1. Resursi od značaja

ID	Naziv	Opis
A1	Kredencijali korisnika	Email i lozinka koje korisnici koriste za prijavu na sistem.
A2	Lični podaci korisnika	Ime, prezime, email, adresa stanovanja...
A3	Podaci za plaćanje	MerchantId, MerchantPassword, PAN...
A4	Biznis logika WebShop-a	Funkcionalnosti koje korisnicima pružaju kupovinu proizvoda putem Interneta.
A5	API Gateway	Pruža korisnicima usluge PSP-a i obezbeđuje komunikaciju između servisa i aplikacija.
A6	Biznis logika PSP servisa	Funckionalnosti za upravljanje korisnicima sistema.
A7	Biznis logika Bank servisa	Funkcionalnosti za plaćanje platnom karticom.
A8	Biznis logika QR servisa	Funkcionalnosti za plaćanje QR kodom.
A9	Biznis logika PayPal servisa	Funkcionalnosti za plaćanje korišćenjem PayPal-a.
A10	Biznis logika Bitcoin servisa	Funkcionalnosti za plaćanje Bitcoin kriptovalutom.
A11	Biznis logika Acquirer banke	Funkcionalnosti banke kupca
A12	Biznis logika PCC centra za platne kartice	Funkcionalnosti za međubankarska plaćanja
A13	Biznis logika Issuer banke	Funkcionalnosti banke prodavca
A14	Baze podataka	Čuvaju podatke koji su neophodni za funkcionisanje sistema.
A15	Repozitorijumi za skladištenje setifikata	Sadrže sertifikate odgovarajućih servisa.
A16	Konfiguracione datoteke	Sadrže konfiguraciju komponenti sistema.

2. Nivoi poverenja korisnika sistema

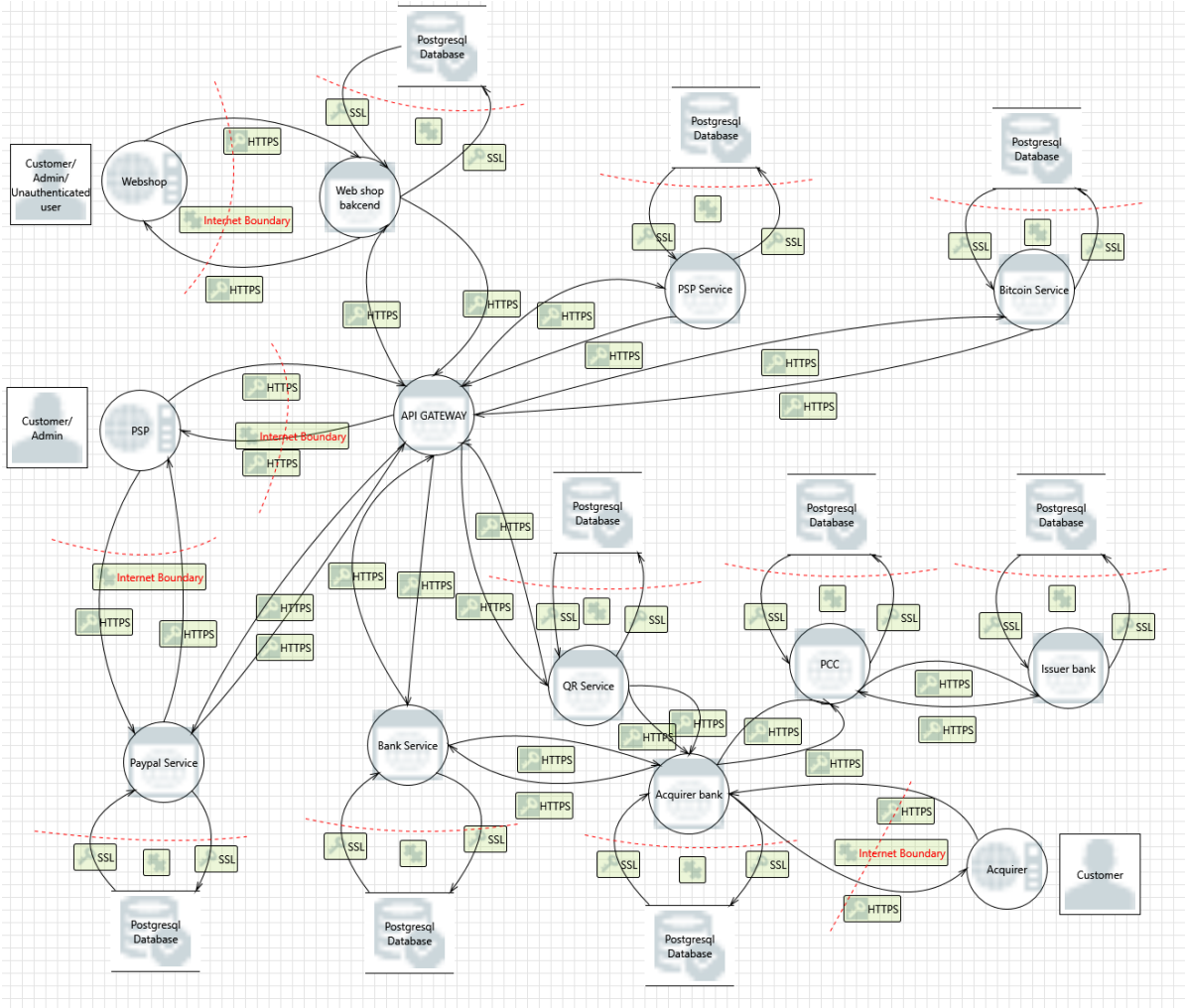
ID	Naziv	Opis
TA1	Neregistrovan korisnik WebShop-a	Pregleda proizvode koje izabrani WebShop nudi.
TA2	Registrovan korisnik WebShop-a (kupac)	Pregleda proizvode, kupuje proizvode, ima uvid u istoriju kupovine proizvoda.
TA3	Administrator WebShop-a	Upravlja proizvodima, vrši pretplate na nove načine plaćanja, vrši uplatu dnevnica.

3. Ulazne tačke sistema

ID	Naziv	Nivoi poverenja
EP1	Stranica za prijavu na sistem (Web Shop)	TA1 – TA3
EP2	Stranica za registraciju na sistem (Web Shop)	TA1 – TA3
EP3	Stranica za pregled proizvoda (Web Shop)	TA1 – TA3
EP4	Stranica za pregled i kupovinu proizvoda iz korpe (Web Shop)	TA2
EP5	Stranica za uvid u istoriju kupovine proizvoda (Web Shop)	TA2

EP6	Stranica za plaćanje dnevnica (Web Shop)	TA3
EP7	Stranica za pretplatu na novi način plaćanja (PSP)	TA3
EP8	Stranica za biranje načina plaćanja (PSP)	TA2
EP9	Stranica za plaćanje platnom karticom (Acquirer Bank)	TA2
EP10	Stranica za plaćanje QR kodom (Acquirer Bank)	TA2
EP11	Stranica za plaćanje putem PayPal-a (PSP)	TA2
EP12	Stranica za uspešno/neuspešno plaćanje (Web Shop)	TA2

4. Dijagram toka podataka



5. Identifikacija pretnji

ID	Opis	Uticaj na sistem	Verovatnoća pojavljivanja
	Spoofing:		
T1	Spoofing of Source Data Store	Medium	Low
T2	Spoofing of Destination Data Store	Medium	Low

T3	Spoofing of Web Service Process	High	High
	Tampering:		
T4	Data Store Could Be Corrupted	High	Low
T5	Web Service Memory Tampered	Low	Low
T6	Replay Attacks	High	High
T7	Potential SQL Injection Vulnerability for SQL Database	High	High
T8	XSS-malicious injections	High	Low
	Repudiation:		
T9	Potential Data Repudiation by Web Service	High	Low
T10	Data Store Denies File System/SQL Database Potentially Writing Data	High	Low
	Information disclosure:		
T11	Weak Access Control for a Resource	Medium	Medium
T12	Authorization Bypass	Medium	Medium
T13	Data Flow Sniffing	High	High
T14	Weak Authentication Scheme	High	Low
	Denial of Service:		
T15	Potential Process Crash or Stop for Web Service	High	Medium
T16	Data Flow is Potentially Interrupted	High	High
T17	Data Store Inaccessible	High	Low
T18	Potential Excessive Resource Consumption	High	Medium
T19	Repeated bot attacks	Medium	Low
	Elevation of privilege:		
T20	Web Service May be Subject to Elevation of Privilege Using Remote Code Execution	High	High
T21	Elevation by Changing the Execution Flow in Web Service	Medium	High
T22	Elevation Using Impresonation	Medium	Medium
T23	Cross Site Request Forgery	Medium	Low

6. Analiza rizika

Rizik = Verovatnoća * Uticaj na sistem

Uticaj / Verov.	Low	Medium	High
Low	Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	High

ID	Opis	Rizik
	Spoofing:	
T1	Spoofing of Source Data Store	Low
T2	Spoofing of Destination Data Store	Low
T3	Spoofing of Web Service Process	High
	Tampering:	
T4	Data Store Could Be Corrupted	Medium
T5	Web Service Memory Tampered	Low
T6	Replay Attacks	High
T7	Potential SQL Injection Vulnerability for SQL Database	High
T8	XSS-malicious injections	Medium
	Repudiation:	
T9	Potential Data Repudiation by Web Service	Medium
T10	Data Store Denies File System/SQL Database Potentially Writing Data	Medium
	Information disclosure:	
T11	Weak Access Control for a Resource	Medium
T12	Authorization Bypass	Medium
T13	Data Flow Sniffing	High
T14	Weak Authentication Scheme	Medium
	Denial of Service:	
T15	Potential Process Crash or Stop for Web Service	High
T16	Data Flow is Potentially Interrupted	High
T17	Data Store Inaccessible	Medium
T18	Potential Excessive Resource Consumption	High
T19	Repeated bot attacks	Low
	Elevation of privilege:	
T20	Web Service May be Subject to Elevation of Privilege Using Remote Code Execution	High
T21	Elevation by Changing the Execution Flow in Web Service	High
T22	Elevation Using Impresonation	Medium
T23	Cross Site Request Forgery	Low

7. Protivmere

ID	Opis	Protivmere
	Spoofing:	
T1	Spoofing of Source Data Store	Da, HTTPS komunikacija je enkriptovana.
T2	Spoofing of Destination Data Store	Da, HTTPS komunikacija je enkriptovana.
T3	Spoofing of Web Service Process	Da, autentifikacijom, HTTPS komunikacija je enkriptovana.
	Tampering:	

T4	Data Store Could Be Corrupted	Ne, antivirus softveri će biti razmatrani na višem nivou bezbednosti.
T5	Web Service Memory Tampered	Da, prosleđivanjem podataka umesto pokazivača, korišćenje HTTPS-a (TLS), ne smeštamo podatke u fajlove.
T6	Replay Attacks	Da, upotrebom HTTPS-a, ograničavanjem trajanja i invalidacijom tokena, blokiranjem naloga usled neuspešnih pokušaja prijavljivanja na sistem.
T7	Potential SQL Injection Vulnerability for SQL Database	Da, prepared statement queries kreirani su u repository sloju, ispravno filtriranje, korišćenje Hibernate-a.
T8	XSS-malicious injections	Da, XSS sanitizer, ESAPI properties.
	Repudiation:	
T9	Potential Data Repudiation by Web Service	Da, logging podataka i akcija i čuvanje u log fajlovima.
T10	Data Store Denies File System/SQL Database Potentially Writing Data	Da, logging podataka i akcija i čuvanje u log fajlovima.
	Information disclosure:	
T11	Weak Access Control for a Resource	Da, autorizacija i autentifikacija.
T12	Authorization Bypass	1. Ne, potrebna dodatna autorizacija i ne ostavljati ,,otvorena vrata'' prilikom ažuriranja koda. 2. Da, odrađena autorizacija se obavlja.
T13	Data Flow Sniffing	Da, HTTPS komunikacija je enkriptovana, osetljivi i bitni podaci su enkriptovani.
T14	Weak Authentication Scheme	Da, upotrebnom jedinstvenog mejla i primoravanjem na korišćenje jake lozinke uz poštovanje šablona.
	Denial of Service:	
T15	Potential Process Crash or Stop for Web Service	Da, pokretanjem više instanci, try-catch blok.
T16	Data Flow is Potentially Interrupted	Da, HTTPS komunikacija je enkriptovana, osetvljivi i bitni podaci su enkriptovani, otklonjenji maliciozni upiti ka bazi.
T17	Data Store Inaccessible	Ne, potrebno konstantno praviti backup baze u određenim intervalima .

T18	Potential Excessive Resource Consumption	Ne
T19	Repeated bot attacks	Ne, potrebno korišćenje load balancing-a i klastera.
	Elevation of privilege:	
T20	Web Service May be Subject to Elevation of Privilege Using Remote Code Execution	Da, sanitizer, escape-ovanjem i validacijom podataka.
T21	Elevation by Changing the Execution Flow in Web Service	Da, sanitizer, escape-ovanjem i validacijom podataka.
T21	Elevation Using Impresonation	Da, autorizaija i autentifikacija korisnika.
T23	Cross Site Request Forgery	1. Da, slanje tokena tokom svakog korisnikovog zahteva.. 2. Ne, postoji mogućnost za unapređenje zaštite na svim mestima.