Universitatea Tehnică din Cluj-Napoca
Facultatea de Automatică şi Calculatoare

2020

Propunere de proiect pentru admiterea la studii de master

1. Date personale ale candidatului:

1.1. Nume:	**Bogdan**
1.2. Prenume:	**Dora-Maria**
1.3. An naştere:	1997
1.4. Anul absolvirii universității:	2020
1.5. Adresa:	Strada Iuliu Coroianu, nr.4, bloc B4, sc. A, ap. 18, et. 4
1.6. Telefon:	0740738100
1.7. Fax:	
1.8. E-Mail:	dorabogdan97@gmail.com

2. Date referitoare la forma de învățământ absolvită de candidatul:

2.1. Institutia de învățământ:	**Universitatea Tehnică din Cluj-Napoca**
2.2. Facultatea	**Facultatea de Automatică și Calculatoare**
2.3. Specializarea	Informatică Aplicată

3. Titlul propunerii de cercetare (în limba română):

(Max 200 caractere)

Securitatea unei aplicații web pentru rezervarea biletelor de cinema

4. Titlul propunerii de cercetare (în limba engleză):

(Max 200 caractere)

Website security for booking movie tickets

5. Termeni cheie:

1	securitate
2	criptare
3	decriptare
4	token
5	parolă

6. Durata proiectului 2 ani.

7. Prezentarea propunerii de cercetare:

[ANEXA 1]

8. Date referitoare la lucrarea de licenţă:

8.1. Titlul lucrării de licenţă:

Aplicație web pentru rezervarea biletelor de cinema

8.2. Rezumatul lucrării de licenţă: **(Max 2000 caractere)**

Pentru lucrarea de licență s-a dezvoltat o aplicație web pentru rezervarea biletelor de cinema. Scopul său este de a eficientiza munca depusă în procesul de rezervare atât pentru utilizatori, cât și pentru administratori, servind ca sistem de management pentru administratori și ca platformă de rezervare pentru utilizatori.

Aplicația a fost scrisă în mediul de dezvoltare integrat Intellij, folosind limbajul de programare Java. Este divizată în două părți: partea de back-end și partea de front-end. Pentru partea de back-end s-a utilizat Spring Boot, iar pentru front-end Thymeleaf, CSS și JavaScript. Pentru implementarea și gestionarea bazei de date s-a folosit MySQL Workbench.

Pentru implementarea aplicației s-a utilizat șablonul Model-View-Controller care presupune împărțirea sistemului în 3: model, view și, respectiv, controller. Controller se ocupă de cererile primite de la utilizator. Coordoneaza resursele necesare pentru aceste cereri și apelează partea de Model adecvată. Partea de Model reprezintă datele aplicației și se ocupă cu actualizarea View-ului. Partea de View se referă la interfața cu utilizatorul, ceea ce vede utilizatorul, și este responsabilă cu afișarea datelor primite de la Model.

Baza de date a cinematografului joacă un rol important în buna funcționare a aplicației, deoarece aceasta este responsabilă de menținerea integrității datelor și de stocarea acestora. Baza de date este alcătuită din 6 tabele, fiecare având un nume sugestiv pentru datele ce au fost stocate în aceasta.

Pentru securitate s-a folosit un login simplu pe bază de utilizator și parolă. Înainte ca datele noului utilizator să fie salvate în baza de date, parola utilizatorului este criptată. Pentru criptare s-a folosit „BcryptPasswordEncoder”, unul dintre mecanismele de codificare suportate de Spring Security.

9. Activitatea științifică a candidatului:

[ANEXA 2]

DATA: 20.07.2020

TITULAR DE PROIECT,
Nume, prenume: **Bogdan Dora-Maria**
Semnătura:

7. Prezentarea programului de cercetare:

7.1. STADIUL ACTUAL AL CUNOASTERII IN DOMENIU PE PLAN NATIONAL SI INTERNATIONAL, RAPORTAT LA CELE MAI RECENTE REFERINTE DIN LITERATURA DE SPECIALITATE.*

Securitatea ocupă un rol foarte important în orice sistem, cerințele utilizatorului cu privire la menținerea datelor confidențiale trebuie îndeplinite.

În articolul [1], autorii descriu vulnerabilitățile de securitate ale aplicațiilor web și metodele prin care acestea pot fi soluționate. Aceștia susțin că factorul decisiv în protecția parolelor este lungimea caracterelor și nu complexitatea acestora.

În articolul [2], autorii afirmă că parola rămâne cheia componentă a majorității sistemelor de autentificare online și că spargerea acestora amenință direct utilizatorii. Pentru a îmbunătăți securitatea parolei, utilizatorul ar trebui să utilizeze parole unice și puternice pentru diferite conturi. Una dintre metodele descrise în lucrare este securitatea bazată pe token, fiind cea mai bună modalitate de autentificare a utilizatorilor. Datele stocate în token sunt de obicei criptate pentru a preveni citirea neautorizată.

Autorii din [3] susțin că vulnerabilitatea cea mai comună de securitate este SQL Injection. Aceasta, cu ajutorul comenzilor SQL, trimite un cod care poate accesa, modifica sau șterge informații din baza de date, compromițând securitatea aplicației.

7.2. OBIECTIVELE PROIECTULUI **

Obiectivele principale ale proiectului sunt:

- Îmbunătățirea securității parolei prin implementarea token-ului
- Eliminarea amenințărilor de tip SQL Injection
- Detectarea autentificării utilizatorului de pe mai multe dispozitive simultan
- Trimiterea unor e-mail-uri de verificare a autenticității utilizatorului în cazul în care acesta se loghează de pe un dispozitiv nou
- Analiza parolei în timp real și catalogarea acesteia în funcție de complexitatea ei în una din cele trei categorii: slabă, medie, puternică

7.3. DESCRIEREA PROIECTULUI***

Pe baza articolelor din secțiunea 7.1 și pe baza rezultatelor obținute la licență, există multe abordări și îmbunătățiri ce pot fi aduse pentru securitatea aplicației.

Pentru început, se va implementa autentificarea pe bază de token care presupune verificarea utilizatorului de fiecare dată când acesta trimite un nou request. Token-ul va avea informații precum: numele utilizatorului, id-ul corespunzător, rolul și data creării și expirării token-ului.

Se va implementa un sistem de avertizare pentru trimiterea unor e-mail-uri de verificare atunci când utilizatorul folosește un dispozitiv nou. E-mail-ul va conține un număr aleator pe care utilizatorul trebuie să-l introducă într-un câmp aferent din pagină.

O altă funcționalitate privind securitatea ce va fi implementată este analiza parolei în timp real și catalogarea acesteia în funcție de complexitatea ei în una din cele trei categorii (slabă, medie și puternică) și recomandarea ca utilizatorul să folosească caractere speciale.

Toate obiectivele vor fi implementate după mai multe studii în domeniul securității web și după cercetarea celor mai bune metode de implementare.

7.4. REFERINȚE BIBLIOGRAFICE

[1] Abdulghani Ali Ahmed, Lee Mei Khay, Securing user credentials in web browser: Review and suggestion, *Conference on Big Data and Analytics,* 16-17 Nov. 2017, Kuching, Malaysia
[2] Shuang Liang, Yue Zhang, Bo Li, Xiaojie Guo, Chunfu Jia and Zheli Liu, SecureWeb: Protecting Sensitive Information Through the Web Browser Extension with a Security Token, *TSINGHUA SCIENCE AND TECHNOLOGY,* Volume 23, p. 528, 2018
[3] Voitovych O.P., Yuvkovetskyi O.S., Kupershtein L.M., SQL Injection Prevention System, *Radio Electronics & InfoCommunications,* September 11-16, 2016, Kiev, Ukraine

7.5. OBIECTIVELE ȘI ACTIVITĂȚILE DE CERCETARE DIN CADRUL PROIECTULUI**:**

An	Obiective științifice (Denumirea obiectivului)	Activități asociate
An 1	1. Autentificarea pe bază de token	1. Implementare
		2. Testare
	2. Eliminarea amenințărilor de tip SQL Injection	1. Studiu bibliografic
		2. Implementare

An 2	1. Trimiterea de e-mail-uri atunci când utilizatorul se conectează de pe un dispozitiv nou	1. Găsirea unei soluții cât mai eficiente pentru trimiterea de e-mail-uri și implementarea acesteia
		2. Testare
	2. Detectarea autentificării utilizatorului de pe mai multe dispozitive	1. Implementare
		2. Testare

7.6. CONSULTANȚI*****

9. Activitatea stiintifica a candidatului:

9.1. PREMII OBTINUTE LA MANIFESTARI STIINTIFICE.

9.2. PARTICIPAREA CU LUCRARI LA SESIUNI DE COMUNICARI STIINTIFICE.

9.3. PUBLICATII.

9.4. PARTICIPAREA IN PROGRAME DE CERCETARE-DEZVOLTARE NATIONALE SI INTERNATIONALE

(nume proiect/director proiect/cadru didactic care a supervizat cercetarea – pentru proiecte din UTCN)
(nume proiect/director proiect/institutia in care s-a derulat cercetarea – pentru proiecte din afara UTCN)

9.5. BURSE OBTINUTE.

- FINANTATORUL;
- PERIOADA SI LOCUL;
- PRINCIPALELE REZULTATE SI VALORIFICAREA LOR;
