NIŠTAGRAM

XWS PROJEKAT

Razviti platformu (društvenu mrežu) za deljenje slika i video materijala širom Interneta.

Učesnici/Korisnici sistema

- Neregistrovani korisnik - pretražuje i razgleda dostupne slike i video materijale na javnim profilima.
- Registrovani korisnik - pored pretrage i pregleda, ima mogućnost kačenja sopstvenih slika i video materijala, kao i dopisivanje sa svojim pratiocima.
- Administrator - upravlja i održava kompletan sistem, ima kompletan pristup sistemu. Upravlja poslovnim korisnicima, slikama, video materijalima (u slučaju nepropisnog sadžaja), kao i ostalim entitetima. Može da registruje nove agente za reklame (*ad provider*-e), odobrava već podnete zahteve za registraciju, ažurira permisije i role postojećim korisnicima.
- Agent - kreira zahteve za plasiranje reklama svojih proizvoda, odnosno kreira marketinške kampanje. Takođe ima pristup različitim analizama i izveštajima koji se odnose na reklame.

Moduli sistema

- **Front-End Ništagrama** - Obezbeđuje interfejs i funcionalnosti neophodne korisnicima, agentima i administratorima.
- **Back-End Ništagrama** - Sadži kompletnu poslovnu logiku aplikacije koja se zasniva na mikroservisnoj arhitekturi.
- **Agensta aplikacija** (Front-End i Back-End) - predstavlja web prodavnicu (monolitna apliklacija). Koristi API za reklame koji nudi Back-End Ništagrama kako bi promovisala svoje proizvode.

Funkcionalnosti

Ništagram

1. Obezbediti sledeće funkcionalnosti **neregistrovanim korisnicima**:
    1. Pregled slika i video materijala na javnim profilima.
    2. Pretragu javnih profila, pretragu tagova i lokacija. Pretraga treba da prikaže samo javno dostupne slike i video materijale.
    3. Registracija na sistem (obavezan jedinstven *username*).

2. Obezbediti sledeće funkcionalnosti **registrovanim korisnicima**:
    1. Sve funkcionalnosti kojima raspolaže neregistrovani korisnik.
    2. Logovanje na sistem.
    3. Preporučivanje drugih profila kao potencijalne pratioce. **Za implementaciju ove funkcionalnosti neophodno je koristiti graf bazu**.
    4. Slanje zahteva za verifikaciju profila. U zahtevu mora da stoji pravo ime i prezime, kategorija (influencer, sports, new/media, business, brand, organization itd.) i sliku oficijalnog dokumenta (lična karta, vozačka dozvola, pasoš).
    5. Zapraćivanje drugih profila:
        a. Zapraćivanje treba da omogući prikaz slika i video materijala prilikom njihovog kreirana od strane zaprećenog profila.
        b. Zapraćivanje javnog profila je uvek omogućeno.
        c. Zapraćivanje privanog profila mora da se odobri od strane privatnog profila. Odobreni zahtev omogućava pristup sadržaju koji se nalazi na profilu. Zparaćivanje između dva privatna profila mora da bude bidirekciono.
    6. Objavljivanje sopstvenih slika i video materijala. Prilikom objavljivanja moguće je dodati tagove, lokacije i opis. Objavljivanje sadžaja je moguće u sledećim oblicima:
        a. **Post** koji se trajno nalazi na korisnikovom profilu. Prilikom kreiranja *post*-a, neophodno je podeliti ga sa ostalim pratiocima. *Post* omogućava sledeće opcije: like, **dislike**, komentare, čuvanje postova (*favorites*). Sačuvani post-ovi mogu se grupisati u kolekcije.
        b. **Story** koji je vidljiv pratiocima 24 sata, dok vlasnik ima trajni pristup svim *story*-jima. Omogućiti definisanje bliskih prijatelja i objavljivanje *story*-ja samo bliskim prijateljima. *Story*-je je moguće istaći na profil kao **story highlights**.
        c. **Album** koji predstavlja skup više slika i video materijala koji se deli istovremeno kao *post* ili *story*.

7. Razmenjivanje poruka sa drugim profilima:
    a. Slanje tekstualnih poruka.
    b. Slanje post-ova, story-ja i albuma. Ukoliko se šalje link ka sadžaju nekog privatnog profila koji nije zapraćen od strane primaoca, ispisuje se poruka da je sadržaj nedostupan.
    c. Slanje jednokratih slika i video materijala koje je moguće samo jednom pogledati, nakon čega im se više ne može pristupiti.
    d. Privatni profil može da primi poruku od nezapraćenog profila ali mu se nudi opcija da taj profil prihvati, odbije ili obriše poruku.
8. Ažuriranje i podešavanje profila:
    a. Dodavanje i izmena ličnih podataka: ime, email, broj telefona, pol, datum rođenja, *username*, web sajt i biografija.
    b. Podešavanje privatnosti profila:
        i. Da li je profil javan ili privatan.
        ii. Da li korisnik želi da prima poruke od profila koje nije zapratio.
        iii. Da li drugi profili mogu da taguju profil na svojim *post*-ovima, *story*-jima i komentarima.
        iv. *Mute*-ovanje drugih profila (profilu se više ne prikazuje sadžaj od *mute*-ovanih profila prilikom njihovih objavljivanja, ali im i dalje može pristupiti) .
        v. Blokiranje drugih profila, nakon čega sa istima nije moguće vršiti bilo kakav vid interakcije.
    c. Podešavanje notifikacija za zapraćene profile, poruke, *post*-ove, *story*-je i komentare.
9. Prijavljivanje neprikladnog sadržaja.
10. Pregled sadržaja koji je *like*-ovan i *dislike*-ovan od strane profila.

3. Obezbediti sledeće funkcionalnosti **agentima**:
    1. Slanje zahteva za registraciju. Pored osnovnih informacija o agentu, u zahtevu moraju da se nalaze validan email, kao i link do web sajta agenta.
    2. Agent poseduje sve funkcionalnosti kao i registrovani korisnik. Takođe, poseduje funkcionalnosti koje se odnose na reklame:
        a. Kreiranje,izmena i brisanje kampanje. Kampanja predstavlja zahtev za plasiranje jedne ili više reklama. Reklama može biti slika ili video materijal koja može u sebi da sadži link ka sajtu agentove web prodavnice ili nekog konkretnog agentovog proizvoda. Kampanje mogu biti tipa *post* ili *story*. Kampanja može biti jednokratna i višekratna. Jednokratna kampanja se ciljnoj grupi prikazuje samo jednom u definisano vreme. Višekratna kampanja ima datum početka i kraja, kao i informaciju o tome koliko puta ju je neophodno plasirati ciljnoj grupi u toku dana. Višekratne kampanje je moguće menjati ali se izmene uvažavaju tek nakon 24 sata (ovo ograničenje može biti i veće, poput nekoliko dana, ali bitno je obezbediti da se kampanje ne mogu menjati

u svakom trenutku). Sadžaj kampanje tj. slike i video materijali se ne mogu menjati. **Svi *edge case*-ovi rukovanja kampanjama se ostavljaju studentu da ih reši onako kako mu najviše ima smisla**.

b. Kamapnja se realizuje tako što se njen sadžaj dodaje na profil agenta i deli **odredjenoj ciljnoj grupi profila** i svim pratiocima agentovog profila. Neophodno je osmisliti adekvatan način za određivanje ciljne grupe. Kod višekratnih kampanja neophodno je samo jednom okačiti slike i video materijale na profil agenta. **Plasiranje kampanja treba da se radi automatski u vreme definisano u samoj kampanji (exposure date/s)**.

c. Agenti mogu angažovati druge profile (*influencer*-e) za plasiranje svojih kampanja. U slučaju da je *influencer* privatan profil mora da odobri zahtev za praćenje poslat od strane agenta. Svaku kampanju *influencer* mora da odobri da bi se stekao preduslov za njeno plasiranje. Plasiranje kampanje se radi tako što se sadžaj kampanje kači na profil *influencer*-a.

d. Monitoring plasiranih kampanja. Svakoj kampanji neophodno je voditi evidenciju koliko ima komentara, *like*-ova i *dislike*-ova kada je u pitanju *post*. Takođe, neophodno je voditi evideniju o tome koliko puta je kampanja bila plasirana ciljnoj gupi, kao i koliko su puta korisnici zaista kliknuli na link koji se nalazi u slici ili video materijalu. Link koji se nalazi u slici ili video materijalu mora da sadži informaciju o tome od kog *post*-a ili *story*-ja je potekao (ovo je naročitno bitno za *influencer*-e kako bi se imao uvid koji *influencer*-i su najuticajniji).

3. Upravjanje API tokenima koji omogućavaju pristup funkcionalnostima koje se odnose na reklame. **Token ne sme da autorizuje pristup ostalim funkcionalnostima**.

4. Obezbediti sledeće funkcionalnosti **administratorima**:
   1. Pregled i obradu zahteza za verifikaciju profila.
   2. Pregled prijavljenih zahteva za neprikladan sadžaj. Admin može da ukloni neprikladan sadžaj sa određenog profila, kao i da ugasi ceo profil.
   3. Registrovanje novih i odobravanje postojećih zahteva za agente.

Agentska apllikacija

5. Obezbediti sledeće funkcionalnosti u **agentskoj aplikaciji**:
    1. Registracija korisnika.
    2. Pregled, kreiranje, izmena, brisanje proizvoda. Proizvod treba da sadži barem sliku, cenu i raspoloživo stanje.
    3. Kupovinu proizvoda pauzećem (plaćanje se vrši prilikom isporuke robe, nije potrebno implementirati sistem za plaćanje).
    4. Rad sa kampanjama koje koriste API Ništagrama namenjen za reklame.
    5. Kreiranje izveštaja koji koristi API Ništagrama namenjen za monitoring kampanja. Izveštaji treba da daju informacije koje kampanje su bile najuspešnije i dovele do povećanja prihoda agentu i vredi ih plasirati u narednom periodu. Studentu se ostavlja zadatak da osmisli kako će procesirati podakte koje nudi API Ništagrama i prikazati ih u izveštaju. **Izveštaje je neophodno čuvati u *XML document base* bazi i omogućiti opciju generisanja u PDF format.**

Način realizacije projekta i ocenjivanje

Projekat se realizuje timski, pri čemu timovi broje do 4 člana. Studenti treba da:

- Razviju model podataka neophodan za realizaciju kompletnih funkcionalnosti (Analizirati koji podaci se koriste u sistemu kao i koje međuzavisnosti postoje).
- Definišu neophodne komunikacije kako bi ceo sistem funkcionisao na adekvatan način (Definisati adekvatne servisne endpointe pri čemu treba voditi računa o tome da je Ništagram neophodno razviti kao skup mikroservisa).
- Realizuju sve navedene funkcionalnosti vodeći računa o svim graničnim slučajevima, odnosno omogućiti pravilno funkcionisanje aplikacije (**za sve slučajeve koji nisu pokriveni u specifikaciji studentima se daje mogućnost da ih reše na način koji je njima najprikladniji**).

Za ocenu 6 neophodno je implmentirati:

- Sve funkcionalnosti neregistrovanog korisnika: 1.1, 1.2, 1.3 i funkcionalnosti 2.1, 2.5 i 2.6, 2.8.a.
- Svi servisi moraju da se izvršavju u kontejnerima i definisati *docker compose* za njihovo pokretanje.

Za ocenu 7 neophodno je implementirati:

- Sve stavke navedene za ocenu 6.
- Funkcionalnosti: 2.4, 2.8, 2.9, 2.10, 4.1.

Za ocenu 8 neophodno je implementirati:

- Sve stavke naveden za ocenu 7.
- Funkcionalnosti: 3.1, 4.3, 4.2, 3.2.a, 3.2.b, 3.2.c, 3.3, 5.1, 5.2, 5.3, 5.4.
- Primeniti SAGA obrazac za sihronizaciju podataka između mikroservisa.

Za ocenu 9 neophodno je implementirati:

- Sve stavke navedene za ocenu 8.
- Funkcionalnosti: 2.7, 3.2.d, 5.5.

Za ocenu 10 neophodno je implementirati sledeće:

- Sve stavke navedene za ocenu 9.
- Funcionalnosti: 2.3
- *Monitoring* i *tracking* Ništagram mikroservisne aplikacije pomoću *Prometheus*, *Grafana* i *Jaeger* alata.

Bezbednost u sistemima elektronskog poslovanja

Ništagram rešenje je neophodno obezbediti integracijom bezbednosnih kontrola u njegove module, kao i uvođenjem bezbednosnih alata koji su opisani u ovom poglavlju.

PKI

Implementirati alat za podršku infrastrukture javnih ključeva. Specifikacija projektnog zadatka je definisana kroz skup funkcionalnih i nefunkcionalnih zahteva za rad sa sertifikatima i ključevima. Potrebno je dizajnirati i implementirati PKI vođeni ovim zahtevima.

Bezbednost modula

Potrebno je obezbediti čitav Ništagram sistem. Svaku bezbednosnu kontrolu treba integrisati prateći best practice konfiguraciju i šablone bezbednog dizajna (višeslojna odbrana, najmanja privilegija, jednostavan dizajn, itd.).

Zaštita podataka

Osetljivi podaci sa kojim aplikacija radi treba da budu obezbeđeni u skladištu, u transportu i tokom upotrebe. Identifikovati osetljive podatke, definisati i implementirati prikladne bezbednosne kontrole. Podaci čije skladištenje se ne može izbeći treba da budu šifrovani ili heširani ukoliko je to prikladno. Poruke u internoj komunikacije treba da imaju očuvanu poverljivost, integritet i neporecivost, kao i da budu zaštićene od reply napada. Komunikacija između veb-čitača i servera treba da bude zaštićena sigurnom konfiguracijom HTTPS protokola. Sertifikate generisati putem PKI alata.

Kontrolna pristupa

Korisnički interfejsi modula treba da podrži prikladne mehanizme za autentifikaciju i autorizaciju. Mehanizmi autentifikacije treba da podrže bezbednu registraciju, prijavu na sistem, odjavu, promenu lozinke i resetovanje lozinke. Autorizacija podrazumeva kontrolu pristupa po RBAC modelu.

OWASP Top 10

Kompletan sistem treba da reguliše sve rizike sa OWASP Top 10 liste, gde je neophodno sastaviti temeljan izveštaj kako su koji rizici adresirani. Objasniti koje grupe napada su relevantne, kako je sistem zaštićen od njih, ili kako bi bio zaštićen prilikom postavljanja u produkciju.

Zadatak za 9

Potrebno je da svaki student iz tima kreira model pretnji za proizvoljno odabran mikroservis. Model pretnji podrazumeva sagledavanje ranjivosti, pretnji, napada, kontrola za njihovo sprečavanje i negativnih uticaja uz arhitekturne dijagrame i dijagrame tokova podataka. Pored dijagrama, potrebno je odgovoriti na sledeća pitanja:

- Odakle napadač može da sprovede napad i pod kojim uslovima?
- Kakve napade može da sprovede i koje su posledice?
- Na koji način se napadi mogu sprečiti?

Zadatak za 10

Za najvišu ocenu je neophodno realizovati jednu od celina definisanih u ovom poglavlju.

Single sign-on

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

Penetration testing

Sprovesti penetraciono testiranje veb-aplikacija i servera 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.

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.