Model pretnji

Tim 8: *Jelena Popov, Nikola Brodić, Dušan Nikolić*

1. Resursi od značaja

ID	Naziv	Opis
A1	Kredencijali korisnika	Kredencijali koje korisnici koriste za prijavu na sistem.
A2	Lični podaci korisnika	First Name, Last Name, E-mail, City, Country...
A3	Podaci za plaćanje	MerchantId, MerchantPassword, ClientId, ClientSecret, PAN, Security Code...
A4	Baze podataka	Čuvaju sve podatke neophodne za funkcionisanje pojedinačnih servisa.
A5	Biznis logika Literary Society servisa	Sve funkcionalnosti koje servis obezbeđuje.
A6	Biznis logika Literary Society servisa	Sve funkcionalnosti koje servis obezbeđuje.
A7	Biznis logika Payment Gateway servisa	Sve funkcionalnosti koje servis obezbeđuje.
A8	Biznis logika PayPal servisa	Sve funkcionalnosti koje servis obezbeđuje.
A9	Biznis logika Bitcoin servisa	Sve funkcionalnosti koje servis obezbeđuje.
A10	Biznis logika Bank servisa	Sve funkcionalnosti koje servis obezbeđuje.
A11	Biznis logika PCC servisa	Sve funkcionalnosti koje servis obezbeđuje.
A12	API Gateway	Obezbeđuje komunikaciju između dostupnih servisa.
A13	Skladišni prostor za datoteke	Sadrži dokumenti koje servisi čuvaju i koriste.
A14	Repozitorijumi za skladištenje sertifikata (*keystore, truststore*)	Sadrže sertifikate odgovarajućih servisa i servisa kojima se veruje.
A15	Konfiguracione datoteke	Sadrže konfiguraciju komponenti sistema.

2. Nivoi poverenja korisnika sistema

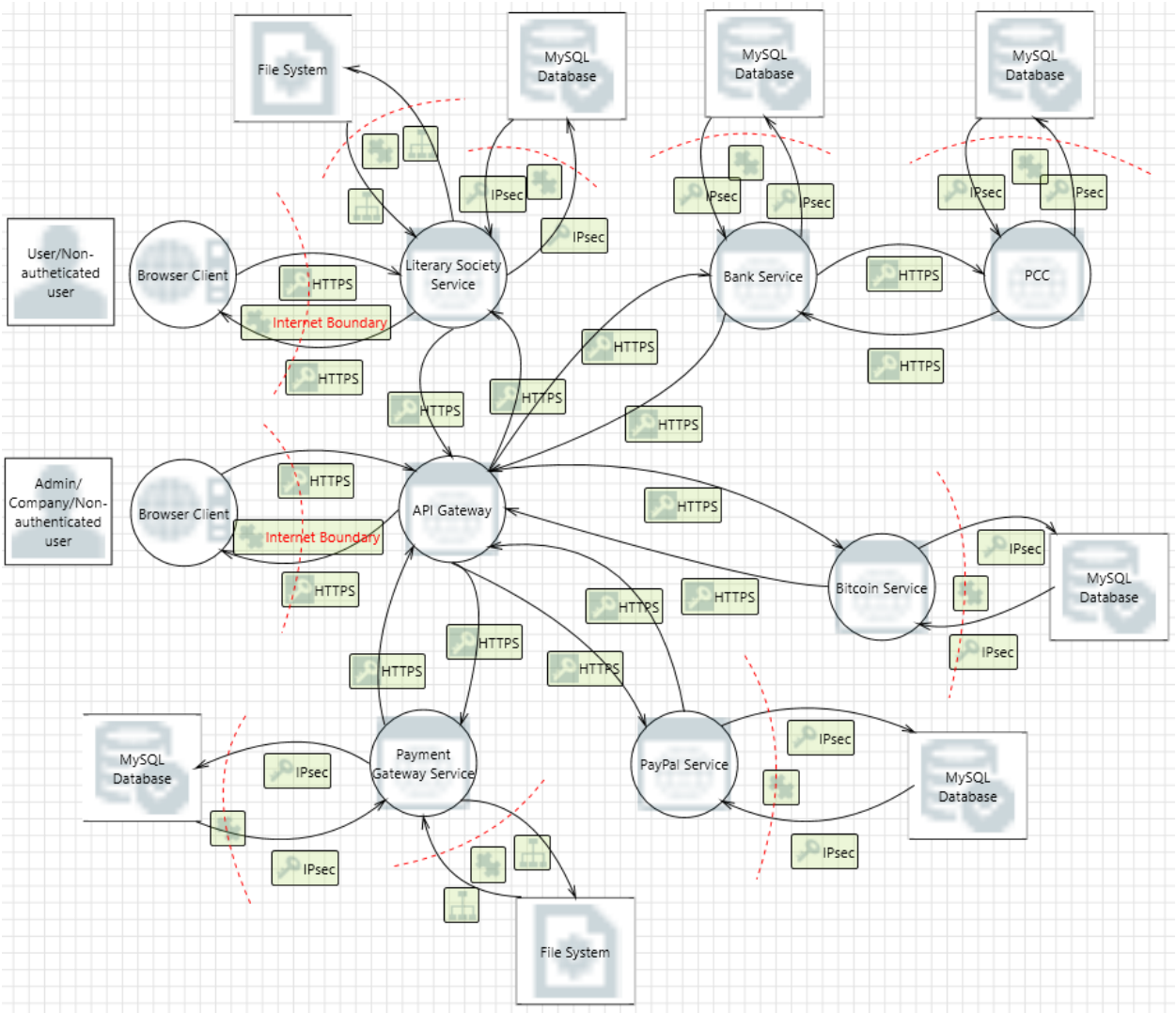
ID	Naziv	Opis
TA1	Neregistrovani korisnik Literary Society servisa	Pretražuje i kupuje dostupne knjige.
TA2	Administrator Literary Society servisa	Obrađuje zahteve za registaciju i upravlja načinima plaćanja koje Literary Society servis podržava.
TA3	Prodavac Literary Society servisa	Oglašava knjige koje želi da prodaje.
TA4	Pisac Literary Society servisa	Izdaje knjige i kupuje članarinu jednokratno ili putem pretplate.
TA5	Čitalac Literary Society servisa	Kupuje i preuzima dostupne knjige. Ako je beta-čitalac, učestvuje u procesu izdavanja knjige davanjem komentara na rukopis.

TA6	Urednik Literary Society servisa	Kupuje i preuzima dostupne knjige. Učestvuje u procesu izdavanja knjige kao glavni urednik.
TA7	Lektor Literary Society servisa	Kupuje i preuzima dostupne knjige. Učestvuje u procesu izdavanja knjige kao lektor.
TA8	Član odbora Literary Society servisa	Kupuje i preuzima dostupne knjige. Učestvuje u procesu registracije pisca i procesu utvrđivanja plagijarizma kao član odbora.
TA9	Neregistrovani korisnik Payment Gateway servisa	Kreira zahtev za registrovanje nove kompanije ili novog načina plaćanja.
TA10	Administrator Payment Gateway servisa	Obrađuje zahteve za registraciju novih kompanija i novih načina plaćanja.
TA11	Kompanija Payment Gateway servisa	Prosleđuje zahteve za plaćanje ka Payment Gateway-u.

3. Ulazne tačke sistema

ID	Naziv	Nivoi poverenja
EP1	Stranica za prijavu na sistem (Literary Society)	TA2 - TA8
EP2	Stranica za registraciju na sistem (Literary Society)	TA1
EP3	Stranica za verifikaciju email adrese (Literary Society)	TA1
EP4	Stranica za resetovanje lozinke (Literary Society)	TA2 - TA8
EP5	Stranica za promenu lozinke (Literary Society)	TA2 - TA8
EP6	Stranica za obradu zahteva za registraciju (Literary Society)	TA2
EP7	Stranica za upravljanje podržanim načinima plaćanja (Literary Society)	TA2
EP8	Stanica za dodavanje knjige (Literary Society)	TA3
EP9	Stranica za unos podataka za podršku dostupnih načina plaćanja (Literary Society)	TA3
EP10	Stranica za izvršavanje dodeljenog zadatka (Literary Society)	TA4 - TA8
EP11	Stranica za kreiranje zahteva za izdavanje knjige (Literary Society)	TA4
EP12	Stranica za kupovinu članarine (Literary Society)	TA4, TA5
EP13	Stranica za pretplatu na članarinu (Literary Society)	TA4, TA5
EP14	Stranica za registraciju kompanije (Payment Gateway)	TA9
EP15	Stranica za registraciju načina plaćanja (Payment Gateway)	TA9
EP16	Stranica za prijavu na sistem (Payment Gateway)	TA10
EP17	Stranica za promenu lozinke (Payment Gateway)	TA10
EP18	Stranica za obradu zahteva za registraciju kompanija i načina plaćanja (Payment Gateway)	TA10

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 the Web Service Process	High	High
	Tampering:		
T4	Data Store Could Be Corrupted	High	Medium
T5	Web Service Memory Tampered	Low	Low

T6	Replay Attacks	High	Medium
T7	Potential SQL Injection Vulnerability for SQL Database	High	High
	Repudiation:		
T8	Potential Data Repudiation by Web Service	High	Low
T9	Data Store Denies File System/SQL Database Potentially Writing Data	High	Low
	Information disclosure:		
T10	Weak Access Control for a Resource	Low	Medium
T11	Authorization Bypass	Medium	Medium
T12	Data Flow Sniffing	High	High
T13	Weak Authentication Scheme	High	High
	Denial of Service:		
T14	Potential Process Crash or Stop for Web Service	High	Medium
T15	Data Flow Is Potentially Interrupted	High	High
T16	Data Store Inaccessible	High	Low
T17	Potential Excessive Resource Consumption	High	Medium
	Elevation of privilege:		
T18	Web Service May be Subject to Elevation of Privilege Using Remote Code Execution	High	High
T19	Elevation by Changing the Execution Flow in Web Service	Medium	High
T20	Elevation Using Impersonation	Medium	Medium
T21	Cross Site Request Forgery	Medium	Low

6. Analiza rizika

Rizik = Verovatnoća pojavljivanja * Uticaj na sistem

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

7. Protivmere

ID	Opis	Protivmere
	Spoofing:	
T1	Spoofing of Source Data Store	Ne
T2	Spoofing of Destination Data Store	Ne
T3	Spoofing the Web Service Process	Da, autentifikacijom upotrebom Spring Security

	Tampering:	
T4	Data Store Could Be Corrupted	Ne
T5	Web Service Memory Tampered	Da, prosleđivanjem podataka umesto pokazivača
T6	Replay Attacks	Da, upotrebom HTTPS-a i ograničavanjem trajanja i invalidacijom tokena
T7	Potential SQL Injection Vulnerability for SQL Database	Da, MySQL ne dozvoljava izvršavanje multi-statement-a
	Repudiation:	
T8	Potential Data Repudiation by Web Service	Da, logging-om podataka
T9	Data Store Denies File System/MySQL Database Potentially Writing Data	Da, logging-om podataka
	Information disclosure:	
T10	Weak Access Control for a Resource	Da, definisanjem prava pristupa
T11	Authorization Bypass	Ne
T12	Data Flow Sniffing	Da, upotrebom HTTPS-a i šifrovanjem osetljivih podataka
T13	Weak Authentication Scheme	Da, definisanjem pattern-a za lozinku, proverom sa kompromitovanim lozinkama...
	Denial of Service:	
T14	Potential Process Crash or Stop for Web Service	Da, pokretanjem više instanci
T15	Data Flow Is Potentially Interrupted	Da, upotrebom HTTPS-a i šifrovanjem osetljivih podataka
T16	Data Store Inaccessible	Ne
T17	Potential Excessive Resource Consumption	Ne
	Elevation of privilege:	
T18	Web Service May be Subject to Elevation of Privilege Using Remote Code Execution	Da, sanatizacijom, escape-ovanjem i validacijom podataka
T19	Elevation by Changing the Execution Flow in Web Service	Da, sanatizacijom, escape-ovanjem i validacijom podataka
T20	Elevation Using Impersonation	Da, definisanjem privilegija za korisnike i njihovom proverom
T21	Cross Site Request Forgery	Ne