PCI DSS

Tim 13: Aleksa Goljović R2 29/21, Jelena Cupać R2 30/21, Milan Marinković R2 31/21

II PROTECT CARDHOLDER DATA

Requirement 3: Protect stored cardholder data

3.1. Svesti podatke koji se skladište na minimum

- Čuvali smo samo neophodne podatke

3.2. Podatke za autentifikaciju ne treba čuvati nakon autorizacije

- Nismo čuvali podatke za autentifikaciju i nismo ih pisali u log porukama

3.3. Ceo PAN broj ne sme da se prikaže

- Nigde se ne prikazuje ceo PAN broj

3.4. Onemogućiti čitanje PAN broja iz baze

- Onemogućeno je čitanje PAN broja iz baze šifrovanjem istog (simetrično šifrovanje).

3.5. Dokumentovati i implementirati procedure za zaštitu ključeva

3.6. Dokumentovati i implementirati sve procese i procedure za upravljanje ključevima

3.7. Osigurati da su svi upoznati sa bezbednosnim propisima i operativnim procedurama za zaštitu podataka koji se skladište

Requirement 4: Encrypt transmission of cardholder data across open, public networks

4.1. Koristiti bezbednosne protokole, kao što je SSL/TLS, SSH itd. da bi se zaštitili osetljivi podaci tokom prenosa

- Koristili smo HTTPS sa TLS v1.3

4.2. Nezaštićen PAN broj ne sme da se šalje preko platformi za razmenu poruka (e-mail, instant messaging, chat..)

- PAN broj se ne šalje preko platformi za razmenu poruka

4.3. Osigurati da su svi upoznati sa bezbednosnim propisima i operativnim procedurama za zaštitu podataka, koji se šalju sa jedne na drugu lokaciju

III MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

Requirement 6: Develop and maintain secure systems and applications

- Ispunili smo zahteve Owasp Top 10 projekta
- Nismo koristili prave PAN brojeve

IV IMPLEMENT STRONG ACCESS CONTROL MEASURES

Requirement 7: Restrict access to cardholder data by business need to know

- Implementirali smo potpuni RBAC, gde su definisane role i permisije
- Implementirali smo Spring Security

Requirement 8: Identify and authenticate access to system components

8.1. Definisati i implementirati procedure za pravilno upravljanje korisnicima, koji nisu potrošači, i administratorima, koji ne koriste sve komponente sistema

- Ukoliko korisnik nije aktivan 90 dana, njegov nalog biva blokiran
- Ukoliko korisnik pokuša da se uloguje tri puta neuspešno sa iste IP adrese, biće privremeno blokiran

8.2. Najmanje jedan mehanizam za potvrdu identiteta

- Obezbedli smo autentifikaciju lozinkom i tokenom
- Za lozinku je definisana politika, mora da bude minimalno 8 karaktera duga i treba da sadrži broj, specijalni karakter, malo i veliko slovo, takođe, proverava se i da li se nalazi na black listi nesigurnih lozinki

8.4. Dokumentovati procedure za autentifikaciju (smernice kako zaštiti kredencijale, uputstvo za promenu lozinke..)

8.5. Ne koristiti grupne, deljene ili generičke IDs, lozinke..

8.6. Mehanizam za potvrdu identiteta dodeliti pojedinačnom nalogu

8.7. Svaki pristup bazi podataka treba da bude ograničen

8.8. Osigurati da su svi upoznati sa bezbednosnim propisima i operativnim procedurama za potvrdu identiteta i da su dokumentovani, u upotrebi i poznati svim stranama

V REGULARLY MONITOR AND TEST NETWORKS

Requirement 10: Track and monitor all access to network resources and cardholder data

- Sav saobraćaj je logovan