**PCI DSS**

1. **Build and Maintain a Secure Network and Systems**
2. **Protect Cardholder Data:**
   * **Protect stored cardholder data.**

Podaci o kartici koje je bilo neophodno čuvati u bazi su heširani, dok se CVV kontrolni broj uopšte ne skladišti, nego se računa od dostupnih podataka.

1. **Maintain a Vulnerability Management Program:**
   * **Develop and maintain secure systems and applications.**

Skenirali smo i otkrili ranjivosti u zavisnostima pomoću Snyk alata.

1. **Implement Strong Access Control Measures:**
   * **Restrict access to cardholder data by business need-to-know.**

Implementiran je RBAC model za autorizaciju pristupa podacima.

* **Identify and authenticate access to system component**

Implementirana je dvofaktorska autentifikacija korisnika pri prijavi agencije. Prilikom registracije, generiše se qr kod koji je potrebno skenirati I ovim putem se dobija PIN koji je neophodno koristiti prilikom prijave na sistem, uz obavezne kredencijale (email i lozinka). Unos lozinke je ograničen tako da mora da sadrži najmanje 8 karaktera, jedno veliko slovo i broj. Ako korisnik unese pogrešnu lozinku 3 puta, nalog se zaključava. Takođe, kada se korisnik prijavi, trajanje sesije mu je ograničeno na 30 minuta, nakon čega mu token više ne važi.

1. **Regularly Monitor and Test Networks:**
   * **Track and monitor all access to network resources and cardholder data.**

Implementirano je logovanje svih bitnih događaja na nivou pojedinačnih servisa.

* + **Regularly test security systems and processes.**

Izvršeno je penetraciono testiranje sistema.

1. **Maintain an Information Security Policy**