SIGURNOST OPERACIJSKIH SUSTAVA I APLIKACIJA 2021./2022.

Prva laboratorijska vježba: Autentifikacija i autorizacija

Uvod

OAuth2.0 je industrijski standardni protokol koji omogućuje korisniku da web stranici ili aplikaciji treće strane odobri pristup zaštićenim resursima korisnika, bez nužnog otkrivanja njihovih dugoročnih vjerodajnica ili čak identiteta. OAuth 2.0 se usredotočuje na jednostavnost razvojnog programera klijenta, a istovremeno pruža specifične tokove autorizacije za web aplikacije, desktop aplikacije, mobilne i ostale uređaje. Ova specifikacija i njezina proširenja razvijaju se unutar IETF OAuth radne skupine.

OAuth uvodi **autorizacijski** sloj i odvaja ulogu klijenta od uloge vlasnika resursa. U OAuth-u, klijent zahtijeva pristup resursima koje kontrolira vlasnik i koje se nalaze na poslužitelju i izdaje mu se drugačiji skup vjerodajnica od onih vlasnika resursa. Umjesto korištenja vjerodajnica vlasnika za pristup zaštićenim resursima, klijent dobiva pristupni token - niz koji označava određeni opseg, životni vijek i druge atribute pristupa. Pristupne tokene klijentima treće strane izdaje autorizacijski poslužitelj uz odobrenje vlasnika resursa. Zatim klijent koristi pristupni token za pristup zaštićenim resursima na poslužitelju.

Detaljnije o OAuth2.0 možete pročitati na poveznicama:

- https://auth0.com/docs/authenticate/protocols/oauth
- https://oauth.net/2/

Zadatak

U materijalima za ovu laboratorijsku vježbu nalazi se već implementirana Java web aplikacija izrađena pomoću SpringBoot framework-a (https://spring.io/projects/spring-boot). Aplikacija sadrži dva entiteta: Student i Record. Entitet Student sadrži dva atributa userName i passWord, dok entitet Record sadrži atribute recordName, recordDate, recordOrigin i recordValue. Također oba entiteta sadrže jedinstveni identifikator. Svi podaci kreirani u jednoj sesiji aplikacije se zapisuju u H2 bazu podataka (https://www.h2database.com/html/main.html) kojoj se može pristupiti preko url-a http://localhost:8080/h2-console/ jednom kada je aplikacije pokrenuta. Metode nad resursima koje su dostupne su one za dohvat svih resursa određenog tipa i kreiranje novog resursa određenog tipa. Metodama se može pristupiti preko HTTP zahtjeva GET /students i POST /students odnosno GET /records i POST /records.

Vaš je zadatak modificirati aplikaciju na način da će pratiti svojstva protokola OAuth2.0 za autorizaciju. Resursima trebaju moći pristupati samo autentificirani i autorizirani korisnici u skladu s protokolom. Zaštićene resurse ne smiju moći dohvatiti neovlašteni korisnici, te

autorizacija mora biti implementirana praćenjem svojstva OAuth2.0 protokola i korištenjem JWT tokena. Lozinke spremljene u bazi ne smiju biti zapisane u čistom tekstu (proučiti neke od funkcija za derivaciju ključeva).

Napomene: Iako je dana aplikacija u materijalima, ona ne mora nužno biti korištena već je moguće implementirati svoju aplikaciju (npr. koristeći Django REST framework), no bitno je ispuniti zadatak.

Upute za pokretanje

Izvorni kod aplikacije nalazi se u repozitoriju prve laboratorijske vježbe pod nazivom "Aplikacija". Zip datoteku potrebno je raspakirati, uvesti i pokrenuti na sljedeći način ovisno o IDE-u koji se koristi:

1) Eclipse IDE
    a) Uvoz projekta: File -> Import… -> Maven -> Existing Maven Projects -> <Lokacija root direktorija projekta>
    b) Pokretanje aplikacije: Pokrenuti Lab1Application.java kao Java aplikaciju
2) IntelliJ IDEA
    a) Uvoz projekta: File -> Open -> <Lokacija root direktorija projekta>
    b) Pokretanje aplikacije: Pokrenuti Lab1Application.java kao Java aplikaciju

Predaja

Potrebno je predati:

1. **Izvještaj** koji sadrži postupak modifikacije ili izrade aplikacije (isječci ključnih dijelova aplikacije koji osiguravaju ispravno rješenje postavljenog zadatka). U izvještaju potrebno je dati komentare te isječke demonstracije aplikacije s funkcionalnostima navedenim u zadatku. Preporučamo font veličine 11 pt.

2. **Izvorni kod** modificirane aplikacije

Predajte rješenje u jednoj **zip** datoteci naziva 1_lab_<JMBAG>.zip. Svaka zip datoteke treba sadržavati izvještaj u pdf formatu naziva 1_lab_<JMBAG>.pdf i direktorij imena "Kod" u kojem se nalaze sve datoteke vezane uz izvorni kod.

Rok za predaju vježbe je **2.5.2022. u 23:59.** Za ispunjavanje minimuma i prolaz predmeta potrebno je poslati rješenje laboratorijske vježbe do navedenog roka. Međutim, postoji **parcijalno** bodovanje laboratorija.

U slučaju problema ili nedoumica prilikom izrade vježbe molimo da pravovremeno kontaktirate nastavno osoblje putem mailing liste predmeta sosa@zemris.fer.hr (isključivo koristeći fer.hr adresu) ili putem platforme MS Teams.

Važno: Dozvoljeno je i poželjno diskutiranje mogućih pristupa rješavanju vježbe između studenata. Međutim, samu laboratorijsku vježbu studenti moraju raditi samostalno. Nastavno osoblje će provesti provjere sličnosti predanih rješenja, a ponašanje koje nije u skladu s

Kodeksom ponašanja studenata FER-a ćemo prijaviti Povjerenstvu za stegovnu odgovornost studenata te odrediti dodatne sankcije u sklopu predmeta.