SIGURNOST RAČUNARSKIH MREŽA (SRM)

Tema 11:

Sigurnost baza podataka

URLs:

- Zvanična Web strana: www.viser.edu.rs/predmeti.php?id=122
- Dodatni resursi: www.conwex.info/draganp/teaching.html
- Knjige:

  www.conwex.info/draganp/books.html
- Teme za seminarske radove:

  www.conwex.info/draganp/SRM_seminarski_radovi.html

Napomena

- Ovo je skraćena verzija prezentacije / predavanja na temu **“Sigurnost baza podataka”**

Sigurnost baza podataka

- Sadržaj poglavlja i predavanja:
  - 11.1 Kontrola pristupa
  - 11.2 Ostali aspekti zaštite
  - 11.3 Napad SQL injection

Quote

"Where is the wisdom we have lost in knowledge? Where is the knowledge we have lost in information?"

– T. S. Eliot

Potrebna predznanja

- Programiranje
- Za primenu:
  - Računarske mreže i protokoli
  - Operativni sistemi
  - Sistemsko programiranje
  - Strukture i modeli podataka, baze podataka

Uopšteno o problemu

- Serveri baza podataka (engl. *Database servers*) su verovatno među najvažnijim serverima svake institucije ili kompanije.
- Razvoj Interneta i višeslojnih arhitektura doveo je do toga da su mnogi serveri baza podataka praktično „javno dostupni“, tj. da korisnici mogu da im pristupe preko posebne aplikacije koja se izvršava na Web serveru koristeći samo čitač Weba (engl. *Web browser*).
- Ovo predavanje se bavi onim aspektom sigurnosti koji spada u takozvanu „sivu zonu“ odgovornosti. Punu odgovornost za zaštitu baze podataka administrator mreže najverovatnije neće preuzeti, jer provera postojanja SQL upita u podacima koje unosi korisnik zaista i nije njegov posao. S druge strane, od projektanta i administratora baze podataka ne možete očekivati da vam konfigurišu mrežnu barijeru i formiraju šifrovan tunel ka serveru baze podataka.

11.1 Kontrola pristupa

- **Tabele** (engl. *tables*) su objekti koji služe za skladištenje podataka.
- **Indeksi** (engl. *index*) su specijalne tabele koje omogućavaju brz pristup podacima u tabeli (ukoliko je tabela indeksirana po atributu po kom se vrši pretraživanje).
- **Pogledi** (engl. *views*) omogućavaju izdvajanje podskupa informacija iz tabele ili grupe tabela (podskup redova i/ili kolona).

Provera identiteta korisnika

- Sistem za upravljanje bazama podataka (engl. *DataBase Management System, DBMS*)
- Korisnici se na bazu prijavljuju pomoću korisničkih naloga koje pravi administrator baze podataka. Administrator korisnicima zadaje inicijalnu lozinku čiji se heš čuva u bazi, a korisnik može promeniti svoju lozinku kada god želi. Korisnik mora uneti ispravnu lozinku pri povezivanju na bazu, da bi se sprečila neautorizovana upotreba. Na ovaj način se, korišćenjem informacija smeštenih u bazi, proverava identitet korisnika. Administrator baze podataka može definisati pravila za složenost lozinke, kojim bi se odredila minimalna dužina, ili obavezna upotreba malih slova, velikih slova i cifara.
- Lozinke za prijavljivanje korisnika na bazu ne treba čuvati u bazi podataka u obliku otvorenog teksta.
- Neki sistemi za upravljanje bazama podataka obezbeđuju više metoda za proveru identiteta korisnika.

Ovlašćenja i uloge

- Korisnicima se dodeljuju ovlašćenja (engl. privileges) za povezivanje na bazu i rad sa njenim objektima.
- Ovlašćenja korisnicima može dodeljivati administrator baze, vlasnik objekata ili neki drugi autorizovani korisnik kome je dato to pravo.
- Ovlašćenja omogućavaju korisnicima da obavljaju određene akcije nad bazom (sistemska ovlašćenja) ili objektima baze (objektna ovlašćenja).

Sistemska i objektna ovlašćenja

- **Sistemska ovlašćenja** najčešće dodeljuje administrator baze podataka.
  - U ova ovlašćenja spadaju, na primer, CREATE DATABASE, CREATE PROCEDURE, CREATE TABLE, CREATE VIEW i CREATE USER, koja redom dozvoljavaju korisniku da krera novu bazu podataka, uskladištenu proceduru, tabelu, pogled i novi korisnički nalog.
- **Objektna ovlašćenja** korisniku omogućavaju da izvrši operacije nad konkretnim objektima baze (kao što su tabele, pogledi i uskladištene procedure).
  - Ako korisnik treba da vidi podatke neke tabele, potrebno mu je dodeliti SELECT ovlašćenje nad tom tabelom (isto važi za INSERT, UPDATE, DELETE, ...).
  - Dakle, ovaj vid zaštite podrazumeva da se za svaku tabelu koja se nalazi u bazi posebno odrede prava pristupa za svakog korisnika.
  - Na primer, korisnik koji vrši unos podataka može imati samo pravo upisa (INSERT) dok drugi korisnik može samo vršiti izmene (UPDATE).

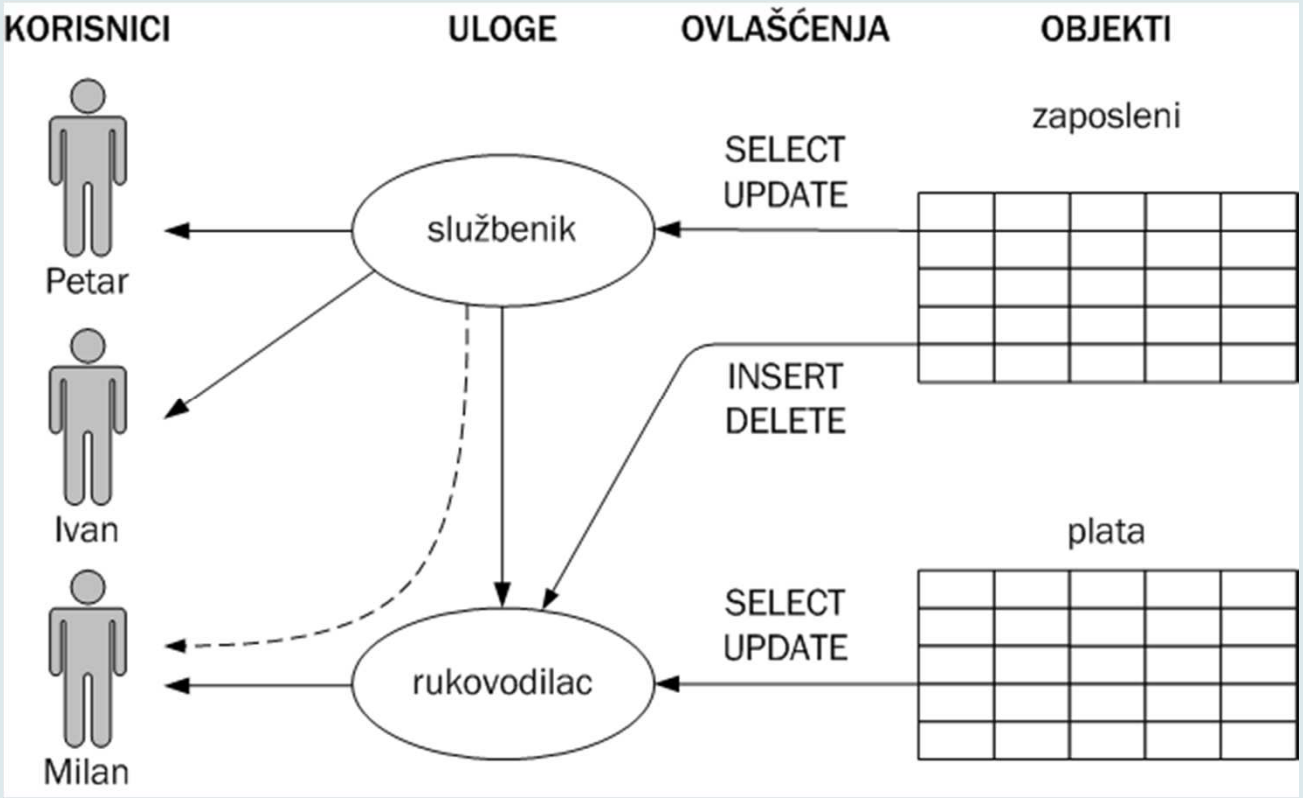
Princip minimalnih ovlašćenja

- Princip minimalnih ovlašćenja predviđa da korisnicima treba dodeliti samo minimum ovlašćenja potrebnih za obavljanje njihovih poslova nad bazom. To takođe predviđa:
  - granularnost ovlašćenja, kao sredstvo za ograničavanje pristupnih prava
  - upotrebu uloga, koje sadrže grupe (skup) ovlašćenja i olakšavaju administraciju
  - upotrebu pogleda, koji ograničavaju pristup na definisane podskupove postojećih podataka
  - upotrebu uskladištenih procedura, čijom se upotrebom može izbeći dodela konkretnih prava nad baznim tabelama korisnicima.

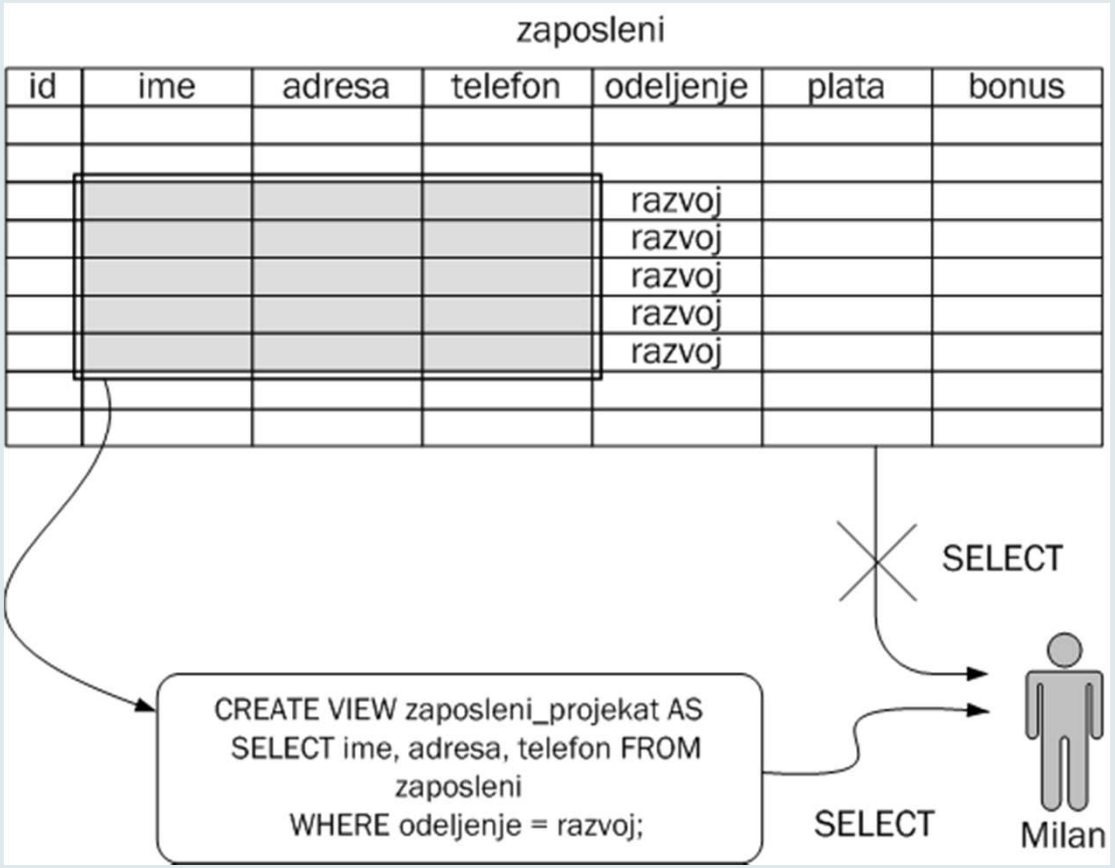
Uloge

- Upravljanje ovlašćenjima može biti veoma složen posao.
- Da bi se pojednostavila administracija korisnika i prava koja imaju u sistemu, koristi se sistem uloga (engl. *roles*).
- Uloge su korisnički definisane kolekcije ovlašćenja, koje se mogu dodeljivati ili oduzimati drugim korisnicima, ili čak drugim ulogama.
- Jednom korisniku ili grupi korisnika može se dodeliti jedna uloga ili grupa uloga.
- Dodavanjem novih ovlašćenja ulozi, svi korisnici koji pripadaju toj ulozi, automatski dobijaju novo ovlašćenje.

Upotreba uloga



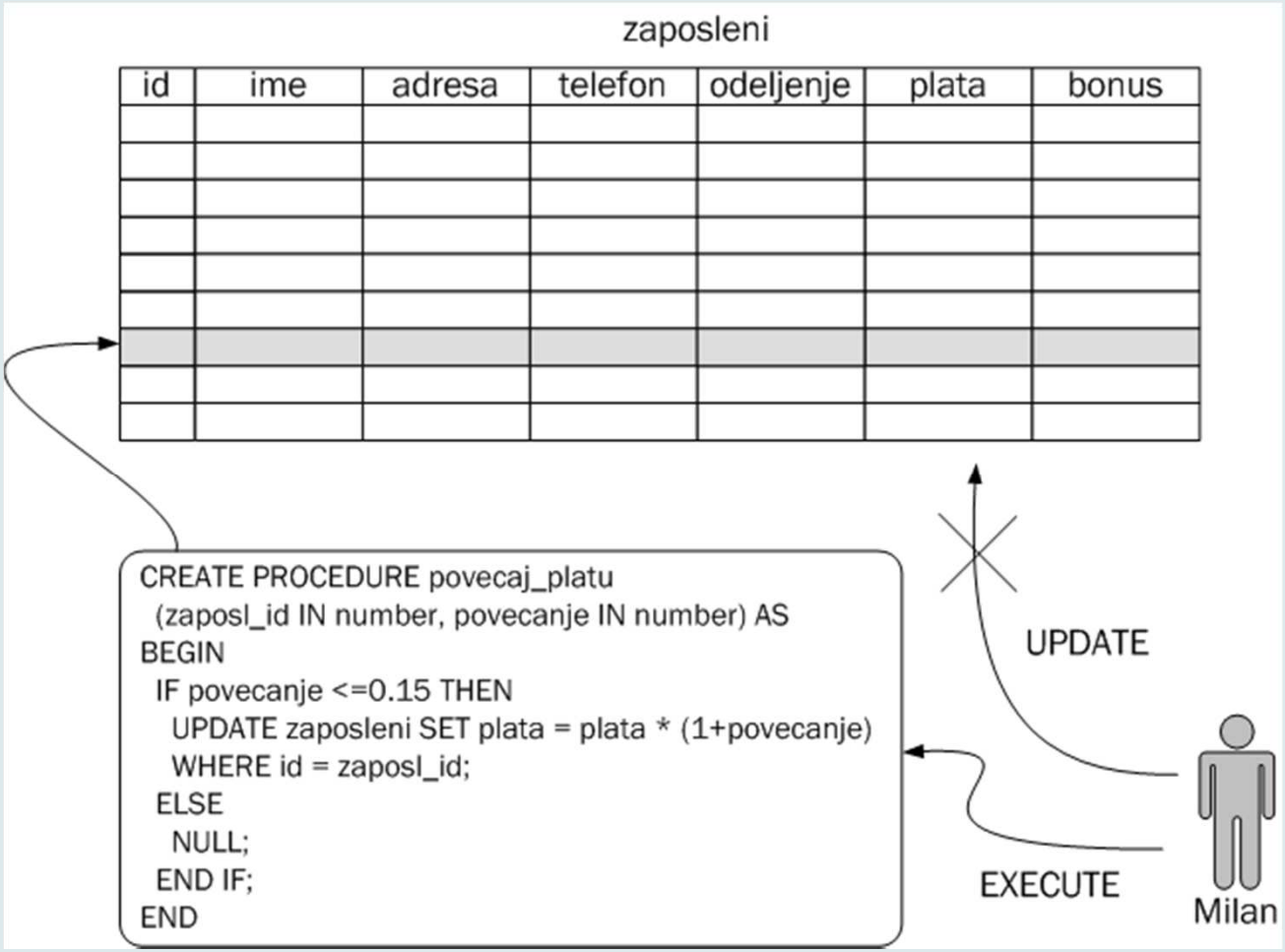
Upotreba pogleda



Uskladištene procedure i okidači

- Uskladištene procedure (engl. *stored procedures*) čine skup instrukcija koje se u prevedenoj formi čuvaju u bazi. Postoje dva tipa: procedure (ne vraćaju vrednost) i funkcije (vraćaju vrednost).
- Paket je grupa uskladištenih procedura koje se zajedno čuvaju i održavaju.
- Okidači (engl. *triggers*) su uskladišteni, događajima upravljani (engl. *event-driven*) programi koji se izvršavaju usled pojave događaja za koji su vezani. Događaji za koje se mogu vezati okidači najčešće su izvršenje INSERT, UPDATE ili DELETE SQL upita.

Upotreba uskladištene procedure - primer



Virtuelne privatne baze podataka

- Virtuelna privatna baza podataka (VPD) omogućava granularnu kontrolu pristupa pridruživanjem jednog ili više sigurnosnih pravila (engl. *policy*) tabelama ili pogledima.
- U slučaju direktnog ili indirektnog pristupa tabeli kojoj je pridruženo sigurnosno pravilo, server podataka poziva funkciju sigurnosnog pravila.
- Funkcija sigurnosnog pravila vraća uslov pristupa koji se naziva predikat (WHERE klauzula) koji se dodaje izvornom SQL iskazu.

11.2 Ostali aspekti zaštite

- Upotreba najnovijih zakrpa za DBMS
- Ograničavanje pristupa DBMS serveru
- Korišćenje troslojnog modela
- Skrivanje strukture baze podataka
- Korišćenje složenih lozinki
- Brisanje nepotrebnih objekata
- Provera podrazumevane kontrole pristupa
- Provera ulaznih podataka
- Procena mogućnosti proboja

11.3 Napad SQL injection

- Verovatno najosetljivija tačka u pogledu očuvanja sigurnosti baza podataka jeste provera podataka koje korisnik šalje bazi. Ako je posetiocima neke web stranice dozvoljen unos podataka u bazu, potrebno je proveriti da li podaci koje je uneo korisnik sadrže neke SQL naredbe.
  - Na primer, posle poslednjeg unetog podatka, korisnik može uneti komandu DELETE FROM IME_TABLE; COMMIT; Ako ne postoji provera unosa, ova naredba će obrisati neku tabelu iz baze.
- Napad SQL injection je direktna posledica lošeg dizajna aplikacije koja kreira dinamičke SQL upite na osnovu interakcije sa korisnikom. To omogućava napadaču da prosledi bazi podataka SQL upit po svojoj volji. Ukoliko se ovo zanemari i ostavi prostor za mogući napad, svako dalje obezbeđivanje DBMS postaje beskorisno.
- Iako su SQL injection napadi po svojoj prirodi jednostavni (napadač aplikaciji prosleđuje unos koji sadrži SQL upit), poželjno je da napadač koji želi da izmeni podatke u bazi poznaje strukturu baze (koje tabele postoje, od kojih se kolona koja tabela sastoji itd). Izvođenje napada nad bazom čija je struktura nepoznata je znatno komplikovanije.

Vrste SQL Injection napada

- **Modifikacija SQL upita.** Napadač modifikuje SQL upit pomoću skupovnih operacija (najčešće UNION) ili menja WHERE klauzulu sa ciljem dobijanja drugačijeg rezultata. Najpoznatiji napad ove vrste je modifikacija WHERE klauzule upita za proveru identiteta korisnika tako da klauzula uvek daje rezultat TRUE.
- **Umetanje koda.** Napadač unosi novi SQL upit ili novu komandu u postojeći SQL upit. Ova vrsta napada funkcioniše isključivo kod DBMS koji podržavaju višestruke SQL upite po jednom zahtevu bazi podataka (na primer, EXECUTE naredba u MS SQL Serveru). Ovakav napad na Oracle DBMS se teško ostvaruje.
- **Umetanje funkcijskih poziva.** Napadač umeće Oracle-ove ugrađene ili neke korisničke funkcije u ranjiv SQL upit. Ovi funkcijski pozivi se zatim mogu iskoristiti za izvršavanje funkcijskih poziva operativnog sistema ili za izmenu podataka u bazi.
- **Prekoračenja bafera (engl. *buffer overflow*).** Ovo je podvrsta prethodno opisane vrste SQL injection napada. Ranjivost postoji u nekim funkcijama DBMS-a koje mogu izazvati prekoračenje Buffer-a.

Ostalo što može koristiti napadaču

- Korišćenje poruka o greškama
- Određivanje imena tabela i kolona
- Određivanje tipova podataka
- Određivanje verzije DBMS-a
- Određivanje korisničkih imena i lozinki

Zaštita od SQL Injection napada

- SQL Injection napad može biti jednostavno sprečen malim izmenama aplikativnog koda. Programeri aplikacija baza podataka moraju biti disciplinovani u primeni zaštitnih mera za svaku proceduru i funkciju koja može biti dostupna preko mreže. Svaki dinamički SQL iskaz mora biti zaštićen. Jedan nezaštićeni SQL iskaz može dovesti do kompromitovanja aplikacije, podataka ili servera baze podataka.

- Upotreba vezanih promenljivih
- Provera unosa
- Sigurnost funkcija
- Poruke o greškama

Traffic camera SQL Injection attack ☺

Vežbe

- Detalji o problematici sigurnosti baza podataka, kao i praktični primeri, obrađuju se na vežbama iz ovog predmeta

- Takođe, detaljniji opisi i objašnjenja se mogu naći u knjizi koja prati predmet i predavanja **"Sigurnost računarskih sistema i mreža"**

Literatura

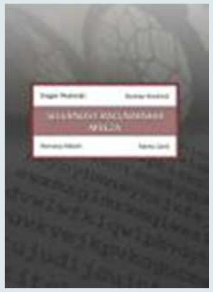
- D. Pleskonjić, N. Maček, B. Đorđević, M. Carić: **"Sigurnost računarskih sistema i mreža"**, Mikro knjiga, Beograd, 2007., ISBN: 978-86-7555-305-2, knjiga – udžbenik
- www.conwex.info/draganp/books_SRSiM.html
- www.mikroknjiga.rs/store/prikaz.php?ref=978-86-7555-305-2

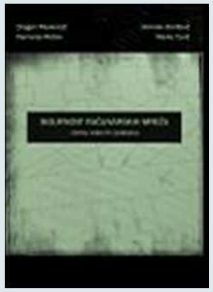
- Za predavanje 11:
  - Poglavlje 11: Sigurnost baza podataka

Literatura - nastavak

- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-16-5, knjiga - udžbenik
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - priručnik za laboratorijske vežbe"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-49-1
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - zbirka rešenih zadataka"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-55-6

www.conwex.info/draganp/books.html





Dodatna literatura

- **Applied Cryptography**
  Bruce Schneier
  John Wiley & Sons, 1995

- **Cryptography and Network Security**
  William Stallings
  Prentice Hall, 1998

- **The CISSP Prep Guide – Mastering the Ten Domains of Computer Security**
  Ronald L. Krutz, Russell Dean Vines
  John Wiley & Sons, 2001

  Druge knjige i razni *online* resursi

- ***Napomena:*** tokom predavanja će biti naglašena dodatna literatura, po potrebi.

Pitanja

?