SEP: PCI DSS

- Standard sigurnosti podataka za industriju platnih kartica (PCI DSS) razvijen je kako bi ohrabrio i poboljšao sigurnost podataka o vlasnicima kartica i omogućio globalno usvajanje konzistentnih mera sigurnosti podataka. PCI DSS pruža osnovne tehničke i operativne zahteve dizajnirane za zaštitu podataka računa. PCI DSS se odnosi na sve subjekte uključene u obradu platnih kartica - uključujući trgovce, procesore, preuzimatelje, izdavatelje i pružatelje usluga. PCI DSS se takođe primenjuje na sve druge entitete koji skladište, obrađuju ili prenose podatke o vlasnicima kartica i/ili osetljive autentifikacione podatke. U nastavku je pregled 12 PCI DSS zahteva visokog nivoa:

I Izgraditi i održavati bezbednu mrežu i sisteme

1. instalirati i održavati konfiguraciju zaštitnog zida da bi se omogućila zaštita podataka o vlasnicima kartica
2. ne koristiti podrazumevane vrednosti za sistemske lozinke i druge bezbednosne parametre

II Zaštiti podatke o vlasnicima kartica

3. zaštititi uskladištene podatke o vlasnicima kartica
4. šifrovati prenos podataka o vlasnicima kartica preko otvorenih javnih mreža

III Održavati programe upravljanja ranjivosti

5. zaštititi sve sisteme od zlonamernog softvera (malvera) i redovno ažurirati antivirusni softver ili programe
6. razviti i održavati sigurne sisteme i aplikacije

IV Sprovesti jake mere kontrole pristupa

7. ograničiti pristup podacima o vlasnicima kartica prema poslovnim potrebama
8. identifikacija i autentifikacija pristupa komponentama sistema
9. ograničiti fizički pristup podacima o vlasnicima kartica

V Redovno nadgledati i testirati mreže

10. pratiti i nadgledati sav pristup mrežnim resursima i podacima o vlasnicima kartica
11. redovno testirati sigurnosne sisteme i procese

VI Održavati politiku sigurnosti informacija

12. održavati politiku koja se bavi informacijskom sigurnošću za svo osoblje

- Podaci o vlasnicima kartica i osetljivi podaci za autentifikaciju definisani su na sledeći način:

Podaci o računu	
Podaci o vlasnicima kartica uključuju:	***Podaci o osetljivoj autentifikaciji uključuju:***
• osnovni broj računa (PAN) • ime vlasnika kartice • datum važenja • servisni kod	• podaci magnetne trake ili ekvivalent na čipu • CAV2/CVC2/CVV2/CID • PIN-ovi / blokovi PIN-ova

1. ***instalirati i održavati konfiguraciju zaštitnog zida da bi se omogućila zaštita podataka o vlasnicima kartica*** – out of scope

2. ***ne koristiti podrazumevane vrednosti za sistemske lozinke i druge bezbednosne parametre*** – out of scope

3. ***zaštititi uskladištene podatke o vlasnicima kartica*** – skladištiti samo ono što je zaista neophodno, ne skladištiti osetljive podatke nakon što se korisnik autorizuje, ne skladištiti sadržaj magnetnih traka, ne skladištiti kod za verifikaciju kartice, ne skladištiti PIN, ako se mora prikazati PAN mora biti maskiran (vidljivo treba da bude samo prvih 6 ili samo poslednje 4 cifre), PAN ne čuvati u osnovnom obliku nego ga heširati (ili koristiti index tokene, kriptografske ključeve), dokumentovati i implementirati procedure za skladištenje kriptografskih ključeva koji su korišćeni za kriptovanje podataka o vlasnicima kartica, kriptografske ključeve čuvati u kriptovanom obliku i na što je moguće manje mesta, dokumentovati i implementirati procedure za upravljanje kriptografskim ključevima (generisati jake ključeve, sigurna distribucija ključeva, sigurno skladištenje ključeva), zamena starog ključa novim nakon isteka perioda važenja, zamena ključeva ako se ispostavi da je ugrožen integritet korišćenog ključa, sprečiti neovlašćenu zamenu ključeva. Korišćen AES algoritam (128, 192 i 256-bitni ključevi), režim rada CBC.

4. ***šifrovati prenos podataka o vlasnicima kartica preko otvorenih javnih mreža*** – prihvatanje samo proverenih ključeva i sertifikata, protokol od poverenja, jačina enkripcije, npr. PAN se nikad ne šalje u originalnom obliku preko recimo mejla. Korišćen AES algoritam (128, 192 i 256-bitni ključevi), režim rada CBC. Upotreba SSLv2 protokola (HTPPS umesto HTTP).

5. ***zaštititi sve sisteme od zlonamernog softvera (malvera) i redovno ažurirati antivirusni softver ili programe*** - out of scope

6. ***razviti i održavati sigurne sisteme i aplikacije*** – detektovati i klasifikovati ranjivosti u sistemu (low, medium, high), koristiti lažni PAN (ne neke stvarno postojeće) za testiranje rada sistema, razdvajanje nadležnosti između testnih (razvojnih) i proizvodnih okruženja, uklanjanje testnih podataka i naloga pre nego što se sistem pusti u produkciju, back-up procedure, prevencija XSS napada (validacija svih parametara, utilizing context-sensitive escaping → izbegavanje/korišćenje eskejpovanja; XSS greške se javljaju kada aplikacija uzima podatke koje je dostavio korisnik i šalje ih veb pretraživaču bez prethodnog potvrđivanja ili kodiranja tog sadržaja. XSS omogućava napadačima da izvrše skriptu u pretraživaču žrtve, koja može oteti korisničke sesije, ometati veb lokacije, eventualno uvesti crve i sl.), nepravilna kontrola pristupa (kao što su nesigurne direktne reference objekta, neuspeh u ograničavanju pristupa URL-u, prelazak direktorijuma i neuspeh u ograničavanju korisničkog pristupa funkcijama), CSRF (CSRF napad prisiljava pretraživač prijavljenog korisnika (žrtve) da pošalje prethodno provereni zahtev ranjivoj veb aplikaciji, što napadaču omogućava da izvrši sve operacije koje menja stanje koje je žrtva ovlašćena da izvrši (kao što je ažuriranje detalja računa, kupovina ili čak i autentifikacija na aplikaciju), neispravna autentifikacija i upravljanje sesijama (sigurna autentikacija i upravljanje sesijama sprečavaju neovlašćene osobe da ugroze legitimne akreditive naloga, ključeve ili tokene sesije koji bi inače omogućili uljezu da preuzme identitet ovlašćenog korisnika). Uočene potencijalne ranjivosti sistema, korišćeni lažni nalozi za plaćanje i testiranje rada u test API okruženju, sprečen XSS napad tako što se vrši validacija svih podataka sa kojima se radi u okviru sistema a osetljivi podaci se kriptuju, realizovane permisije kako bi se sprovela kontrola pristupa funkcijama sistema, onemogućen CSRF napad

tako što je eksplicitno disable-ovan u konfiguraciji aplikacije, prilikom pokušaja logovanja vrši se provera korisničkih kredencijala pa je sprečena mogućnost pojave neispravne autentifikacije, sesijama se upravlja tako što se koriste adekvatne security klase (videti klasu KorisnikService).

7. ***ograničiti pristup podacima o vlasnicima kartica prema poslovnim potrebama*** - ograničiti pristup komponentama sistema i podacima o vlasnicima kartica samo onim pojedincima čiji posao zahteva takav pristup, definisati potrebe za pristupom za svaku ulogu uključujući: komponente sistema i resurse podataka kojima svaka uloga treba da pristupi da bi obavila svoj deo posla, kao i zahtevani nivo privilegije (npr. korisnik, administrator) za pristup resursima, ograničiti pristup privilegovanim korisničkim ID-ovima na najmanje privilegije potrebne za obavljanje poslova, dodeliti pristup na osnovu klasifikacije i funkcije pojedinačnog osoblja, osigurati da su sigurnosne politike i operativne procedure za ograničavanje pristupa podacima o vlasnicima kartica dokumentovane, u upotrebi i poznate svim zainteresovanim stranama. Korišćen je princip razdvajanja nadležnosti – za svaku ulogu su definisane funkcije koje može da obavlja (permisije) i za svaku ulogu su vezane samo one funkcije/privilegije koje su minimalno neophodne kako bi se odgovarajući deo posla mogao obaviti. Prilikom registracije na sistem svaki korisnik se smatra ili čitaocem (ako nema titulu) ili recenzentom (ako ima titulu) jer oni imaju najmanje privilegije.

8. ***identifikacija i autentifikacija pristupa komponentama sistema*** – svakom korisniku dodeliti jedinstveni ID (pre nego što se razmotri mogućnost da mu se dozvoli pristup podacima o vlasnicima kartica – npr. admin ima to pravo), kontrolisano obavljanje CRUD operacija nad korisnicima, odmah opozvati/sprečiti pristup za sve ukinute korisnike, ukolniti korisnika koji nije bio aktivan 90 dana, ograničiti broj mogućih pokušaja za pristup (npr. ako se pri logovanju pogreši kombinacija kredencijala 3x zaredom sprečiti logovanje na neko vreme ili tražiti reset lozinke), trajanje zaključavanja postaviti na najmanje 30 min ili dok administrator ne odobri otključavanje naloga, ako je sesija neaktivna 15+ min potrebna je ponovna autentifikacija korisnika, pored ID-a potreban je još neka metoda za autentifikaciju kao što je lozinka, token uređaja/smart kartica ili biometrijski podatak, kriptovati kredencijale korisnika, proveravati identitet pre pokušaja ažuriranja korisničkih podataka, proveravati kvalitet/jačinu lozinke, promeniti lozinku na bar 90 dana, zabraniti korisniku da kao novu lozinku postavu neku od prethodno već korišćenih, postaviti podrazumevanu lozinku i zahtevati da se pri prvom logovanju ona promeni, koristiti multifaktorsku autentifikaciju, ne koristiti grupne/deljene/generičke ID-ove, tamo gde se koriste drugi mehanizmi autentifikacije (npr. fizički ili logički sigurnosni tokeni, pametne kartice, sertifikati itd) - upotreba ovih mehanizama mora biti dodeljena na sledeći način: mehanizmi autentifikacije moraju biti dodeljeni pojedinačnom računu i ne smeju se deliti na više naloga, moraju se uspostaviti fizičke i/ili logičke kontrole kako bi se osiguralo da samo predviđeni račun može koristiti taj mehanizam za dobijanje pristupa, sav pristup bilo kojoj bazi podataka koja sadrži podatke o vlasniku kartice (uključujući pristup od strane aplikacija, administratora i svih drugih korisnika) je ograničen na sledeći način: svi korisnički pristupi, korisnički upiti i akcije korisnika na bazama podataka su putem programskih metoda, samo administratori baza podataka imaju mogućnost direktnog pristupa bazama podataka ili njihovom upitu, ID aplikacije za aplikacije baze podataka mogu se koristiti samo od strane aplikacija (a ne od strane pojedinačnih korisnika ili drugih neaplikacijskih procesa). Svaki korisnik ima svoj jedinstveni ID, CRUD operacije dozvoljene su samo određenoj ulozi (adminu), uklonjeni korisnici se brišu iz liste korisnika koji su aktivni pa im se zabranjuje pristup sistemu, za autentifikaciju se koristi kombinacija jedinstvene email adrese i lozinke, svakom registrovanom korisniku je dozvoljeno da promeni lozinku u bilo kom trenutku s tim da se prvo mora autentifikovati, bazi podataka pristupa se

isključivo putem impementiranih programskih metoda u okviru kojih se izvršavaju potrebni upiti nad bazom.

9. ***ograničiti fizički pristup podacima o vlasnicima kartica*** - out of scope

10. ***pratiti i nadgledati sav pristup mrežnim resursima i podacima o vlasnicima kartica*** – implementirati revizorske tragove kako bi se svi pristupi komponentama sistema povezali sa svakim pojedinačnim korisnikom, primeniti automatske tragove revizije za sve komponente sistema da bi se rekonstruisali sledeći događaji: pokušaj pristupa podacima o vlasnicima kartice od strane svakog pojedinačnog korisnika, sve radnje preduzete od strane bilo kog pojedinca sa root ili administratorskim privilegijama, pristup svim revizijskim tragovima, nevažeći pokušaji logičkog pristupa, upotreba i izmena mehanizama identifikacije i autentifikacije - uključujući, ali ne ograničavajući se na, kreiranje novih naloga i povećanje privilegija - i sve promene, dopune ili brisanja na naloge sa root ili administratorskim privilegijama, inicijalizacija/zaustavljanje/pauziranje dnevnika revizije, kreiranje i brisanje objekata na nivou sistema. Loguju se aktivnosti koje se obavljaju unutar sistema.

11. ***redovno testirati sigurnosne sisteme i procese*** - out of scope

12. ***održavati politiku koja se bavi informacijskom sigurnošću za svo osoblje*** - out of scope

BEZBEDNOSNI MEHANIZMI IMPLEMENTIRANI U PROJEKTU:

- HTTPS
- logovanje aktivnosti u aplikaciji → Logger klasa, na nivou kontrolera
- heširanje lozinke → umesto MD5+salt korišćen je BCryptPasswordEncoder
- kriptovanje email adrese → korišćen je AES algoritam, umesto ECB sad radi u CBC režimu
- provera često korišćenih lozinki
- svaki korisnik u bilo kom trenutku može promeniti lozinku (obavezna autentifikacija)
- merchantId i merchantPassword se kriptuju AES algoritmom u CBC režimu rada
- security: PreAuthorize i hasAuthority zamenjeni permisijama, @Transactional, JSON web token
- XSS i CSRF sprečeni (videti podešavanje unutar WebConfiguration klase)