Model pretnji

1. Uvod

U ovom dokumentu detaljno je razrađen model pretnji za PSP sistem.
Provajder usluga plaćanja (PSP - Payment Service Provider) je sistem koji pruža preduzećima i pojedincima mogućnost prihvatanja plaćanja putem različitih kanala, kao što su kreditne kartice, paypal, bitcoin i qr kodom. PSP je aplikacija mikroservisne arhitekture koja se sastoji iz sledećih mikroservisa: Api Gateway, Service Registry, PayPal, Crypto, Bank, Auth servisa.

Verzija aplikacije: 1.0

2. Dekomponovanje modula

Dekompozicija se može izvršiti na više načina, sve dok to ima smisla za ljude koji su je izvršili. Jedan problem je i koliko daleko ići u toj dekompoziciji.

2.1. Resursi

Resursi podataka		
ID	NAZIV	OPIS
1	Podaci o web shopovima	Informacije o web shopovima poput emaila, lozinke
2	Transakcije	Podaci o transakcija, iz kojih je moguće saznati statističke informacije, kao i cenu i vreme plaćanja
3	Podaci vezani za metode plaćanje	Podaci specifični za metode plaćanja poput: PAN, API tokena, Merchant ID, client secret

Servisni resursi		
ID	NAZIV	OPIS
1	Baza podataka	Baza koja sadrži sve struktuirane podatke
2	Poslovna logika PSP	Biznis logika PSP, funkcionalnosti koje on obezbeđuje

Tehnički resursi		
ID	NAZIV	OPIS
1	Sertifikat	Služi za bezbednu komunikaciju pomoću HTTPS
2	Log fajlovi	Log fajlovi čuvaju informacije o aktivnostima PSP i web shopova
3	Konfiguracioni fajlovi	Informacije potrebne za ispravno funkcionisanje i konfiguraciju komponenti sistema. Tu se nalaze podaci o host-u i port-u servisa, kredencijali za pristup bazi podataka.

2.2. Ulazne tačke

Ovde su predstavljene ulazne tačke visokog nivoa koje se odnose na kompletan podsistem.

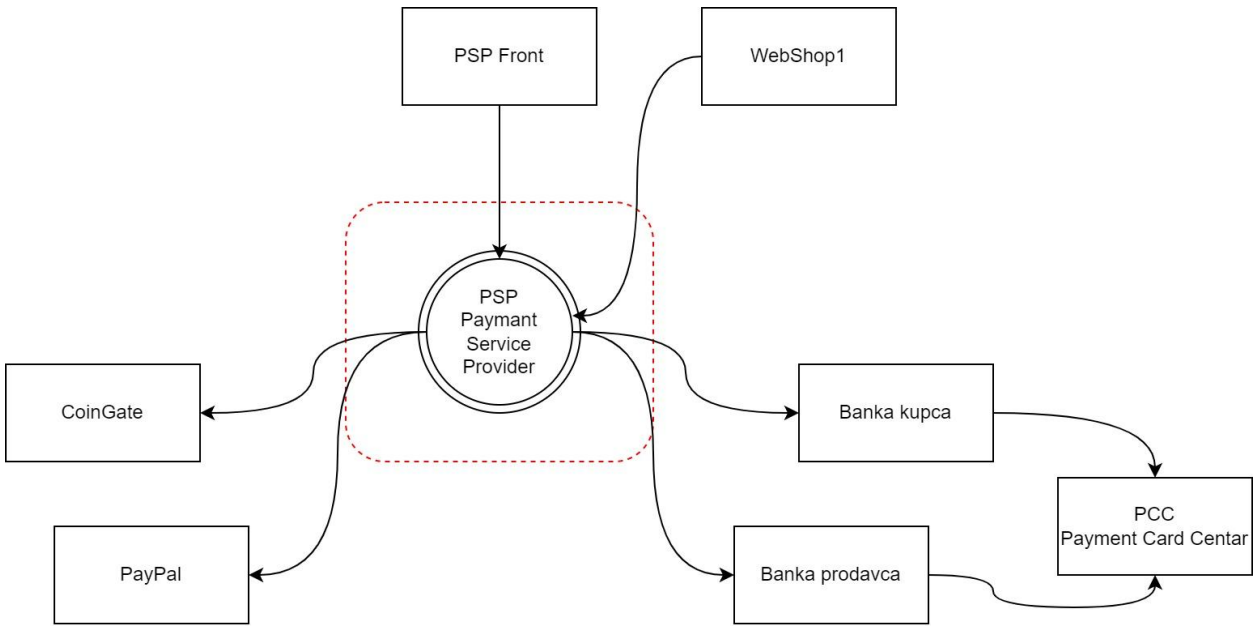
Ulazne tačke		
ID	NAZIV	OPIS
1	HTTP port	Komunikacioni kanal korišten od strane eksternih entiteta kako bi pristupili sistemu
2	Fajl sistem	Svaka aplikacija zavisi od sistema fajlova na operativnom sistemu koji koristi. Na primer konfiguracioni fajl

2.3. Eksterne zavisnosti i biblioteke

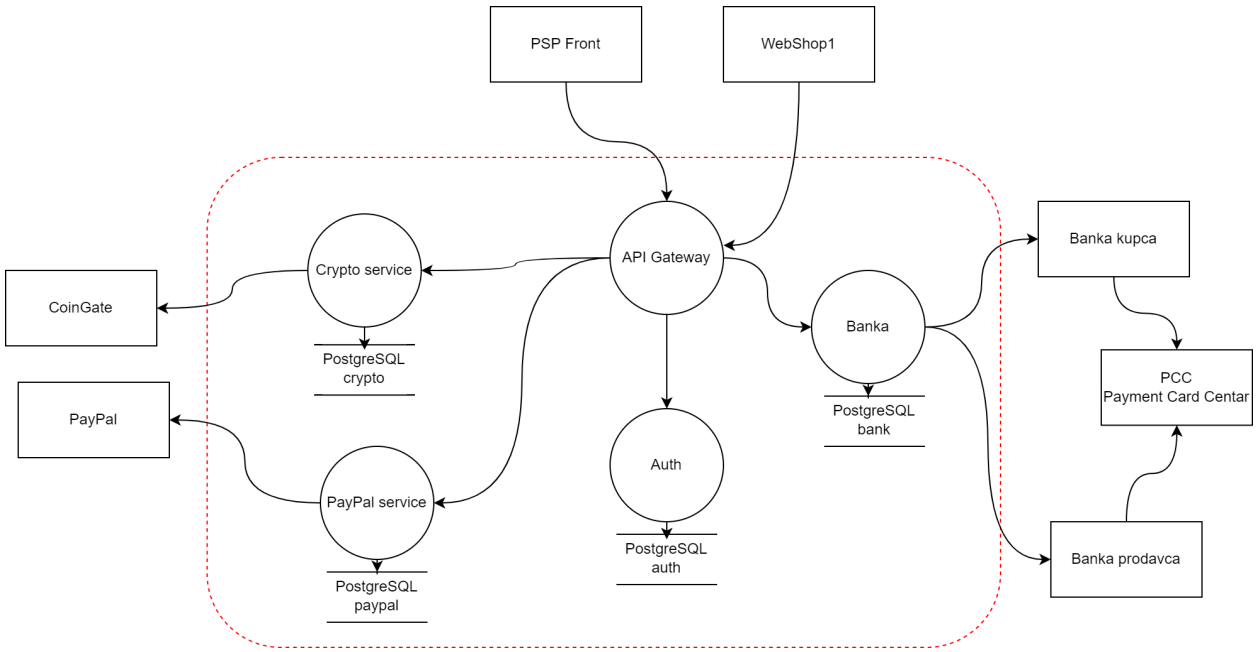
Infrastruktura	
ID	OPIS
1	PostgreSQL Baza za skladištenje podataka
2	HTTPS (TLS)

Tehnologije	
ID	OPIS
1	Java 11
2	Spring Boot 2.3.0 - Spring security 5.3.2 - Spring-boot-starter-data-jpa - Spring-boot-starter-log4j2 - Spring-boot-starter-data-rest - Spring-boot-eureka
3	Frontend je implementiran pomoću Angular 13.3.10 framework-a

2.4. Diagram toka upravljanja (DFD)



Slika 1 - konceptualni nivo toka podataka PSP



Slika 2 - Detaljan nivo toka podataka PSP

3. Analiza pretnji

Pretnje				
ID	SCENARIO NAPADA	KATEGORIJA	VEROVATNOCA	PROTIVMERE
1	Anonimni spoljni napadač prisluškuje osetljive podatke - kao što tokeni, secrete, lozinke	Information Disclosure	Low	DA. Koristi se TLS preko HTTP-a, odnosno konfigurisan je HTTPS, preko kojeg se odvija komunikacija.
2	XSS napad - napadač unosi script tag kroz input polje	Information Disclosure	Low	DA. Angular vrši sanitizaciju input polja na frontend-u
3	Maliciozni korisnik upućuje veliki broj zahteva ka serveru u cilju da ga preoptereti.	Denial of service	Medium	NE. Potrebno je obezbediti dobar monitoring kako bi se moglo uočiti ovakvo ponašanje i preventivno blokirati korisnik ili privremeno onemogućiti izvršavanje ovakve akcije. Možemo integrisati 3th party sisteme za zaštitu.
4	Napadač pristupa funkcionalnosti za koju nema permisiju.	Elevation of Privilege	Medium	DA. Implementiran je RBAC mehanizam i na bekendu i na frontendu.
5	SQL Injection	Information Disclosure	Low	DA. Spring JPA implementira mehanizme koji sprečavaju injection napade

6	Kupac poriče operaciju cancel order	Repudiation	High	DA. PSP generiše log fajlove koji dokazuju neporecivost.
7	Maliciozni korisnik pokušava da iskoristi ranjivost iz prethodnih verzija biblioteka sistema	Elevation of Privilege	Medium	DA. Redovno se ažuriraju verzije biblioteka i radnih okvira

4. Analiza rizika

Analiza rizika						
ID	VEROVATNOCA	NEGATIVNI UTICAJ	OZBILJNOST	RAZLOG	STRATEGIJA	REŠENJE
1	Low	High	High	Pošto se radi o sistemu PSP koji mora da bude maksimalno bezbedan jer su u pitanju finansije, ovo je prioritet	Reduce	HTTPS
2	Low	Medium	Low	Napadač ovim napadima nema preveliki uticaj na PSP	Accept	
3	Medium	Medium	Medium	Za sistem PSP je vrlo važno da bude stalno dostupan korisnicima, takođe važno nam je da ne napravimo grešku, da blokiramo korisnika koji nije napadač	Reduce	Implementirati ili integrisati AI alat koji će da prepoznaje ovakve napade
4	Medium	High	High	Nedopustivo je da bilo ko ima mogućnost da menja podatke o metodama plaćanja	Reduce	Implementirati RBAC mehanizam
5	Low	High	Medium	Nedopustivo je da maliciozni korisnik izvrši neku interakciju sa našom bazom podataka	Remove	Izbaciti one delove softvera koji ne podržavaju zaštitu od Injection napada
6	High	High	High	Nedopustivo je da korisnici lažno tvrde da su platili nešto kad nisu	Reduce	Implementirati logovanje aktivnosti korisnika i PSP sistema
7	Medium	Medium	Medium	Opasno je da koristimo biblioteke za koje se zna da imaju bezbednosnu ranjivost. Jer onda naš sistem može biti takođe napadnut od bilo kog napadača koji zna za ranjivost biblioteke koju mi koristimo	Remove	Ukloniti legacy biblioteke i delove projekta koji ne ispunjavaju bezbednostni standard

TIM 7

Članovi Tima:

Sanja Drinić

Kristina Stojić

Đorđe Krsmanović

Rastislav Kukučka