Projektni zadatak iz predmeta

Bezbednost u sistemima elektronskog poslovanja

Računarstvo i automatika - generacija 2022/2023.

1. Namena sistema

U okviru projektnog zadatka potrebno je implementirati informacioni sistem koji vodi evidenciju zaposlenih u IT firmi. U okviru informacionog sistema treba da postoje servisi za rad sa zaposlenima, servis za nadgledanje događaja u sistemu kao i PKI servis za upravljanje sertifikatima. Pristup sistemu imaju zaposleni inženjeri, menadžeri za ljudske resurse, menadžeri projekata i administratori sistema. Osnovna namena aplikacije je vođenje evidencije o zaposlenima, trenutno aktivnim i prethodnim projektima kao i svim događajima od bezbednosnog značaja u okviru sistema.

2. Tipovi korisnika

Sistem razlikuje sledeće vrste korisnika:

- **Inženjer softvera:** može da ažurira lične podatke, radno iskustvo i iskustvo na projektima na kojima je radio u okviru firme. Ne može da kreira nove projekte niti da menja podatke o postojećim projektima. Može da vidi svoj senioritet na profilu, ali nema prava da ga menja.
- **Menadžer projekta:** može da dodaje i ažurira zaposlene inženjere na projektima, da menja podatke o projektima na kojima radi i da menja svoje lične podatke.
- **Menadžer ljudskih resursa:** može da pregleda podatke o zaposlenima, njihova iskustva i projekte, ima pristup svom profilu i može da menja lične podatke.
- **Administrator:** ima prikaz svih zaposlenih u sistemu, može da dodaje nove zaposlene, može da kreira i upravlja projektima, nadgleda događaje u celokupnom sistemu i upravlja korisničkim permisijama.
- **Neautentifikovani korisnici:** imaju mogućnost da šalju zahtev za registraciju i, ako su već registrovani, da vrše prijavu na sistem.

3. Infrastruktura javnih ključeva

Bitan čvor za bezbednost ovog sistema predstavlja podsistem za infrastrukturu javnih ključeva (u daljem tekstu PKI). Uz pomoć ovog podsistema, administrator (u daljem tekstu admin) može da poveća bezbednost. Pored admin-a, PKI mogu da koriste intermediary i end entiteti, koji imaju prava da pregledaju svoje sertifikate i da ih preuzmu. Ovaj podsistem je potrebno razviti nezavisno od

ostatka sistema. Definisane uloge u PKI sistemu su nezavisne od prethnodno pomenutih uloga u tački 2.

Admin može centralizovano da izdaje sertifikate za digitalne entitete u svom sistemu. Adminu treba omogućiti da izda bilo koji sertifikat u lancu sertifikata, što podrazumeva izdavanje samopotpisanih sertifikata, intermediate sertifikata (CA) i end-entity sertifikata. Pitanje za razmatranje : da li se svi sertifikati čuvaju u istom KeyStore fajlu? Da li treba čuvati informacije o tome kom tipu entiteta se sertifikat izdaje (servisu, podsistemu, korisniku)? Neophodno je uzeti u obzir da može postojati **proizvoljno mnogo** nivoa intermediary sertifikata. Pored admina, svaki CA (vlasnik intermediate sertifikata) može da izdaje nove intermediate ili end-entity sertifikate. Obratiti pažnju koje sertifikate CA može da ponudi za potpisivanje novih sertifikata.

Potrebno je omogućiti šablon za sertifikate koji prati X.509 standard i omogućava korisniku brže kreiranje zahteva za izdavanje sertifikata. Šablonom se definišu ekstenzije koje će ući u sertifikat, a pre svega namena sertifikata. Prilikom provere validnosti sertifikata i izdavanja novih sertifikata, potrebno je proveriti da li se sertifikat koristi u skladu sa odabranim ekstenzijama. Admin treba da ima uvid u sertifikate koji postoje na sistemu. Adminu treba što više olakšati popunjavanje svih podataka koji su potrebni za sertifikat.

PKI treba da uzme u obzir validnost sertifikata u kontekstu izbora izdavaoca. Kada izdajem sertifikat koji nije samopotpisan, koje sertifikate mogu da ponudim kao opciju za njegovo potpisivanje? Kada je sertifikat validan? Da li je validnost sertifikata određena samo datumom njegovog isteka?

Admin ima mogućnost da povuče sertifikat. PKI treba da pruži servis za proveru da li je sertifikat povučen. Koju tehniku za proveru povučenosti sertifikata treba koristiti (CRL ili OCSP)? Šta se desi sa sertifikatima koje je intermediary sertifikat potpisao pošto je on povučen? Obratite pažnju na vreme trajanja sertifikata (root CA, subordinate/intermediate CA, end user).

4. Funkcionalni zahtevi

4.1. Registracija korisnika

Ukoliko korisnik još uvek nije registrovan na sistem, a želi da koristi aplikaciju, mora prvo da se registruje na odgovarajućoj stranici. Registracija obuhvata unos email adrese, lozinke, imena, prezimena, adrese prebivališta, grada, države, broja telefona i zvanje. Lozinka se unosi u dva polja da bi se otežalo pravljenje grešaka prilikom odabira nove lozinke. Obratiti pažnju na minimalnu dužinu lozinke kao i vrste karaktera koje lozinka mora da sadrži. Prilikom skladištenja lozinki potrebno je primeniti *salted password hashing* mehanizam. Nakon popunjavanja forme za registraciju, zahtev se šalje administratoru sistema na reviziju. Prilikom registracije, potrebno je odabrati i poziciju koju zaposleni ima u firmi (menadžer ljudskih resursa, inženjer ili menadžer projekta). Administratori sistema nemaju pravo da se registruju preko ove forme za registraciju.

4.2. Potvrda registracije korisnika

Zahtev za registracijom administrator može da potvrdi ili odbije. Nakon odobravanja zahteva za registracijom, na datu email adresu se šalje link za aktivaciju korisnika. Korisnik ne može da se prijavi na aplikaciju dok se njegov nalog ne aktivira posećivanjem linka koji je dobio u emailu. Ukoliko je zahtev odbijen, korisniku se na email adresu šalje poruka da je zahtev odbijen uz kratku poruku gde administrator navodi razlog odbijanja zahteva. Ukoliko je zahtev za registraciju odbijen, potrebno je osmisliti mehanizam sprečavanja ponovne registracije u određenom vremenskom periodu (na primer na osnovu email-a ili IP adrese). Ukoliko je zahtev prihvaćen a registrovao se inženjer, od datuma potvrde registracije se računa datum zaposlenja inženjera (biće potrebno prilikom provere senioriteta).

Link za aktivaciju koji se dobija na email je zaštićen. Njegovo trajanje je vremenski ograničeno datumom i vremenom trajanja, može da se upotrebi samo jednom, a integritet podataka koji su poslati na link je zaštićen HMAC algoritmom. Pogledati tačku o *passwordless* prijavi na sistem, i uočiti kako bi se na sličan način mogao štititi i ovaj link.

4.3. Prijava na sistem uz pomoć lozinke

Svi korisnici sistema imaju mogućnost prijave pomoću email adrese i lozinke. Ukoliko je korisnik uspešno ulogovan, potrebno je izgenerisati access token i refresh token koji će se poslati na klijentski deo aplikacije. Access token treba da ima datum do kada važi (pogledati tačku za osvežavanje tokena). Dobijeni refresh token i access token treba skladištiti na klijentskom delu, dok access token treba slati kroz zaglavlje prilikom narednih zahteva tog ulogovanog korisnika.

4.4. Prijava na sistem bez upotrebe lozinke

Korisnik može da odabere opciju da se prijavi na sistem samo uz pomoć email adrese (tzv. *passwordless login*). Nakon unosa email adrese, šalje se zahtev pri čemu je na serverskoj strani potrebno generisati jednokratni token sa periodom važenja od maksimalno 10 minuta. Taj token se kao deo “magičnog linka” šalje korisniku na njegovu email adresu. Korisnik ima 10 minuta da otvori email i poseti link. Klikom na link, na serveru se proverava ispravnost tokena. Ukoliko je token ispravan, server će za autentifikaciju korisnika izgenerisati novi par refresh i access tokena. Potom, server će preusmeriti korisnika na klijentsku aplikaciju (front-end), i pri tom će kroz zaglavlje (header) proslediti klijentskom delu apliacije. Voditi računa o tome da se jednom generisani link ne može posetiti više puta.

4.5. Prikaz informacija neautentifikovanim korisnicima

Korisnici koji nisu autentifikovani nemaju prava pristupa ni jednoj stranici, osim stranici za registraciju i prijavu na sistem. Takođe nemaju prava pristupa nikakvim podacima sistema. Potrebno je obezbediti zaštitu pristupa za svaki ulaz u sistem (engl. *endpoint*) i na klijentskoj i na serverskoj strani aplikacije.

4.6. Osvežavanje tokena

Access token ima period važenja od 15 minuta. Ukoliko je access token istekao, a ispravno je generisan i potpisan, korisnik može da pošalje novi zahtev za osvežavanje access tokena, pri čemu će se proveriti identitet tog korisnika na osnovu refresh tokena. Ukoliko u sistemu postoji takav korisnik i on nije blokiran, potrebno je izgenerisati novi access token, koji će se poslati kao odgovor na klijentski deo aplikacije (front-end). Novi izgenerisani token treba da zameni stari u zaglavlju budućih HTTP zahteva sa klijentske strane. Access token može da se osvežava do datuma važenja refresh tokena.

4.7. Profil inženjera

Registrovani korisnik u mogućnosti je da ažurira svoje lične podatke na stranici za prikaz svog profila. Zaposleni ne sme da menja svoju email adresu. Pored osnovnih podataka, korisnik ima mogućnost da ažurira svoje veštine i postavi svoj CV dokument (za veštinu se definiše naziv i brojčana procena u nekom opsegu, npr. Java 5, Python 4).

Pored toga, zaposlenom treba omogućiti prikaz projekata na kojima je radio u okviru IT kompanije. Za svaki projekat se evidentira naziv, trajanje i opis šta je konkretan inženjer radio na projektu. Inženjer ima pravo da pregleda projekte i menja opis sopstvenih zaduženja, ali nema pravo da menja naziv i trajanje projekta. Takođe, inženjer može da vidi samo opis svog posla na projektu, ne i opise drugih inženjera na istom projektu.

4.8. Profil administratora sistema

Administrator može da pregleda sve zaposlene i sve projekte u okviru kompanije. Takođe, može da kreira nove projekte i dodaje zaposlene za projekte. Administrator ima pregled svih inženjera na određenom projektu. Administrator može da ažurira svoje lične podatke i može da registruje druge administratore. Inicijalno postoji jedan predefinisani administrator koji mora da promeni lozinku prilikom prve prijave na sistem.

4.9. Profil menadžera projekta

Menadžer projekta može da ažurira lične podatke. Pored toga, menadžeru projekta treba omogućiti prikaz svih projekata na kojima trenutno radi ili na kojima je radio, kao i prikaz zaposlenih inženjera koji su radili na tim projektima. Menadžer projekta ima mogućnost ažuriranja zaposlenih na projektima. Za svakog zaposlenog potrebno je evidentirati datum početka i završetka rada na projektu.

4.10. Pretraga korisnika

Administrator može da pregleda i pretražuje inženjere. Pretraga treba da bude kombinovana i da obuhvata email adresu, ime, prezime i period zaposlenja inženjera.

4.11. HTTPS

Potrebno je obezbediti komunikaciju klijentskog i serverskog dela aplikacije putem HTTPS protokola. To podrazumeva da izgenerišete nov sertifikat, i iskonfigurišete aplikaciju tako da iskoristi taj sertifikat za HTTPS komunikaciju između svih servisa aplikacije.

4.12. Kontrola pristupa pomoću RBAC modela

Potrebno je implementirati model kontrole pristupa svakom delu sistema uz pomoć uloga i permisija. Jedan korisnik može da ima više uloga, a jednoj ulozi može biti dodeljeno više permisija. Potrebno je na nivou kompletnog sistema (za svaku metodu kontrolera) definisati prava pristupa. Takođe, potrebno je postaviti permisije za sve CRUD operacije koje postoje u sistemu. Administrator sistema ima mogućnost upravljanja permisijama za svaku od uloga sistema. Administrator može da menja ili uklanja permisije, kao i da dinamički određuje koja uloga će imati koju permisiju.

4.13. Kontrola pristupa klijentskom delu aplikacije

Potrebno je obezbediti autorizovan pristup podacima na HTML stranicama klijentskog dela aplikacije. Ukoliko neautorizovan korisnik pokuša da pristupi stranici za koju nema prava, potrebno ga je preusmeriti na početnu stranicu ili stranicu za prijavu na sistem.

4.14. Šifrovanje osetljivih podataka

Osetljive podatke je potrebno šifrovati pre skladištenja u bazi, u skladu sa GDPR smernicama. Za šifrovanje podataka možete koristiti simetrični ili asimetrični algoritam. Obratiti pažnju na generisanje i dužinu ključeva, kao i režim za šifrovanje. Takođe, voditi računa o formatu i načinu skladištenja ključeva za enkripciju. Prilikom učitavanja podataka iz baze, šifrovane podatke je potrebno dešifrovati uz pomoć odgovarajućeg ključa.

4.15. Rukovanje korisnicima

Administrator može da rukuje korisnicima. Može da blokira korisnike tako da ne mogu više da se prijave na sistem, i da više ne mogu da koriste refresh tokene. Takođe, trebalo bi omogućiti svakom korisniku da promeni lozinku i da oporavi nalog ukoliko zaboravi lozinku.

4.16. Šifrovanje i dešifrovanje CV dokumenta

Potrebno je omogućiti šifrovanje CV dokumenta. Prilikom skladištenja dokumenta na nivou operativnog sistema dokument se šifruje koristeći kombinaciju AES i RSA algoritama (koriste se sertifikati). Prilikom zahteva za pregled ili izmenu dokumenta, dokument se dešifruje. Dokument može da bude u xml formatu.

4.17. Postupak pristupa CV dokumentu zaposlenih

CV dokumentu zaposlenih inženjera mogu pristupiti menadžeri ljudskih resursa ili menadžeri projekata na kojima je taj zaposleni radio u okviru firme. Menadžeri ljudskih resursa mogu da vide podatke koji se nalaze u CV dokumentu ali podrazumevano je da nemaju prava da ih menjaju.

4.18. *Logging* mehanizam

Potrebno je implementirati *logging* mehanizam koji ispunjava kompletnost, pouzdanost, upotrebljivost i konciznost (detaljno će svaki od ovih zahteva biti objašnjen na vežbama). Log zapis treba da sadrži dovoljno informacija da dokaže neporecivost. Svaki događaj od bezbednosnog značaja za sistem treba da bude zabeležen. Format loga treba da prati standard i da bude u skladu sa najboljom praksom. Takođe, treba voditi računa o memorijskom zauzeću logova i napraviti mehanizam za rotaciju logova.

4.19. Nadgledanje događaja i upozorenja

Potrebno je omogućiti nadgledanje log zapisa i mehanizam upozorenja na kritične događaje u sistemu u realnom vremenu. Administrator bi trebalo da dobija upozorenja kako bi se adekvatno odgovorilo na pretnje po sistem. Format upozorenja je proizvoljan. Upozorenja je potrebno prikazati i u okviru aplikacije (poput *push* notifikacije) i preko email/SMS servisa.

4.20. ACL

Potrebno je obezbediti kontrolu pristupa datotekama aplikacije na nivou operativnog sistema (*Access Control List*). Razmisliti koje datoteke koje aplikacija koristi su od značaja za kontrolisan pristup.

5. Zadatak za višu ocenu (10 bodova)

Potrebno je implementirati jednu od navedenih stavki po članu tima (dakle svaki student iz tima bira i implementira jednu od ponuđenih stavki).

5.1. Single sign-on

Potrebno je omogućiti single sign-on (u daljem tekstu SSO) prijavu na kompletan sistem. Mehanizam za SSO se mora implementirati konfigurisanjem gotovih rešenja, poput Active Directory ili Keycloak i njihovom integracijom sa ostatkom sistema.

5.2. Penetration testing

Sprovesti penetraciono testiranje modula sistema upotrebom bar dva alata iz grupe: Nmap, Nikto, dirbuster, sqlmap, OWASP ZAP, Burp Suite. Kao rezultat penetracionog testiranja, alati nude generisan izveštaj. Potrebno je priložiti izveštaj pentesting alata i regulisati ranjivosti.

5.3. Two-factor authentication

Potrebno je mogućiti dvofaktorsku prijavu na sistem, gde bi se od korisnika pored lozinke zahtevalo još nešto što “korisnik zna ili poseduje”. Mehanizam se može implementirati pomoću TOTP (Time-based One Time Password) koji bi generisao Google Authenticator ili Microsoft Authenticator.

5.4. Bezbednosna analiza eksternih komponenti

Neophodno je izvršiti bezbednosnu analizu svih third-party komponenti na koje se vaše rešenje oslanja (od operativnog sistema do front-end biblioteka i sve između). Potrebno je sakupiti listu ranjivosti, analizirati ih i izvršiti strategiju za razrešenje mogućih rizika. Za bezbednosnu analizu je moguće koristiti alate poput *OWASP dependency checker-a*. Kao rezultat rada, potrebno je priložiti izveštaj koji je generisan od strane alata.

6. Opšti zahtevi

Potrebno je na nivou celog sistema sprečiti relevantne Injection i XSS napade i izvršiti validaciju podataka koristeći kriterijume validacije definisane po najboljim praksama u zavisnosti od formata i dozvoljenih vrednosti podatka koji se validira.

7. Raspodela funkcionalnosti

Jednočlani timovi rade sledeće funkcionalnosti:

- PKI (tačka 3) - izdavanje sertifikata svih nivoa, prikaz sertifikata, preuzimanje sertifikata i provera validnosti sertifikata
- Funkcionalnosti 4.1, 4.3, 4.7, 4.11, 4.12 i 4.18

Dvočlani timovi rade sledeće funkcionalnosti:

- PKI (tačka 3) - izdavanje sertifikata svih nivoa, prikaz sertifikata, preuzimanje sertifikata, provera validnosti sertifikata, povlačenje bilo kog sertifikata u lancu (rekurzivno povlačenje ostalih sertifikata u lancu), provera povučenosti sertifikata
- Funkcionalnosti 4.1, 4.2, 4.3, 4.6, 4.7, 4.8, 4.11, 4.12, 4.13, 4.14 i 4.18

Tročlani i četvoročlani timovi rade sve tačke specifikacije. Ova raspodela se odnosi i na stare studente.