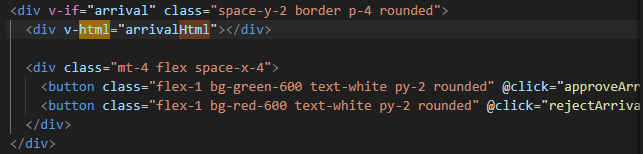
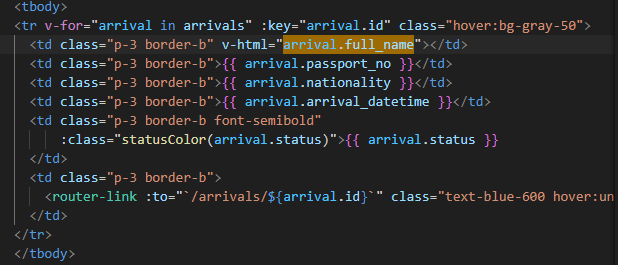
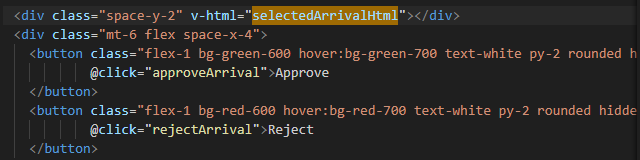
## Bug List

1. **XSS (Cross Site Scripting) – v-html**  
   *Rootcause*  
   Ditemukan penggunaan v-html di:

* Dashboard.vue (v-html="arrival.full\_name", v-html="selectedArrivalHtml")
* ArrivalDetail.vue (v-html="arrivalHtml")  
    
    
  *Impact*  
  Jika data yang di-render berasal dari user tanpa sanitasi, sangat rentan XSS.

Patch: Gunakan library sanitasi seperti DOMPurify sebelum assign ke variabel yang di-render dengan v-html.

Tambahkan import DOMPurify from "dompurify"; dan   
this.arrivalHtml = DOMPurify.sanitize(rawHtml); pada script

A black background with text

AI-generated content may be incorrect.

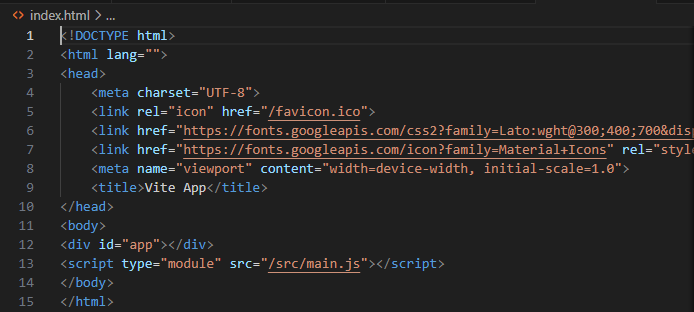
A screen shot of a computer code

AI-generated content may be incorrect.

A screen shot of a computer program

AI-generated content may be incorrect.

1. **Mixed Content**

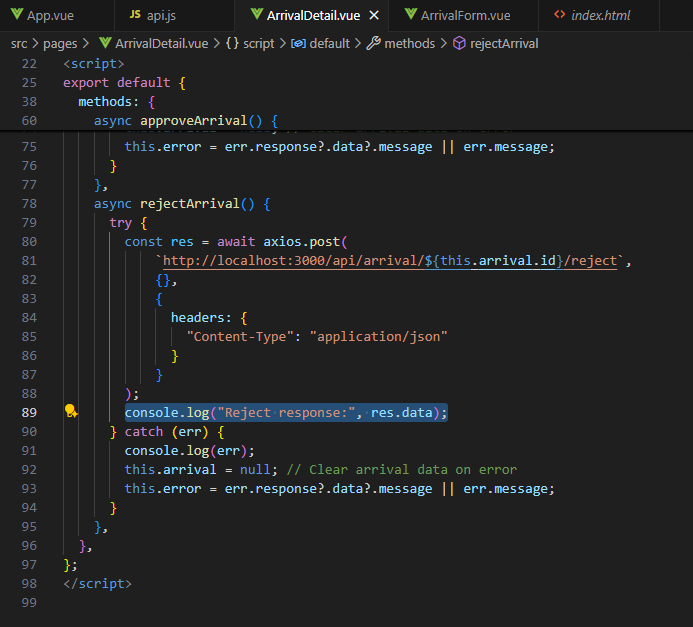
*Rootcause:*  
Tidak ada pengaturan CSP di frontend.Tidak ada meta tag <meta http-equiv="Content-Security-Policy" ...> di file HTML utama (index.html).  
  
*Impact:*

* Aplikasi lebih rentan terhadap serangan XSS (Cross-Site Scripting), karena browser tidak membatasi sumber script, style, atau resource lain yang boleh dijalankan.
* Attacker bisa lebih mudah menyisipkan/meng-inject script berbahaya dari domain luar, baik melalui input user, third-party script, atau dependency yang tidak aman.
* Potensi pencurian data user, pengambilalihan session, deface halaman, atau penyebaran malware meningkat.
* Sulit mendeteksi dan membatasi domain jahat yang mencoba menyisipkan konten/script ke aplikasi Anda.

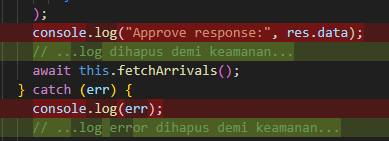
Patch: Tambahkan CSP yang ketat, minimal default-src 'self'.  
A computer screen shot of a computer code

AI-generated content may be incorrect.

1. **Improper Error Handling**

Rootcase: Pastikan error detail tidak ditampilkan ke user di production.  
  
Kode di atas akan menampilkan isi variabel error secara langsung ke user jika terjadi error. Jika isi error berasal dari response backend yang berisi detail teknis (misal: stack trace, pesan error internal), maka detail tersebut bisa terlihat oleh user.

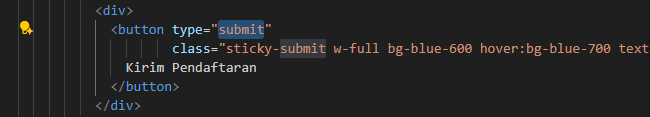
*Impact:*  
Informasi sensitif (data user, response API, error detail) bisa terlihat di browser console oleh siapa saja, termasuk attacker. Bisa membocorkan struktur data, flow aplikasi, atau bahkan credential jika tidak sengaja di-log.

Patch: delete console log  


1. **Submit Button Validation**

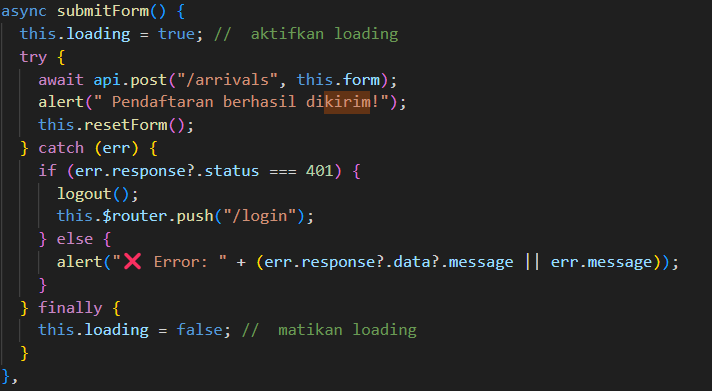
*Rootcause:*

Tidak ada atribut :disabled atau binding ke state loading, sehingga tombol bisa diklik berkali-kali selama proses submit berlangsung.



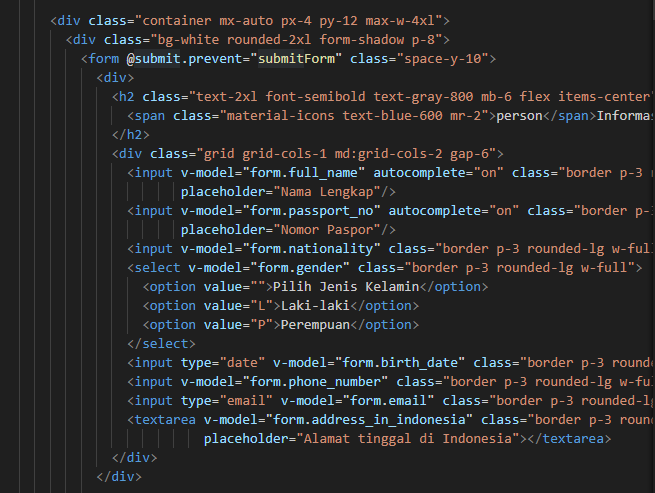
*Impact:*

* User bisa klik submit berkali-kali, sehingga data bisa terkirim ke backend lebih dari satu kali (double submit).
* Bisa menyebabkan data ganda di database (misal: pendaftaran dobel).
* Membebani server dengan request berulang.

Patch:  
Tambah validasi button, apabila sedang loading maka akan menjadi disabled  


1. **Text Input Validation**

*Rootcause*:  
Tidak ada sanitasi input form maupun pengaturan min/max length karakter untuk input teks di ArrivalForm.vue. Semua input teks seperti form.full\_name, form.passport\_no, form.nationality, dan lain-lain hanya menggunakan v-model tanpa validasi panjang karakter atau filter karakter berbahaya.

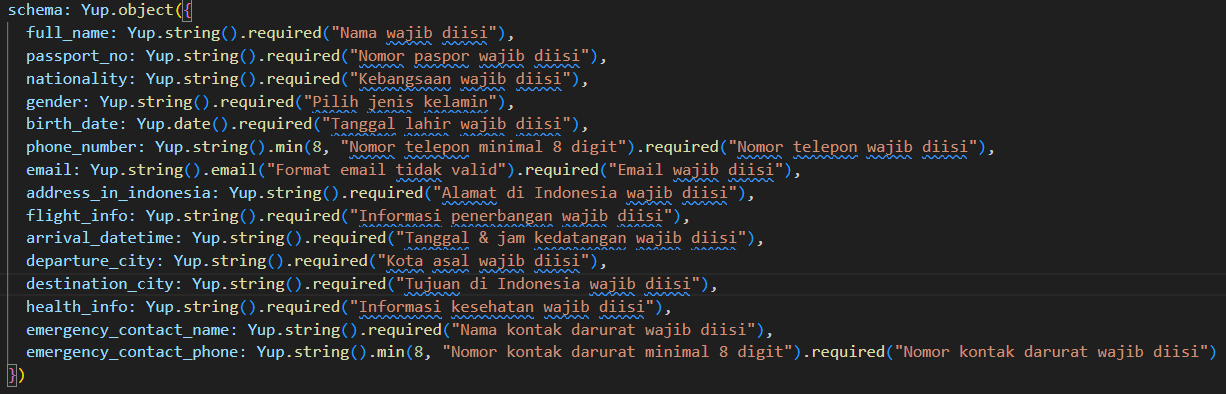


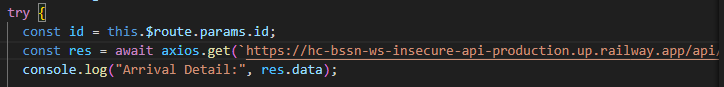
Impact:

* User bisa memasukkan script atau karakter berbahaya yang bisa menyebabkan XSS (Cross-Site Scripting) jika tidak disaring di backend.
* User bisa mengisi data dengan teks yang sangat panjang, menyebabkan error, membebani database, atau merusak tampilan aplikasi.
* Data yang masuk ke backend menjadi tidak konsisten, sulit divalidasi, dan berpotensi menyebabkan bug atau celah keamanan.
* Potensi abuse, misal spam data, deface, atau crash aplikasi karena input yang tidak wajar.

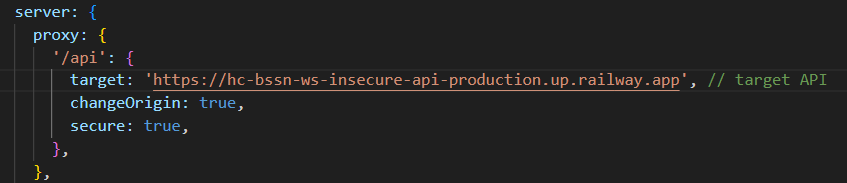
Patch:

Tambahkan validasi menggunakan yup, batas minimal da maksimal karakter, tipe file serta ukuran file  


import \* as Yup from "yup";  


1. **Change Base Url***Rootcause;  
   -* Tidak ada konfigurasi terpusat untuk endpoint API di frontend.  
   - Kurangnya **awareness** bahwa hardcode URL mempersulit maintenance & meningkatkan risiko kebocoran informasi.  
   *Impact:  
   Base URL API terekspos di file JavaScript yang di-load user, memudahkan attacker melakukan direct API call.*  
   *Patch:*Buat **satu file config** yang menyimpan base\_url, lalu impor di semua file.  
   **Before:  
   **

**After:**Ada penambahan code pada [api.js](http://api.js), vite.config.js dan perubahan di masing-masing function



**A screen shot of a computer program

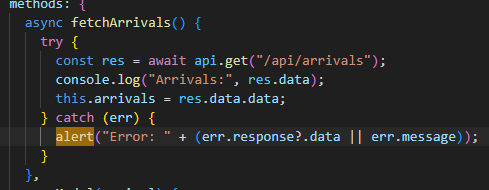
AI-generated content may be incorrect.A computer screen shot of code

AI-generated content may be incorrect.**

1. **Remove Error Alert  
   Rootcause:**Programmer menampilkan error dari backend atau dari proses frontend langsung menggunakan alert(errorMessage), tanpa sanitasi atau formatting.

**Impact:**

Error asli bisa mengandung informasi sensitif (SQL error, stack trace, file path) yang memberi petunjuk pada attacker.

**Patch:**Ganti alert() dengan toast, modal, atau banner yang lebih user-friendly.  
Before:  
  
After:  
Menggunakan SweetAlert untuk UI improvement dan juga mengubah teks wording notifikasi  
A black screen with white text

AI-generated content may be incorrect.

1. **Disable Autocomplete  
   Rootcause:**

Mencegah agar pengguna browser selain user sah mengetahui email / password, dan masuk tanpa credential yang sah

**Impact:**

* Orang di sekitar bisa melihat **dropdown suggestion** berisi email/username saat user mengetik.
* Di komputer publik atau device yang dipakai bersama, **email/password tersimpan di browser** dan bisa digunakan orang lain tanpa izin. Bisa menyebabkan **akun diambil alih** jika password tersimpan otomatis.

**Patch:**

Gunakan autocomplete="off" **hanya** pada perangkat publik/kiosk.  
Before:  


**Ater:  
**

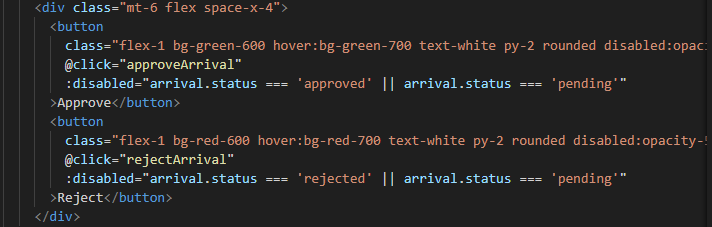
1. **UI Level Access Control  
   Rootcause:**User bisa mencoba melakukan aksi yang sudah tidak valid sesuai dengan statusnya

**Impact:**

Approval bisa diproses lebih dari sekali jika ada multiple klik.

**Patch:**

Membatasi elemen UI berdasarkan status atau hak akses pengguna.  
Before:  


After:  


1. **Role Access Missing**

**Rootcause:**User bisa akses dashboard tanpa login, dan user bisa ke halaman login meskipun statusnya sudah login

**Impact:**Data dan fitur di dashboard bisa diakses tanpa autentikasi.

Informasi sensitif bisa terlihat publik atau dicuri.

**Patch:**  
Tambahkan validasi dan tokenBefore: \*tidak ada redirect dan validasi token  
After: ada validasi token dan redirect  
A screen shot of a computer program

AI-generated content may be incorrect.

A computer screen shot of a program code

AI-generated content may be incorrect.