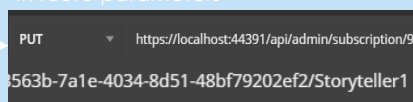
Display subscription with ID in response

Calls GET API with ID in route parameter



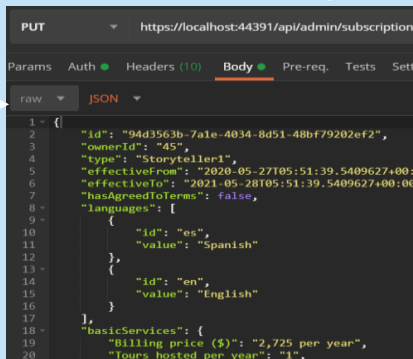
Tour company upgrades subscription for more services

Calls PUT API with ID and subscription type in route parameters



KaJi admin directly edits fields for subscription

Calls PUT API with JSON in body



New authorization layer is achieved through getting user ID and join type queries. It patches the following vulnerabilities which I discovered through testing:

- Escalation of privilege
- Denial of service
- Information disclosure
- Losing data integrity



## Overview

### KaJi Inc.

- Startup for virtual tours in Seattle
- Tours are hosted on mobile app
- Tour companies create and manage tours on website portal

### Problem

- Tour companies have different types of subscriptions that give access to tour hosting service
- Need to create data models for companies' subscriptions
- Need to create REST APIs to manage subscriptions
- Need to add user interface to website to access APIs
- Need to add an extra layer of authorization in all existing APIs

## Software/Tools

