**Bezbednosna analiza eksternih komponenti**

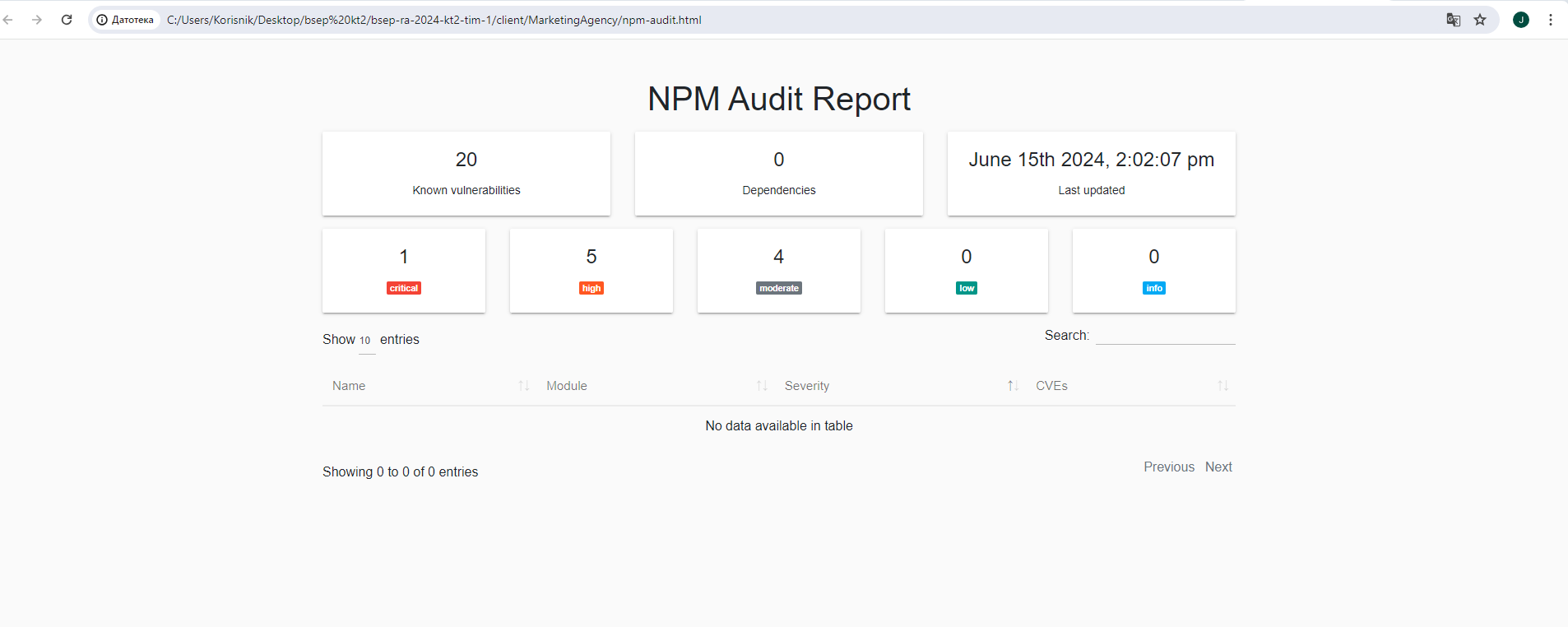
Za bezbednosnu analizu na klijentskoj strani (frontu pisanom u Angularu) korišćen je **“npm audit”**. To je ugrađeni alat koji dolazi sa **“npm”** i može se koristiti za proveru bezbednosnih ranjivosti u zavisnostima Angular projekta.

Za pokretanje i kreiranje izvještaja korišćene su sledeće komande u terminalu:

* npm audit --json > npm-audit-report.json
* npm install -g npm-audit-html
* npm audit --json | npm-audit-html > npm-audit-report.html

**1.Analiza ranjivosti**

Nakon prvog kreiranja izvještaja, alat je pokazivao 10 ranjivosti, od cega je jedna označena kao kritična ranjivost, četiri kao visoke ranjivost i pet kao umjerene ranjivosti.



npm-audit-report.html nakon prvog kreiranja

U nastavku su detaljnija objašnjena svih ranjivosti, jer u ovom izgenerisanom html izvjestaju nisu prikazani, a detalji stoje u npm-audit-report.json fajlu.

**Kritične ranjivosti**

1. **@babel/traverse**
   * **Opis:** Babel ranjiv na izvršavanje proizvoljnog koda pri kompajliranju specifično izrađenog zlonamjernog koda
   * **Izvor:** [GHSA-67hx-6x53-jw92](https://github.com/advisories/GHSA-67hx-6x53-jw92)
   * **Raspon:** <7.23.2
   * **Popravak:** Dostupan

**Visoke ranjivosti**

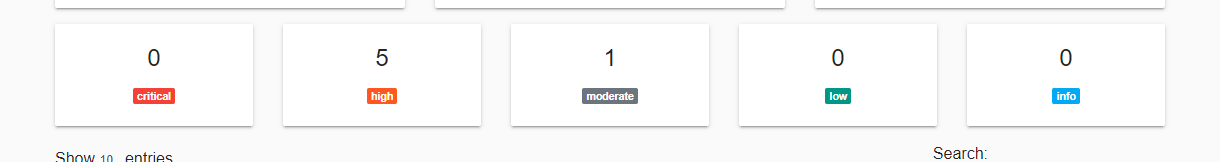
1. **@angular-devkit/build-angular**
   * **Opis:** Ranjivosti povezane s paketima postcss, vite, i webpack-dev-middleware
   * **Raspon:** <=14.2.12 || 15.0.0-next.0 - 15.2.10 || 16.0.0-next.0 - 16.2.12 || 17.0.0-next.0 - 17.3.1
   * **Popravak:** Dostupan
2. **braces**
   * **Opis:** Nekontrolisano trošenje resursa
   * **Izvor:** [GHSA-grv7-fg5c-xmjg](https://github.com/advisories/GHSA-grv7-fg5c-xmjg)
   * **Raspon:** <3.0.3
   * **Popravak:** Dostupan
3. **vite**
   * **Opis:** Više ranjivosti, uključujući XSS i obilaženje server.fs.deny opcije
   * **Izvori:**
     + [GHSA-92r3-m2mg-pj97](https://github.com/advisories/GHSA-92r3-m2mg-pj97)
     + [GHSA-c24v-8rfc-w8vw](https://github.com/advisories/GHSA-c24v-8rfc-w8vw)
     + [GHSA-8jhw-289h-jh2g](https://github.com/advisories/GHSA-8jhw-289h-jh2g)
   * **Raspon:** 4.0.0 - 4.5.2
   * **Popravak:** Dostupan
4. **webpack-dev-middleware**
   * **Opis:** Path traversal ranjivost
   * **Izvori:**
     + [GHSA-wr3j-pwj9-hqq6](https://github.com/advisories/GHSA-wr3j-pwj9-hqq6)
   * **Raspon:** <=5.3.3 || 6.0.0 - 6.1.1
   * **Popravak:** Dostupan
5. **ip**
   * **Opis:** Neispravna identifikacija privatnih IP adresa kao javnih
   * **Izvori:**
     + [GHSA-78xj-cgh5-2h22](https://github.com/advisories/GHSA-78xj-cgh5-2h22)
     + [GHSA-2p57-rm9w-gvfp](https://github.com/advisories/GHSA-2p57-rm9w-gvfp)
   * **Raspon:** <=2.0.1
   * **Popravak:** Dostupan

**Umjerene ranjivosti**

1. **express**
   * **Opis:** Open Redirect ranjivost u malformiranim URL-ovima
   * **Izvor:** [GHSA-rv95-896h-c2vc](https://github.com/advisories/GHSA-rv95-896h-c2vc)
   * **Raspon:** <4.19.2
   * **Popravak:** Dostupan
2. **follow-redirects**
   * **Opis:** Više ranjivosti, uključujući neispravno rukovanje URL-ovima i Proxy-Authorization header
   * **Izvori:**
     + [GHSA-jchw-25xp-jwwc](https://github.com/advisories/GHSA-jchw-25xp-jwwc)
     + [GHSA-cxjh-pqwp-8mfp](https://github.com/advisories/GHSA-cxjh-pqwp-8mfp)
   * **Raspon:** <=1.15.5
   * **Popravak:** Dostupan
3. **postcss**
   * **Opis:** Greška pri parsiranju linijskog povratka
   * **Izvor:** [GHSA-7fh5-64p2-3v2j](https://github.com/advisories/GHSA-7fh5-64p2-3v2j)
   * **Raspon:** <8.4.31
   * **Popravak:** Dostupan
4. **tar**
   * **Opis:** Denial of service zbog nedostatka validacije broja direktorija
   * **Izvor:** [GHSA-f5x3-32g6-xq36](https://github.com/advisories/GHSA-f5x3-32g6-xq36)
   * **Raspon:** <6.2.1
   * **Popravak:** Dostupan

**2.Preduzete mjere za prevazilaženje rizika**

Pokretanjem komande **„npm audit fix“** će automatski pokušati popraviti ranjivosti koje se mogu riješiti bez ručnog intervenisanja. I pokretanjem ove komande dobio sam sledeće rezultate:



Za ranjivosti koje **„npm audit fix“** nije mogao automatski riješiti, morao sam ručno ažurirati određene pakete.

Prvo sam pokušavao da ručno instaliram najnoviju verziju neke bibloteke ili u pojedinim slučajima verziju koja je veća od određene (pr. „npm install @angular-devkit/build-angular@latest” ili npm install @babel/traverse@^7.23.2), ali pošto sam uglavnom dobijao konfliktne situacije jer te bibloteke nisu kompatibilne sa nekim starijim koje postoje u projektu a ne prave nikakvu ranjivost. Onda sam koristio komandu “npm update”, kojom sam izmjenio veliki brojpaketa. (added 70 packages, removed 10 packages, changed 232 packages, and audited 1121 packages in 55s). Nakon toga više nisam imao ranjivosti.

Kad sam probao onda da pokrenem naš front pojavila se jedna greska prilikom kompajliranja:

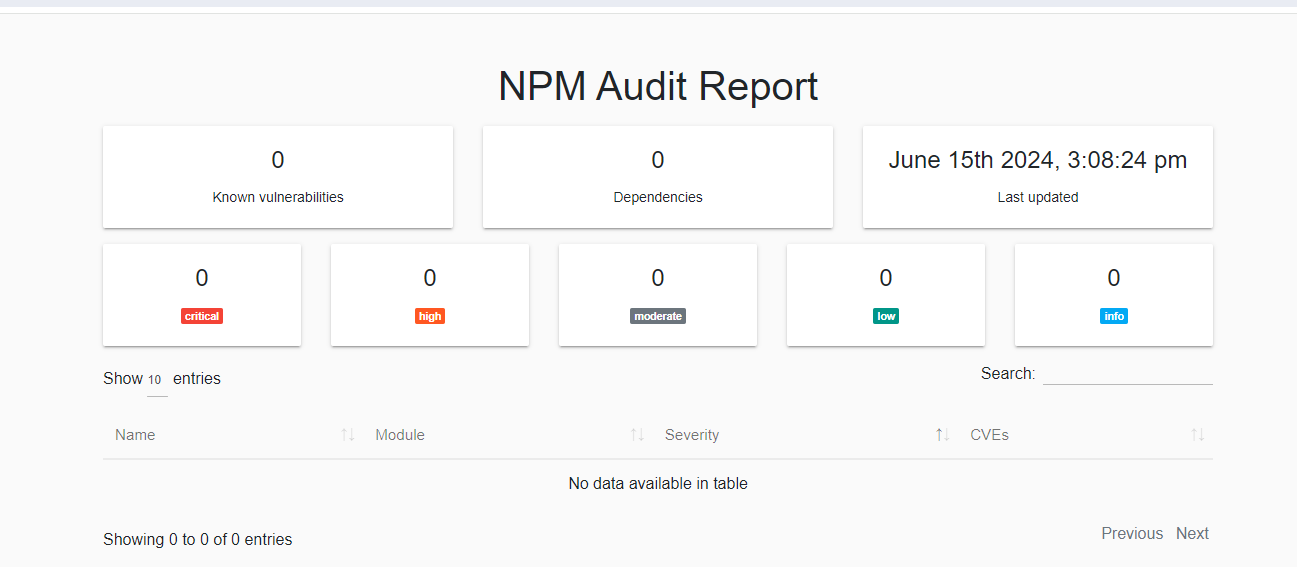
Error: node\_modules/angularx-qrcode/lib/angularx-qrcode.component.d.ts:3:44 - error TS7016: Could not find a declaration file for module 'qrcode'. 'C:/Users/Korisnik/Desktop/bsep kt2/bsep-ra-2024-kt2-tim-1/client/MarketingAgency/node\_modules/qrcode/lib/index.js' implicitly has an 'any' type.

Try `npm i --save-dev @types/qrcode` if it exists or add a new declaration (.d.ts) file containing `declare module 'qrcode';`

3 import { QRCodeErrorCorrectionLevel } from "qrcode";

Nakon čega sam morao da instaliram jos jedan dodatni paket pokretanjem ove komande: npm install --save-dev @types/qrcode. Nakon toga klijentska aplikacija se pokretala normalno.

**3.Novi izvještaj**



npm-audit-report.html na kraju