Implementacija PCI DSS standarda za PaymentServiceProvider komponentu

- Protect cardholder data
    1. Protect stored cardholder data
    2. Encrypt transmission of cardholder data across open, public networks

  Podaci o vlasnicima kartica se ne čuvaju u samom Payment Service Provider-u (PSP-u), već se čuvaju isključivo u banci. PSP čuva samo kredencijale ID-a prodavca, koji su dobijeni od banke prilikom registracije za online prodaju. Ovi podaci su zaštićeni, a lozinke se čuvaju u enkriptovanom formatu.

  Svi podaci koji se prenose između PSP-a i ostalih entiteta enkriptuju se koristeći HTTPS protokol za komunikaciju, obezbeđujući tako siguran transfer podataka preko mreže.

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

  Implementirane su osnovne sigurnosne prakse – razvojno i testno okruženje su razdvojeni od produkcionog time što su dodate različite appsettings.json konfiguracione datoteke. Za potrebe testiranja nisu korišćeni pravi PAN brojevi. Aplikacija je implementirna pridržavajući se najboljih praksi u .NET frameworku. Osigurano je da su svi dependecy-i bez evidentiranih ranjivosti, ali ih je potrebno ažurirati na najnovije verzije.

- Implement Strong Access Control Measures
    1. Restrict access to cardholder data by business need to know
    2. Identify and authenticate access to system components

  PSP kao komponenta kakva je sada trenutno nema implementiran administrativni deo tj korisnike koji bi administrirali podatke i imali određene role. Pristup podacima iz PSP-a je ograničen na opciju odabira načina plaćanja računa za određenog prodavca. Kako bi se zaštitio pristup dostupnim API endpoint-ovim swagger je dostupan samo u Development okruženju.

- Regular Monitor and Test Networks
    1. Track and monitor all access to network resources and cardholder data

  PSP generiše logove koji obuhvataju dvosmernu komunikaciju putem API-ja. To znači da se beleže i pozivi koji se vrše ka PSP API-ju, kao i pozivi koji se primaju od drugih API-ja ili klijentskih aplikacija. Logovi obuhvataju i upite (query-e) ka bazi podataka, što omogućava praćenje svih operacija nad podacima u sistemu. Pored toga, MS SQL baza koja se koristi takođe generiše sopstvene logove, doprinoseći dodatnoj transparentnosti i praćenju svih aktivnosti unutar baze podataka. Takođe, postoji evidencija transakcija kroz posebnu tabelu *TransactionLogs* u bazi podataka, koja prati istoriju promena statusa transakcija i vreme kada su se te promene dogodile. Ova kombinacija logova omogućava praćenje svih aktivnosti i promena u sistemu.