Projektni zadatak iz predmeta

Bezbednost u sistemima elektronskog poslovanja

Računarstvo i automatika - generacija 2023/2024.

1. Namena sistema

U okviru projektnog zadatka potrebno je implementirati informacioni sistem koji vodi evidenciju klijenata i zaposlenih u marketinškoj agenciji. U okviru informacionog sistema treba da postoje servisi za rad sa korisnicima (zaposlenima i klijentima), servis za nadgledanje događaja u sistemu kao i PKI servis za upravljanje sertifikatima. Pristup sistemu imaju zaposleni, klijenti i administratori sistema. Osnovna namena aplikacije je vođenje evidencije o zaposlenima, trenutno aktivnim i prethodnim klijentima kao i svim događajima od bezbednosnog značaja u okviru sistema.

2. Tipovi korisnika

Sistem razlikuje sledeće vrste korisnika:

- **Klijent:** može da ažurira lične podatke, zatraži reklamu i promeni paket usluga. Ne može da dodaje nove pakete usluga niti da menja sadržaj usluga obuhvaćenih paketom. Nema uvid u reklame drugih klijenata.
- **Zaposleni:** može da kreira reklame na zahtev klijenata. Može da ažurira lične podatke. Ima uvid u reklame koje su kreirali drugi zaposleni, ali nema prava da ih menja ili uklanja.
- **Administrator:** ima prikaz svih korisnika u sistemu (zaposlenih i klijenata), može da dodaje nove zaposlene, nadgleda događaje u celokupnom sistemu i upravlja korisničkim permisijama.
- **Neautentifikovani korisnici:** imaju mogućnost da šalju zahtev za registraciju ili, ako su već registrovani, da vrše prijavu na sistem.

3. Funkcionalni zahtevi

3.1. Registracija korisnika (klijenta)

Ukoliko korisnik još uvek nije registrovan na sistem, a želi da koristi usluge marketinške agencije, mora prvo da se registruje na odgovarajućoj stranici. Registracija obuhvata unos email adrese, lozinke, imena, prezimena, adrese prebivališta, grada, države, broja telefona i tipa (fizičko ili pravno lice). Ukoliko se klijent registruje kao pravno lice, onda se umesto imena i prezimena unosi naziv i PIB firme, a adresa prebivališta predstavlja sedište firme. 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 paket usluga koji će dalje definisati povlastice koje klijent ima (osnovni, standardni ili zlatni). Administratori sistema nemaju pravo da se registruju preko ove forme za registraciju.

Napomena: U realnom sistemu, prilikom odobravanja naloga klijent bi izvršio plaćanje odabranog paketa usluga. U ovom sistemu možete smatrati da su usluge fiktivno plaćene u onom trenutku kada administrator odobri zahtev za registraciju.

3.2. Potvrda registracije klijenta

Zahtev za registraciju administrator može da potvrdi ili odbije. Nakon odobravanja zahteva za registraciju, na datu email adresu se šalje link za aktivaciju klijenta. Klijent ne može da se prijavi na aplikaciju dok se njegov nalog ne aktivira posećivanjem linka koji je dobio u *emailu*. Ukoliko je zahtev odbijen, klijentu se na *email* adresu šalje poruka da je zahtev odbijen uz 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).

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.

3.3. Prijava na sistem uz pomoć lozinke

Svi korisnici sistema imaju mogućnost prijave pomoću email adrese i lozinke. Ukoliko je korisnik uspešno prijavljen, 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 klijenta.

3.4. Prijava na sistem bez upotrebe lozinke

Klijent može da odabere opciju da se prijavi na sistem samo uz pomoć email adrese (tzv. *passwordless login*) ako ima standardni ili zlatni paket usluga. 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 klijentu 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 klijenta izgenerisati novi par refresh i access tokena. Potom, server će preusmeriti klijenta na klijentsku aplikaciju (front-end), i pri tom će kroz zaglavlje (header) proslediti tokene klijentskom delu apliacije. Voditi računa o tome da se jednom generisani link ne može posetiti više puta.

3.5. Dvofaktorska autentifikacija

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

3.6. CAPTCHA

Prilikom svake prijave na sistem, zaposleni mora da reši CAPTCHA test. CAPTCHA podrazumeva rešavanje prostih aritmetičkih operacija ili prepoznavanje oblika koje čoveku oduzimaju malo vremena a mašina trenutno ne ume dovoljno brzo da ih reši. Možete se osloniti na postojeća CAPTCHA rešenja poput Google reCAPTCHA ili Cloudflare.

3.7. 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.

3.8. 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 sve dok ne istekne refresh token.

3.9. Profil zaposlenog

Zaposleni u agenciji u mogućnosti je da ažurira svoje lične podatke na stranici za prikaz svog profila. Zaposleni ne sme da menja svoju email adresu. Pored toga, zaposlenom treba omogućiti prikaz svih reklama kreiranih za klijente. Za svaku reklamu se evidentira klijent, slogan, trajanje i opis. Zaposleni ima uvid u sve zahteve za reklamama poslate od strane svih klijenata i može da kreira novu reklamu samo ako je ona vezana za prethodno poslati zahtev.

3.10. Profil administratora sistema

Administrator može da pregleda sve zaposlene i sve klijente u okviru agencije. Administrator može da ažurira svoje lične podatke i može da registruje druge administratore i zaposlene. Administrator ne sme da menja svoju email adresu. Inicijalno postoji jedan predefinisani administrator koji mora da promeni lozinku prilikom prve prijave na sistem. Svaki zaposleni mora da promeni lozinku prilikom prve prijave.

3.11. Profil klijenta

Klijent može da ažurira lične podatke uključujući i svoju email adresu. Pored toga, klijentu treba omogućiti prikaz svih reklama koje su za njega napisane. Klijent u okviru svog profila ima mogućnost kreiranja zahteva za reklamu, pri čemu se evidentira: krajnji rok za kreiranje reklame, period u kom će reklama biti aktivna (od-do) i opis u slobodnoj formi. Klijent nema uvid u zahteve ili reklame drugih klijenata.

3.12. 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. Ukoliko tim izgeneriše novi sertifikat pomoću svog PKI sistema, dobiće dodatne bodove za ovu funkcionalnost.

3.13. 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. 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.

3.14. Kontrola pristupa klijentskom delu aplikacije

Potrebno je obezbediti autorizovan pristup podacima na klijentskom delu 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.

Napomena: Nije dovoljno korisniku aplikacije ipak prikazati stranicu kojoj želi neautorizovano da pristupi, bez mogućnosti izvršavanja funkcionalnosti. Primer: klijent ne sme da pristupi stranici za kontrolu permisija koju vidi administrator, čak i ako klik na dugme za izmenu permisija ne radi ništa.

3.15. 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.

3.16. 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. Blokiranje korisnika se odnosi i na klijente i na zaposlene. Takođe, trebalo bi omogućiti svakom korisniku da promeni lozinku i da oporavi nalog u slučaju da je lozinka zaboravljena.

3.17. *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.

3.18. 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.

3.19. Ograničavanje broja poseta reklamama

Posećivanje reklame je potrebno simulirati pozivom ka neautentifikovanim *endpointu*. Pošto broj klikova po reklami treba biti visok za kratak period, preporuka je napisati skriptu koja simulira posete korisnika. Svaki klijent ima paket koji dozvoljava ograničen broj poseta po reklami. Potrebno je obezbediti ova ograničenja upotrebom ratelimittera. Ograničenja po paketima su:

- Osnovni: do 10 klikova po reklamu po minuti
- Standardni: do 100 klikova po reklamu po minuti
- Zlatni: do 10 000 klikova po reklamu po minuti

3.20. Fizičko brisanje podataka gold klijenata

Korisnici zlatnog paketa imaju pravo na fizičko brisanje podataka (pravo na zaborav). Ovo znači da na njihov zahtev, potrebno je ukloniti sve informacije asocirane sa njima sa platforme, u potpunosti (bez soft delete-a).

4. 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).

4.1. 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.

4.2. 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.

4.3. 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. Nakon generisanja izveštaja, potrebno je prevazići ranjivosti na osnovu smernica iz izveštaja.

4.4. Pristup VPN-u

Potrebno je pristupiti VPN mreži (parametri za pristup će biti podeljeni posle KT2) formiranoj pomoću Wireguard alata i kontaktirati komponentu koja se nalazi u toj mreži putem HTTP GET zahteva. Dobijenu poruku prikazati korisniku na UI.

5. 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.

6. Raspodela funkcionalnosti

Jednočlani timovi rade sledeće funkcionalnosti:

- Funkcionalnosti 3.1, 3.3, 3.6, 3.8, 3.12, 3.13 i 3.17

Dvočlani, tročlani i četvoročlani timovi rade sve tačke specifikacije. Ova raspodela se odnosi i na stare studente.