PCIDSS implementirani mehanizmi

* Protect stored account data  
    
  Svi osetljivi podaci o korisnicima, uključujući informacije o njihovim karticama, čuvaju se u bazi podataka u obliku heširanog formata. Prilikom skladištenja, originalni podaci se konvertuju u heš vrednost pomoću sigurnih heš funkcija. Ovo sprečava neovlašćen pristup čak i ako baza podataka bude kompromitovana.  
  Da bismo dodatno obezbedili osetljive podatke tokom njihovog prenosa između klijenta i servera, implementiran je HTTPS protokol. Korišćenje HTTPS-a omogućava enkripciju podataka tokom komunikacije, čime se smanjuje rizik od presretanja ili manipulacije tokom prenosa.
* Maintain vulnerability management program  
    
  U skladu sa PCIDSS standardom, iskorišćen je program upravljanja ranjivostima kako bi se aktivno identifikovale, pratile i rešavale potencijalne slabosti u bezbednosti aplikacije. Korišćen je OWASP Zap alat za redovno skeniranje aplikacije i otkrivanje ranjivosti. U cilju održavanja visokog nivoa bezbednosti sistema, neophodno je redovno sprovoditi skeniranje ranjivosti. Ova praksa omogućava identifikaciju potencijalnih sigurnosnih rizika i ranjivosti u aplikaciji.
* Implement strong access control measures  
    
  U cilju poštovanja PCIDSS standarda, implementirane su mere kontrole pristupa kako bi se osiguralo da samo ovlašćeni korisnici imaju pristup sistemu. Ovaj princip je realizovan kroz korišćenje sistema za upravljanje identitetima i pristupom - Keycloak.  
  Keycloak se koristi kao centralni sistem za autentifikaciju, pružajući pouzdan i siguran mehanizam za proveru identiteta korisnika.
* Regularly monitor and test networks  
    
  Implementiran je sistem za praćenje i nadgledanje pristupa sistemu. Logovi o svakoj akciji korisnika čuvaju se u MongoDB bazi podataka, pružajući potpunu transparentnost i mogućnost brze analize.
* Restrict physical access to cardholder data  
    
  Kako bi se osiguralo ograničenje fizičkog pristupa podacima o korisnicima kartica, implementiran je API Gateway. API Gateway služi kao centralna tačka pristupa koja omogućava kontrolisani i bezbedan pristup servisima, a direktni pristup tim servisima nije dozvoljen osim preko API Gateway-a. U produkcionom okruženju, pristup servisima trebao bi se omogućiti samo putem API Gateway-a. Direktni pristup servisima trebalo bi da bude onemogućen, čime se postiže dodatan nivo sigurnosti.