Model pretnji

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

1. Resursi od značaja

ID	NAZIV	OPIS
A1	Kredencijali korisnika	Kredencijali koje korisnici koriste za prijavu na sistem (email adresa, lozinka)
A2	Lični podaci korisnika	Ime, prezime, email adresa...
A3	Podaci neophodni za plaćanje	PAN, Security Code, Merchant Id, Merchant password...
A4	Baze podataka	Skladište podatke neophodne za funkcionisanje
A5	Biznis logika psp -a	Funkcionalnosti koje komponenta sistema obezbeđuje
A6	Biznis logika bank servisa	Funkcionalnosti koje komponenta sistema obezbeđuje
A7	Biznis logika PCC servisa	Funkcionalnosti koje komponenta sistema obezbeđuje
A8	Biznis logika paypal servisa	Funkcionalnosti koje komponenta sistema obezbeđuje
A9	Biznis logika bitcoin servisa	Funkcionalnosti koje komponenta sistema obezbeđuje
A10	API gateway	Komunikacija između servisa
A11	Keystore, truststore	Sertifikati servisa
A12	Konfiguracione datoteke	Konfiguracija servisa
A13	Ostale datoteke za skladištenje podataka	Log datoteke, ...

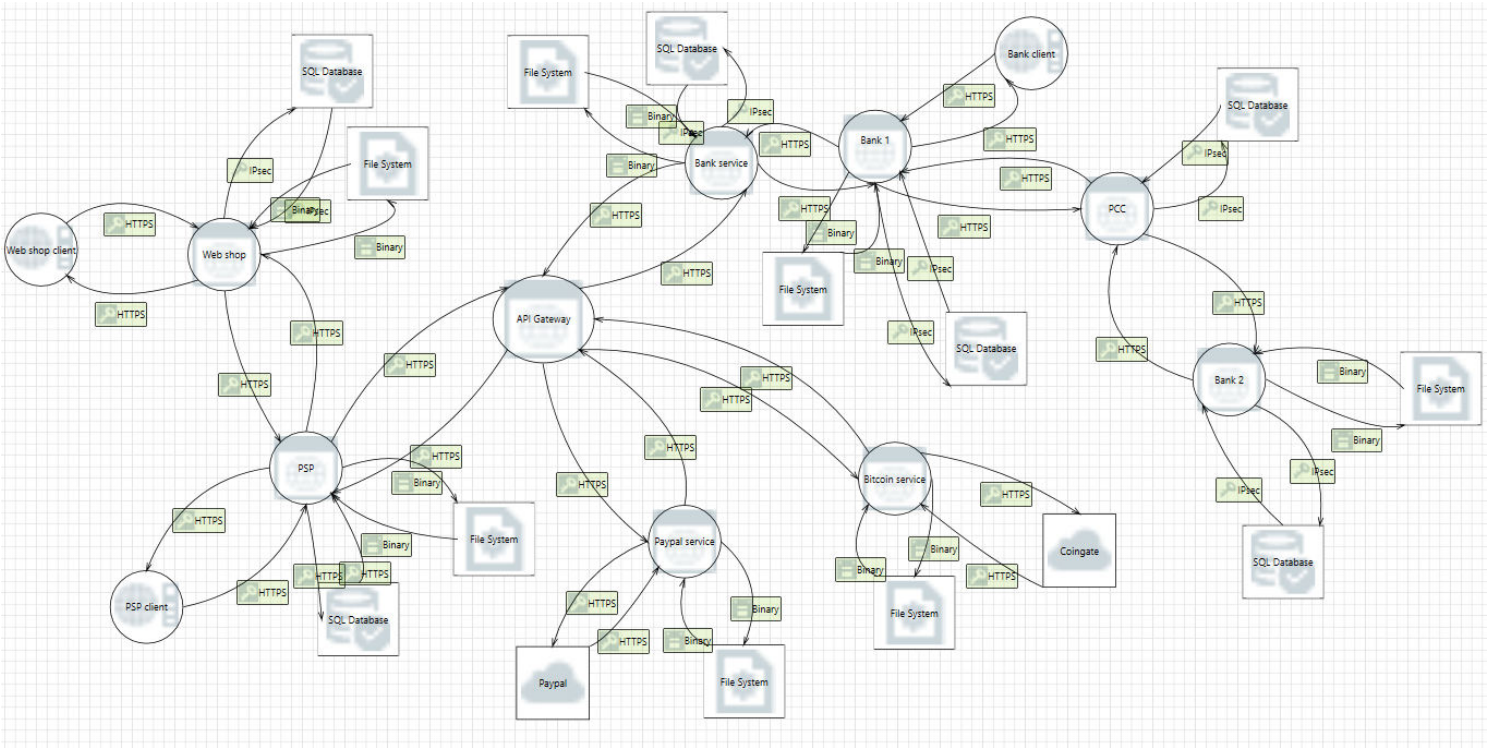
2. Nivoi poverenja korisnika sistema

ID	NAZIV	OPIS
TA1	Prodavac	Prodaje opremu/kurseve/konferencije
TA2	Šef nabavke	Zadužen za kupovinu opreme
TA3	Član opšte službe	Zadužen za kupovinu kurseva/konferencija

3. Ulazne tačke sistema

ID	NAZIV	NIVO POVERENJA
EP1	Stranica za prijavu na sistem (Web shop)	TA1-TA3
EP2	Stranica za kupovinu opreme (Web shop)	TA2
EP3	Stranica za kupovinu kursa/konferencije (Web shop)	TA3
EP4	Stranica za pretplatu	TA3
EP5	Stranica za prijavu na sistem (PSP)	TA1
EP6	Stranica za registraciju na sistem (PSP)	TA1
EP7	Stranica za verifikaciju	TA1
EP8	Stranica za registraciju načina plaćanja (PSP)	TA1
EP9	Stranica za izmenu podržanih načina plaćanja (PSP)	TA1
EP10	Stranica za unos podataka za plaćanje putem banke (Bank)	TA2-TA3

4. Dijagram toka podataka



5. Identifikacija pretnji

ID	OPIS	STRIDE	UTICAJ NA SISTEM	VEROVATNOĆA POJAVLJIVANJA
T1	Gubitak identiteta (korisnik ostavi svoje kredencijale na javnom mestu ili ih podeli sa nekim)	S	L	H
T2	Krađa ili zloupotreba identiteta	S	H	M
T3	Kompromitovanje ličnih podataka korisnika	S	H	L
T4	Lažno predstavljanje	S	H	M
T5	Neautorizovan pristup podacima	T	H	L
T6	Napad na neporecivost (napadač pristupa log datotekama i menja ih u svoju korist)	R	L	L
T7	Replay napadi	I	H	M
T8	Neautorizovan pristup (pristup funkcionalnostima za koje nije autorizovan)	I	M	M
T9	Narušavanje dostupnosti servisa	D	H	L

Objašnjenje:

S - Spoofing – pretvaranje napadača da je neko drugi

T – Tampering – izmena podataka na disku, u memoriji, na mreži...

R – Repudiation – napadač tvrdi da nije uradio nešto

I – Information disclosure – pružiti informacije nekome ko za to nije autorizovan

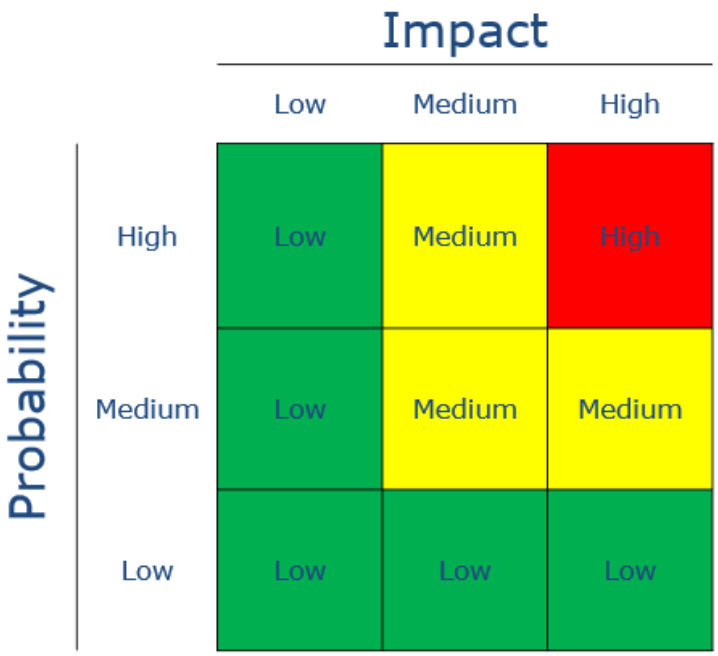
D – Denial of service – ukidanje pristupa servisu/podacima

E – Elevation of privilege – dozvola da neko izvrši operaciju za koju nije autorizovan

H – High, **M** – Medium, **L** – Low

6. Analiza rizika

Rizik = verovatnoća pojavljivanja * uticaj na sistem



ID	RIZIK
T1	L
T2	M
T3	L
T4	M
T5	L
T6	L
T7	M
T8	M
T9	L

7. Protivmere

ID	PROTIVMERA
T1	Ne
T2	Password policy, invalidiranje tokena, blokiranje korisnika nakon neuspešne prijave (tri puta), heširanje lozinke, itd.
T3	Šifrovanje podataka
T4	Verifikacija prilikom registrovanja, dalji rad, two-way authentication
T5	Definisanje prava pristupa
T6	Onemogućavanja pristupa log datotekama
T7	Upotrebom HTTPS-a i ograničavanjem trajanja i invalidiranjem tokena
T8	Definisanje prava pristupa
T9	Ne