Integritet i sigurnost baza podataka

dr Jasmina Novaković

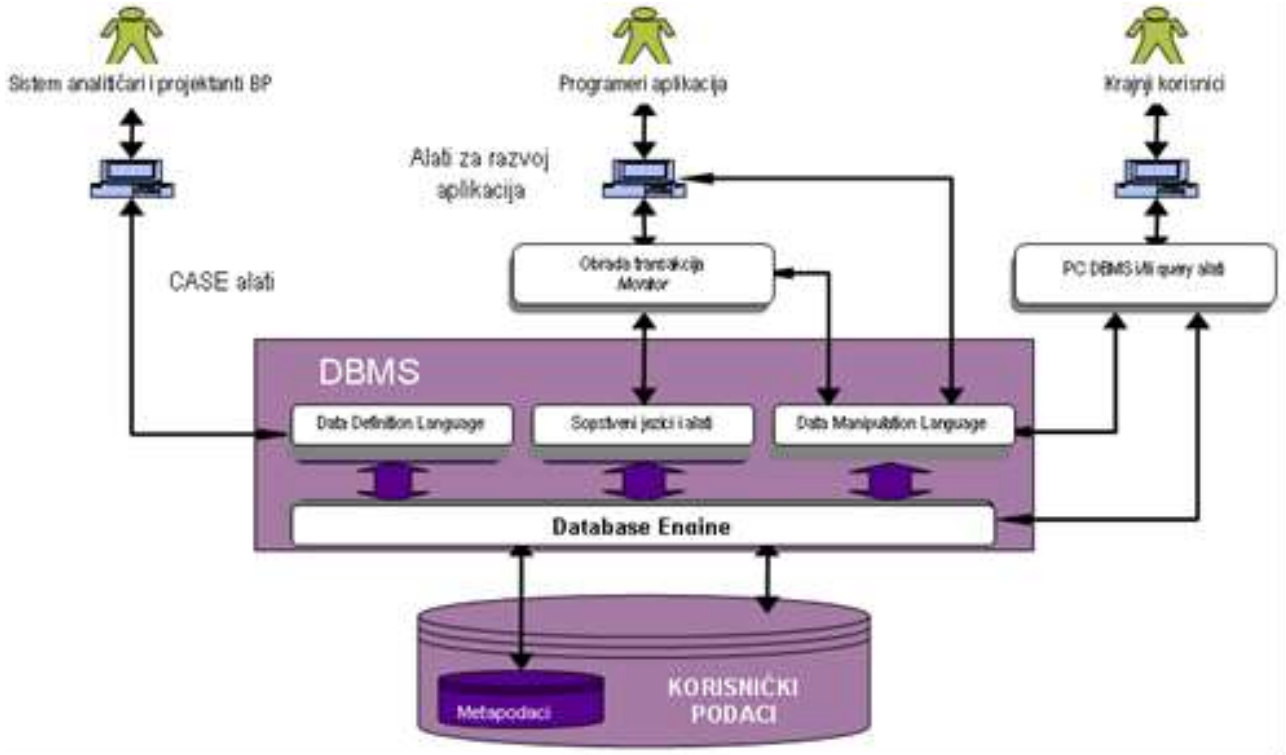
8. INTEGRITET I SIGURNOST BAZA PODATAKA

- U ovom delu razmatra se zaštita baze podataka kroz dva aspekta i to: integritet – zaštitu od slučajnog pogrešnog ažuriranja i sigurnost – zaštitu od neovlašćenog ažuriranja i korišćenja podataka.
- Definišu se problemi čije rešavanje je nužno da bi velika višekorisnička baza podataka mogla uspešno funkcionisati.
- Proučavaju se transakcije koje predstavljaju niz operacija nad bazom podataka i odgovaraju jednoj logičkoj jedinici posla u realnom sistemu.
- Analiziraju se napadi koji se realizuju ubacivanjem koda koji se tretira kao SQL kod.
- Posebno je objašnjena SQL injection ranjivost veb-sajtova koji se oslanjaju na baze podataka.

Nakon proučavanja ovog dela, trebalo bi da možete da:

- definišete koncepte zaštite baza podataka;
- definišete integritet i sigurnost baza podataka;
- razumete transakcije u bazama podataka;
- razumete SQL injection napade.

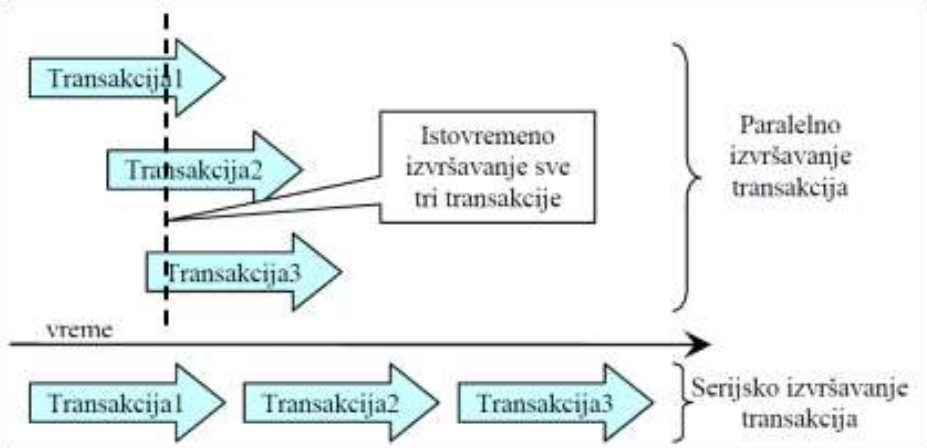
Tipična DBMS arhitektura



Integritet i sigurnost

- Pravila integriteta se dele u dve klase:
  - **Pravila integriteta domena** – definišu se za vrednosti pojedinih atributa nezavisno od vrednosti ostalih atributa u bazi podataka (karakterističan primer je integritet objekta), i
  - **Pravila integriteta relacija** – odnose se na relaciju kao celinu, odnosno definišu kada neka *n*-torka može da se ubaci u relaciju ili kako *n*-torke jedne relacije zavise od *n*-torki druge relacije (karakterističan primer je referencijalni integritet).
- Termin **sigurnost** podataka podrazumeva mehanizme zaštite baze podataka od neovlašćenog korišćenja.

Paralelno i serijsko izvršavanje transakcija



SQL injection napad

- Napad koji se realizuju ubacivanjem koda u kojima su ulazni podaci uključeni u dinamički konstruisan SQL upit, i koji se tretira kao SQL kod predstavlja SQL injection napad.
- SQL injection ranjivost je posebno izražena na veb-sajtovima koji se oslanjaju na baze podataka, jer ih napadači lako nalaze i prodiru u bazu podataka.

SQL injection napadi

- tautologija,
- nelegalni upiti,
- upiti sa unijom,
- nadovezani upiti,
- napadi zaključivanjem.

Tautologija

- Tautologija je iskazna formula koja je istinita u svim mogućim interpretacijama. Jednostavnije govoreći, tautologija je **izraz koji je uvek tačan**, bez obzira na okolnosti.
- Cilj napada zasnovan na tautologiji je da se ubrizga kod u jednu ili više uslovnih naredbi tako da uvek vraćaju vrednost **TRUE**.
- Ovaj napad se koristi za zaobilaženje autentifikacije korisnika i izvlačenje podataka.

Nelegalni upiti

- Nelegalni upiti imaju za cilj otkrivanje ranjivih parametara, otkrivanje šeme baze podataka i pristup podacima.
- Da bi se ovo ostvarilo unose se sekvence koje će rezultovati greškom na serveru baze podataka.
- Prilikom ispisa podataka o nastalom problemu, često se mogu uočiti podaci o arhitekturi sistema koje korisnici ne bi trebalo da vide.