ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ, ΕΚΠΑ

Εφαρμογή διαδικτύου

Δουκάκης-Χιώτης Στέφανος, ΑΜ: 1115201800276

Μάλλιος Αποστόλης, ΑΜ: 1115201800103

Περιεχόμενα

Εισαγωγή

Στόχος της εργασίας είναι η ανάπτυξη επαγγελματικής εφαρμογής δικτύωσης με χρήση του framework Spring boot 2.5 για το νωτιαίο άκρο και Angular 12 για το μετωπιαίο άκρο.
Υλοποιήθηκαν «βασικές» λειτουργίες εφαρμογής κοινωνικής δικτύωσης όπως:

- Δυνατότητα ανάρτησης άρθρων με πολυμέσα, σχόλια και σημειώσεις ενδιαφέροντος σε αυτά.
- Δυνατότητα σύνδεσης χρηστών μεταξύ τους, ώστε να μπορούν να μοιράζονται άρθρα, μηνύματα, αγγελίες.
- Δυνατότητα ανάρτησης αγγελιών και αλληλεπίδρασης χρηστών με αγγελίες συνδεδεμένων χρηστών με αυτούς (φίλοι) αλλά και με αγγελίες των οποίων τα προαπαιτούμενα συνάδουν με τις δεξιότητες του χρήστη.
- Δυνατότητα επεξεργασίας προσωπικών πληροφοριών του χρήστη και επισήμανσής τους ως προσωπικές ή δημόσιες.
- Διαχωρισμός μελών βάσει ρόλων, όπως ο ρόλος του «διαχειριστή», που είναι μοναδικός στην εφαρμογή και ο ρόλος «μέλους» που έχει κάθε εγγεγραμμένος χρήστης.
- Πλήρης κρυπτογράφηση αιτημάτων HTTP που καταφθάνουν στο νωτιαίο άκρο αλλά και προσωπικών ευαίσθητων πληροφοριών του χρήστη, όπως ο κωδικός εισόδου του στην εφαρμογή.

Η βάση δεδομένων δημιουργείται αυτόματα με την πρώτη εκτέλεση του νωτιαίου άκρου. Χρησιμοποιήθηκε βάση MySQL.
Πριν την πρώτη εκτέλεση πρέπει να δημιουργηθεί ένα άδειο schema στη βάση με το όνομα ‘members’, στο οποίο θα δημιουργηθεί η βάση.

Στο αρχείο application.properties θα πρέπει να αλλαχτούν τα στοιχεία σύνδεσης στη βάση. Επίσης, από τις γραμμές 30 και 32 του ίδιου αρχείου, καθορίζεται το μέγιστο μέγεθος αρχείου που μπορεί να εισέλθει μέσω HTTP αιτήματος. Χρειάζεται όμως να γίνει και αλλαγή τοπικά στο SQLWorkBench επιλογή που να επιτρέπει την αποθήκευση αρχείων μεγαλύτερων των 4MB, που είναι η προεπιλογή. Η ανάπτυξη και των δύο άκρων έγινε μέσω του IntelliJIdea, μέσω του οποίου αν γίνει η φόρτωση των δύο φακέλων που εμπεριέχονται στο .rar αρχείο θα εγκατασταθούν οι απαραίτητες βιβλιοθήκες.
Κατά την πρώτη εκτέλεση του νωτιαίου άκρου πρέπει να από-σχολιασθούν οι γραμμές 36 έως 39 και να σχολιασθούν για τις επόμενες εκτελέσεις. Έτσι δημιουργείται ο διαχειριστής της εφαρμογής με email 'admin@admin.com' και κωδικό 'admin' .
Στο μετωπιαίο άκρο στον κατάλογο src/certificate βρίσκονται τα αρχεία που χρησιμεύουν για την SSL κρυπτογράφηση του. Στο package.json στην 6 γραμμή βρίσκεται η εντολή εκκίνησης του άκρου.

Πακέτα Νωτιαίου Άκρου

- Models: περιέχουν τις οντότητες που δημιουργούνται στη βάση δεδομένων, καθώς και βοηθητικές κλάσεις DTO (Data Transfer Object) ώστε αν χρειάζεται η μεταφορά πληροφορίας στο μετωπιαίο άκρο, η οποία έχει ή ευαίσθητο περιεχόμενο ή μη χρήσιμο περιεχόμενο για τη συγκεκριμένη λειτουργία, αυτό να παρακάμπτεται και να μην αποστέλλεται.
- Repositories: κλάσεις που επεκτείνουν την JPARepository μέσω των οποίων δημιουργούνται και εκτελούνται ερωτήματα στη βάση.
- Security: περιέχει την κλάση SecurityConfig η οποία επεκτείνει τη WebSecurityConfigurerAdapter από πακέτο security του Spring framework, το οποίο ελέγχει αν ο χρήστης έχει τη δυνατότητα πρόσβασης στη διεύθυνση του νωτιαίου άκρου που αιτείται να

προσπελάσει, ανάλογα με τον ρόλο που έχει ο συνδεδεμένος χρήστης (διαχειριστής ή μέλος).

- Filters:
  Authentication Filter: Κατά τη σύνδεση του χρήστη στην εφαρμογή δημιουργείται ένα access JSON web token (JWT), το οποίο χρησιμοποιείται από τον χρήστη για να γίνουν τα αιτήματα στο νωτιαίο άκρο. Επίσης δημιουργείται και ένα refresh token, το οποίο χρησιμοποιείται για να δημιουργηθεί ένα νέο access token όταν το ήδη υπάρχον λήξει. Η χρονική διάρκεια του access token είναι 15 λεπτά, ενώ του refresh token 300 λεπτά.
  Κατά την πρώτη εκτέλεση της εφαρμογής πρέπει να επιτραπεί από τον browser η πρόσβαση στη διεύθυνση https://localhost:8443 που τρέχει το νωτιαίο άκρο, πηγαίνοντας στη διεύθυνση και πατώντας Advanced > proceed to localhost .

  Authorization Filter: Επιλέγει ποιες διευθύνσεις στο νωτιαίο άκρο θα δέχονται πρόσβαση χωρίς να γίνει κάποιο filtering και σε ποιες θα πρέπει να γίνεται ταυτοποίηση. Σε αυτές που χρειάζεται ταυτοποίηση χρήστη, χρησιμοποιείται το access JWT, το οποίο λαμβάνεται από τα headers στη μορφή “Bearer + token” (δηλαδή πριν το token βρίσκεται η συμβολοσειρά “Bearer “ με ένα whitespace. Λαμβάνεται το token και ανάλογα με τον ρόλο που βρίσκεται στο “roles” στοιχείο του JWT επιτρέπεται ή όχι η πλοήγηση του χρήστη στη συγκεκριμένη διεύθυνση.
- Controllers: Διαθέτει κλάσεις οι οποίες εκτελούν μεθόδους ανάλογα τη διεύθυνση που θα κληθεί από τον χρήστη. Οι controllers δέχονται αιτήματα από τη διεύθυνση που τρέχει το μετωπιαίο άκρο https://localhost:4200 .
- Services: Λειτουργούν ως middleware ανάμεσα στους controllers και στα repositories ώστε να έρχονται εις πέρας τα αιτήματα στο νωτιαίο άκρο.

Πακέτα/Κατάλογοι Μετωπιαίου άκρου

- Admin: Αποτελεί τις αλληλεπιδράσεις του διαχειριστή στην εφαρμογή.
- Helpers: Βοηθητικά αρχεία για την ταυτοποίηση των χρηστών (διαχειριστή και μελών) κατά την είσοδό τους στην εφαρμογή αλλά και αρχείο interceptor που αναχαιτίζει τα αιτήματα στο νωτιαίο άκρο με το JWT, ώστε να γίνει η σωστή ταυτοποίηση του χρήστη όταν αυτός κάνει κάποιο αίτημα, και που διαχειρίζεται λάθη στα HTTP αιτήματα.
- Home: Αποτελεί τον κορμό του μετωπιαίου άκρου καθώς αποτελεί την αρχική σελίδα της εφαρμογής αλλά περιέχει και ως «παιδιά» τις υπόλοιπες σελίδες (σελίδα αγγελιών, μηνυμάτων, δικτύου, ειδοποιήσεων, προσωπικών δεδομένων και ρυθμίσεων).
- Login: Η σελίδα σύνδεσης του χρήστη.
- Member-Form: Η σελίδα εγγραφής του χρήστη.
- Page-not-found: Σελίδα στην οποία ανακατευθύνονται αιτήματα για σελίδες που δεν υπάρχουν.
- Services: Όπως και στο νωτιαίο άκρο αποτελούν το middleware ανάμεσα στα components και τις διευθύνσεις που ακούει το νωτιαίο άκρο, στέλνοντας τα αιτήματα του χρήστη.
- Welcome: Η αρχική σελίδα που έχει τις επιλογές εγγραφής και σύνδεσης.

Σελίδα εγγραφής και σύνδεσης

Ο χρήστης συμπληρώνει τα στοιχεία του με λατινικούς χαρακτήρες και όλα τα πεδία είναι υποχρεωτικά. Το email θα πρέπει να μην χρησιμοποιείται από κάποιον άλλο χρήστη και ο τηλεφωνικός αριθμός πρέπει να είναι αναγκαστικά 10 χαρακτήρες.
Κατά τη σύνδεση του χρήστη στην εφαρμογή αποθηκεύονται τοπικά στον browser στο local storage πληροφορίες του χρήστη όπως το email, ο ρόλος, τα access και refresh JWT, οι οποίες χρησιμοποιούνται από τα components της εφαρμογής.

Σελίδα Διαχειριστή

Η αρχική σελίδα είναι ανάλογη του ρόλου που έχει ο συνδεδεμένος χρήστης. Ο διαχειριστής έχει τις δυνατότητες να αποσυνδεθεί ή να δει την λίστα με όλους του εγγεγραμμένους χρήστες. Στη λίστα, ο διαχειριστής πατάει στο όνομα του μέλους για να περιηγηθεί στη σελίδα προσωπικών πληροφοριών του μέλους, όπου βλέπει όλες τις πληροφορίες του, ανεξάρτητα αν το μέλος τις έχει επισημάνει προσωπικές ή δημόσιες. Πατώντας πάνω στο email μπορεί να επικοινωνήσει μέσω email με τον χρήστη. Επιλέγοντας μέλη από τη στήλη «Εξαγωγή ως JSON», ο διαχειριστής εξάγει όλα τα δεδομένα (πληροφορίες και δραστηριότητες στην εφαρμογή) των επιλεγμένων χρηστών σε μορφή JSON. Αντίστοιχα στην στήλη «Εξαγωγή ως XML» εξάγονται οι πληροφορίες ως XML.

Επισήμανση: Εξάγεται και η πληροφορία των αποθηκευμένων πολυμέσων που έχει κάνει ο χρήστης σε άρθρα του στην εφαρμογή και για αυτό συνίσταται JSON formatter.

Αρχική σελίδα

Όταν ο χρήστης συνδέεται στην εφαρμογή εισέρχεται στην αρχική σελίδα. Στα αριστερά βρίσκεται πλαίσιο γρήγορης πλοήγησης μέσω του οποίου ο χρήστης μπορεί να περιηγηθεί γρήγορα στο προφίλ του, το δίκτυό του ή την αρχική σελίδα αν βρίσκεται σε κάποια άλλη σελίδα της εφαρμογής. Επίσης παρέχεται κουμπί αποσύνδεσης και στο κάτω μέρος του πλαισίου ο χρήστης βλέπει το email με το οποίο βρίσκεται συνδεδεμένος.

Στο επάνω μέρος της σελίδας βρίσκεται μπάρα μέσω της οποίας ο χρήστης πλοηγείται στο δίκτυό του, στις αγγελίες του, στις προσωπικές του συζητήσεις με φίλους, στις ειδοποιήσεις, στο προφίλ του, στις ρυθμίσεις. Ο χρήστης αναρτά άρθρα, τα οποία μπορεί να συνοδέψει είτε με μία εικόνα, είτε με ένα βίντεο είτε με ένα αρχείο ήχου.

Κάθε πολυμέσο αποθηκεύεται με τον ίδιο τρόπο, δηλαδή παίρνουμε τα τμήματα του αρχείου (τύπος, όνομα αρχείου και bytes) και τα αποθηκεύουμε στην βάση. Ο λόγος που έχουμε διαφορετικές οντότητες για το κάθε πολυμέσο (εικόνα, βίντεο, ήχος) είναι διότι η html χρησιμοποιεί διαφορετικούς τρόπους εμφάνισης αυτών στην σελίδα.

Ο χρήστης βλέπει τα άρθρα που έχει αναρτήσει ο ίδιος αλλά και τα άρθρα των φίλων του σε σειρά, βάσει του πιο πρόσφατου άρθρου και μπορεί να αλληλοεπιδράσει κάνοντας σημείωση ενδιαφέροντος (like) ή σχολιάζοντας. Πατώντας το κουμπί “comment” κάτω από ένα άρθρο ο χρήστης μπορεί να δει τη συζήτηση που γίνεται στο άρθρο και να αφήσει το δικό του σχόλιο. Επίσης, μπορεί να δει τον αριθμό των like των άρθρων όπως και αν έχει κάνει αυτός like. Μετά και το τελευταίο διαθέσιμο άρθρο του χρήστη ή φίλων του, ξεκινά η λίστα με τα προτεινόμενα άρθρα που αποτελείται από αυτά, που έχουν δημοσιεύσει μη συνδεδεμένα άτομα με τον χρήστη, στα οποία έχουν κάνει like τουλάχιστον ένας φίλος του χρήστη. Και αυτά εμφανίζονται από το πιο πρόσφατο στο πιο παλιό και ο χρήστης μπορεί να κάνει like ή να σχολιάσει.

Καρτέλα Δικτύου

Στην καρτέλα δικτύου εμφανίζονται σε μορφή πλέγματος οι φίλοι του χρήστη. Πατώντας σε αυτούς, ο χρήστης πλοηγείται στο προφίλ τους όπου βλέπει τις πληροφορίες τους. Υπάρχει πεδίο αναζήτησης χρηστών στο οποίο ο χρήστης μπορεί να ψάξει και άλλου χρήστες με τους οποίους δεν είναι φίλος, να δει τις πληροφορίες που έχουν επισημάνει ως δημόσιες και να τους στείλει αίτημα φιλίας. Η αναζήτηση χρηστών γίνεται βάσει του email. Αν το email που εισήγαγε ο χρήστης δεν χρησιμοποιείται εμφανίζεται ανάλογο μήνυμα.

Αγγελίες

Στην καρτέλα αυτή εμφανίζονται στον χρήστη αγγελίες τις οποίες έχουν αναρτήσει φίλοι του. Στο τμήμα «προτεινόμενες αγγελίες» εμφανίζονται αυτές που έχουν δημοσιεύσει οι μη συνδεδεμένοι χρήστες, με βάση τις δεξιότητες (skills) που έχει συμπληρώσει ο χρήστης στο προφίλ του. Ο χρήστης μπορεί να κάνει αίτηση για την θέση απασχόλησης που αναγράφεται σε κάθε αγγελία αλλά και να αναρτήσει τις δικές του αγγελίες καταγράφοντας επίσης μονολεκτικά τις δεξιότητες που θέλει να διαθέτει ο ενδιαφερόμενος. Επίσης, μπορεί να δει τις αγγελίες του πατώντας το ανάλογο κουμπί, που τον μεταφέρει στη σελίδα με αυτές, στην οποία μπορεί να δει ποιοι χρήστες έχουν κάνει αίτηση στις αγγελίες του.

Χώρος συζητήσεων

Ο χρήστης μπορεί να συνομιλήσει μόνο με τους φίλους του, οι οποίοι εμφανίζονται ως λίστα κάτω από το “Messages”. Ο χρήστης πατώντας στον φίλο βλέπει τη μέχρι τώρα μεταξύ τους συζήτηση.

Τα μηνύματα ταξινομούνται. Ο χρήστης μπορεί να στείλει νέο μήνυμα στη συζήτηση και όταν το κάνει ανανεώνεται αυτόματα η συζήτηση και μπορεί να δει αν ο χρήστης-φίλος έγραψε κάποιο νέο μήνυμα. Επίσης υπάρχει το κουμπί “Refresh chat” όταν ο χρήστης θέλει να δει νέα μηνύματα χωρίς ο ίδιος να στείλει.

Ειδοποιήσεις

Στη σελίδα ειδοποιήσεις ο χρήστης βλέπει τα αιτήματα φιλίας που του έχουν κάνει άλλοι χρήστες όπως και ειδοποιήσεις like και σχολίων από άλλου χρήστες στα άρθρα του. Στο επάνω μέρος, όπου φαίνονται τα αιτήματα φιλίας, ο χρήστης μπορεί να αποδεχθεί το αίτημα, να το απορρίψει και να περιηγηθεί στην σελίδα του χρήστη που έκανε το αίτημα φιλίας. Στο κάτω μέρος όπου φαίνονται οι ειδοποιήσεις, ο χρήστης βλέπει το όνομα αυτού που έκανε like ή σχόλιο, σε ποιο άρθρο του χρήστη γίνεται η αναφορά και μπορεί να το επισημάνει ως «διαβάστηκε». Οι ειδοποιήσεις που βλέπει ο χρήστης αφορούν αυτές που γίνονται από φίλους και από μη φίλους. Ειδοποίηση δημιουργείται όταν ένας χρήστης σχολιάζει ή κάνει like σε άρθρο άλλου χρήστη.

Προσωπικά Δεδομένα

Στην καρτέλα Προσωπικά Δεδομένα ο χρήστης αναγράφει την επαγγελματική του εμπειρία, τις πληροφορίες σχετικά με την εκπαίδευσή του, τις δεξιότητές του και κάποιο σύντομο βιογραφικό. Μπορεί να ορίσει τις πληροφορίες αυτές ως δημόσιες ή ιδιωτικές αφού πρώτα έχει συμπληρωθεί το πεδίο. Στο πεδίο «δεξιότητες» ο χρήστης καλείται να συμπληρώσει τις ικανότητες του μονολεκτικά, ώστε να χρησιμοποιηθούν για την εύρεση προτεινόμενων αγγελιών (π.χ. c, c++, angular, γλύπτης, ζωγράφος).

Ρυθμίσεις

Στις ρυθμίσεις ο χρήστης μπορεί να αλλάξει το email του και τον κωδικό πρόσβασης. Κατά την αλλαγή του email ο χρήστης ειδοποιείται αν το νέο email που επέλεξε χρησιμοποιείται ήδη και του ζητείται να επιλέξει ένα διαφορετικό.
Στην αλλαγή κωδικού, στο αίτημα στο νωτιαίο άκρο αποστέλλεται το email που είναι αποθηκευμένο στο local storage του browser, μαζί με το access JWT και τον νέο κωδικό. Το νωτιαίο άκρο αποκωδικοποιεί το JWT και ταυτίζει το email που έλαβε από το HTTP αίτημα με αυτό που υπήρχε στο JWT και αν ταυτίζονται η αλλαγή κωδικού εγκρίνεται. Ο τρόπος αυτός χρησιμοποιείται ως δικλείδα ασφαλείας, ώστε να μην μπορεί κάποιος χρήστης να αλλάζει τον κωδικό κάποιου άλλου, απλά αλλάζοντας το αποθηκευμένο email στο local storage του browser.

Επίλογος

Καίριο ζήτημα κατά την ανάπτυξη της εφαρμογής ήταν η δημιουργία δικλείδων ασφαλείας που μειώνουν σημαντικά τα κενά ασφαλείας ως προς τα δεδομένα και την ακεραιότητα των χρηστών. Κατά την λήψη των δεδομένων από τη βάση επειδή εμπεριέχονταν χρήσιμες αλλά και μη χρήσιμες πληροφορίες (ανάλογα το αίτημα) υπήρχε δυσκολία στο χρόνο φόρτωσης της απάντησης του αιτήματος. Για παράδειγμα κατά την λήψη των μελών στο νωτιαίο άκρο στο *MemberServiceImpl*, μέσω των *getSpecifiedMembers()* και *findMemberByEmail()*, γίνεται χρήση της συνάρτησης *findByEmail()* της JPARepository που εξάγει όλες τις πληροφορίες που έχει το μέλος, μαζί και με όλα τα collections που έχει (σ.σ. : βλέπε models>Member).
Το πρόβλημα αντιμετωπίστηκε αλλού με την “Lazy” ανάκτηση αυτών των δεδομένων και αλλού με την χρήση DTOs όπως προαναφέρθηκε.