



Universitatea Tehnică a Moldovei

SISTEM DE MANAGEMENT AL UTILIZATORILOR ÎN APLICAȚIILE WEB

Masterand:

Marii Alexandru

Conducător:

conf. univ., dr. Ababii Victor

Chișinău – 2019

ADNOTARE

**La teza de masterat: „Sistem de management al utilizatorilor în aplicațiile web”,
elaborată de Marii Alexandru, Chișinău, 2019**

Cuvinte cheie: jeton de acces, jeton de identitate, sistem, aplicație web, autentificare, autorizare, integrare, JWT, criptare, semnare, OpenID Connect, Angular 8, .NET Core, serviciu, aplicație client, roluri.

Lucrarea de față are ca scop proiectarea și implementarea unui sistem web care ar permite managementul de utilizatori în mai multe aplicații web.

Proiectul vizează implementarea unui sistem care să efectueze eficient managementul cu utilizatorii în aplicațiile integrate cu acesta. Aceasta presupune că o dată integrat cu acest sistem, va dispărea necesitatea de a adăuga componenta de management de utilizatori din aplicația propriu zisă.

Tehnologiile utilizate sunt: Angular 8 pentru elaborarea funcționalităților aplicației client a sistemului, .NET Core 2.2 pentru elaborarea interfețelor de program a sistemului, MSSQL pentru baza de date, Bootstrap 4 pentru stilizarea aplicației client, OpenID Connect pentru interacțiune sistem-sistem.

Memoriul explicativ conține Introducere, 3 capitole, concluzii, bibliografie cu 19 titluri, dintre care 66 pagini text de bază, 29 figuri.

Capitolul 1: definește cadrul teoretic al elaborării lucrării, analiza situației în domeniul de proiectare, definiții generale din cadrul autentificării și autorizării, scurta descriere a diferitor protocoale de autentificare, avantajele și dezavantajele diferitor protocoale de autentificare.

Capitolul 2: definește arhitectura sistemului, descrierea succintă a tehnologiilor utilizate și caracteristicile acestora.

Capitolul 3: descrie modalitatea de implementare a sistemului și conține modelarea sistemului, prezentarea tuturor componentelor sistemului, modalitatea de funcționare a acestora și interacțiunea dintre ele.

ANNOTATION

**On the master's thesis: „ User management system in web applications”,
elaborated by Marii Alexandru, Chişinău, 2019.**

Keywords: access token, identity token, system, web application, authentication, authorization, integration, JWT, encryption, signing, OpenID Connect, Angular 8, .NET Core, service, client application, roles.

The present work aims to design and implement a web system that would allow user management in several web applications.

The project aims to implement a system that efficiently performs the management with the users in the applications integrated with it. This means that once integrated with this system, the need to add the user management component of the application itself will disappear.

The technologies used are: Angular 8 for the elaboration of the functionalities of the client application of the system, .NET Core 2.2 for the elaboration of the application program interfaces, MSSQL for the database, Bootstrap 4 for the stylization of the client application, OpenID Connect for the interaction between systems.

The report contains Introduction, 3 chapters, conclusions, bibliography with 19 titles, including 66 pages of main text and 29 figures.

Chapter 1: defines the theoretical framework of the elaboration of the paper, the analysis of the situation in the field of design, general definitions within the authentication and authorization, the brief description of different authentication protocols, the advantages and disadvantages of different authentication protocols.

Chapter 2: defines the system architecture, brief description of the technologies used and their characteristics.

Chapter 3: describes how to implement the system and contains the modeling of the system, presentation of all the components of the system, how they work and the interaction between them.

CUPRINS

INTRODUCERE.....	8
1. ANALIZA SITUAȚIEI ÎN DOMENIUL DE PROIECTARE	9
1.1 Introducerea in domeniul de studiu.....	9
1.2 Autentificare și autorizare – generalități	10
1.3 Protocoale de autentificare	11
2. METODOLOGIA ȘI TEHNOLOGIILE UTILIZATE ÎN DEZVOLTARE	21
2.1 Arhitectura sistemului	21
2.2 Algoritmi de procesare și transmitere a datelor	22
2.3 Limbaje de programare și framework-uri	31
3. IMPLEMENTAREA SISTEMULUI.....	36
3.1 Modelarea sistemului	36
3.2 Interfețele de programare a aplicației (API)	46
3.3 Descrierea aplicației web	49
3.4 Integrarea serviciilor cu sistemul	55
CONCLUZII	57
BIBLIOGRAFIE	58
ANEXA 1 (Crearea jetoanelor de autentificare).....	59
ANEXA 2 (Managementul de jetoane).....	60
ANEXA 3 (Validarea jetoanelor).....	61
ANEXA 4 (Algoritmul de hashing și verificare a parolelor).....	62
ANEXA 5 (Extragerea datelor din jetonul expirat)	63
ANEXA 6 (Controller utilizat pentru integrare)	64
ANEXA 7 (Crearea jetoanelor semnate pentru comunicarea Sistem-Sistem).....	66

INTRODUCERE

Trăim într-un timp când tehnologiile IT se dezvoltă cu pași enormi. Atunci când toată informația tinde a trece de la suport de hârtie la suport digital apare necesitatea de a proteja această informație de accesarea de către persoane terțe care nu au dreptul de a o vizualiza sau modifica. Limitarea accesului la date este una dintre cele mai utilizate modalități de protejare a acestora.

Pentru a limita accesul la date este necesar mai întâi de a identifica utilizatorul prin procesul de autentificare după care de a identifica drepturile acestuia prin intermediul autorizării.

Există câteva metode de a efectua procesul de autentificare :

- Autentificare bazată pe formular
- Autentificare cu certificat client SSL
- Autentificare terță parte

Companiile mici adesea utilizează metoda de autentificare bazată pe formular, sau autentificarea terță parte care sunt relativ simplu de implementat.

Companiile medii utilizează autentificarea terță parte care oferă un nivel mai înalt de încredere, partea terță luând toate problemele de autentificare asupra lor livrând spre final o identitate de încredere a solicitantului.

Companiile mari preferă să dezvolte propriul sistem de autentificare a utilizatorilor bazat pe toate aceste trei metode.

Toate aceste metode trebuie luate în calcul dezvoltarea arhitecturii unei aplicații și în dependență de necesitate de utilizat cel mai comodă metodă pentru a satisface necesitățile aplicației furnizate. Ca exemplu dacă este necesară doar statistica utilizării aplicației este destul de utilizat autentificarea prin formular pentru a evita consumul excesiv de resurse și timp.

BIBLIOGRAFIE

- [1] https://www.ibm.com/support/knowledgecenter/ro/SSYJ99_8.5.0/plan/authentication.html
- [2] <https://studfiles.net/preview/2886463/page:3/>
- [3] http://www.aut.upt.ro/~bgroza/Slides/Slides_Autenticare.pdf
- [4] <https://studfiles.net/preview/2886463/>
- [5] «Современные операционные системы», 2-е издание, э. Таненбаум
- [6] <http://citforum.ru/security/articles/galatenko/>
- [7] https://ru.wikipedia.org/wiki/%D0%9E%D0%B4%D0%BD%D0%BE%D1%80%D0%B0%D0%B7%D0%BE%D0%B2%D1%8B%D0%B9_%D0%BF%D0%B0%D1%80%D0%BE%D0%BB%D1%8C
- [8] https://en.wikipedia.org/wiki/Challenge%20response_authentication
- [9] <https://openid.net/connect/faq/>
- [10] <https://developers.onelogin.com/openid-connect>
- [11] https://ru.wikipedia.org/wiki/JSON_Web_Token
- [12] <https://github.com/Flibberty-GEA>
- [13] <https://docs.microsoft.com/ro-ro/dotnet/core/>
- [14] <https://proglib.io/p/10-things-about-dotnet-core/>
- [15] <https://metanit.com/web/typescript/1.1.php>
- [16] <https://ru.wikipedia.org/wiki/AngularJS>
- [17] [https://ru.wikipedia.org/wiki/Bootstrap_\(%D1%84%D1%80%D0%B5%D0%B9%D0%BC%D0%B2%D0%BE%D1%80%D0%BA\)](https://ru.wikipedia.org/wiki/Bootstrap_(%D1%84%D1%80%D0%B5%D0%B9%D0%BC%D0%B2%D0%BE%D1%80%D0%BA))
- [18] <https://use-web.ru/news.php?id=53&tid=2>
- [18] https://ru.wikipedia.org/wiki/C_Sharp
- [19] <http://inf.ucv.ro/~mihaiug/courses/is/lab/lab3-4>