Universitatea Tehnică a Moldovei

# SECURITATEA SERVICIILOR REST API UTILIZÂND PROTOCOLUL OAUTH2

# SECURITY OF REST API SERVICES USING OAUTH2 PROTOCOL

**Masterand:**

**Ciubotaru Radu**

**Conducător:**

**conf.univ., dr. Beşliu Victor**

**Chişinău – 2019**

MINISTERUL EDUCAȚIEI, CULTURII ȘI CERCETĂRII
al REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei
FACULTATEA Calculatoare, Informatică şi Microelectronică
Departamentul Ingineria Software și Automatică

Admis la susţinere
Şef de catedră: conf. univ., dr. Ciorba Dumitru
_____
„15" decembrie 2019

# Securitatea serviciilor REST API utilizând protocolul OAuth2

Teză de master în

Tehnologii Informationale

Masterand: Ciubotaru Radu (_____)
Conducător: conf.univ., dr. Beşliu Victor (_____)

Chişinău – 2019

**Rezumat**

Proiectul tezei de master prezintă o metodă de securizare a aplicațiilor REST API. Metoda cercetată este protocolul de autentificare OAuth2.

Protocolul OAuth2 este un standard deschis de autorizare, care permite unei aplicații terțe acces limitat la resursele de utilizator protejate, fără a crea un cont nou. Acest protocol include mai multe metode de autorizare, în dependență de clientul (aplicație web) care lucrează cu aplicația API.

În această lucrare am elaborat o aplicație be bază de servicii API și ca metodă de securitate a punctelor finale de accesare a resurselor am setat protocolul OAuth2. Aplicația API este scrisă în limbajul JAVA, și utilizează o serie de biblioteci ajutătoare pentru configurarea protocolului de securitate. Am integrat în această aplicație instrumentul Swagger acesta înlocuind clientul (aplicația web).

Protocolul este configurat să accepte doar clienți confidențiali, ceea ce obligă clientul să păstreze confidențialitatea credențialelor utilizatorului. Aplicația dezvoltată, nu permite accesarea resurselor de către mai mulți clienți, aceasta permite accesarea doar de către un client. Metoda de autentificare se numește "Resource owner password credentials". Aceasta înseamnă că utilizatorul, numit și proprietarul resursei, va trebui la început să introducă numele utilizatorului și parola, o dată ce aplicația autentifică utilizatorul, acesta va primi un token de acces pe care îl va folosi în continuare pentru a accesa alte resurse.

Tehnologia aleasă este foarte actuală în prezent, și este folosită în proiecte gigante, cum ar fi rețelele de socializare (Facebook, Instagram) sau Google. Această metodă de autentificare este cel mai des folosită de utilizatorii rețelelor de socializare, și anume atunci când utilizatorii se autentifică în aplicații terțe apăsând doar un buton (în cazul utilizării facebook "Log in with Facebook").

În acest proiect de master, am cercetat detailat protocolul de autentificare OAuth2 și aplicația dezvoltată poate servi la baza dezvoltării unui proiect enterprise.

**Abstract**

This thesis summarizes a method of security of REST API services using OAuth2 protocol.

OAuth2 is an open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords. This mechanism is used by companies such as Amazon, Google, Facebook, Microsoft and Twitter to permit the users to share information about their accounts with third party applications or websites.

Generally, OAuth provides to clients a "secure delegated access" to server resources on behalf of a resource owner. It specifies a process for resource owners to authorize third-party access to their server resources without sharing their credentials. Designed specifically to work with Hypertext Transfer Protocol (HTTP), OAuth essentially allows access tokens to be issued to third-party clients by an authorization server, with the approval of the resource owner. The third party then uses the access token to access the protected resources hosted by the resource server.

OAuth is a service that is complementary to and distinct from OpenID. OAuth is also distinct from OATH, which is a *reference architecture* for *authentication*, not a *standard* for *authorization*. However, OAuth is directly related to OpenID Connect (OIDC) since OIDC is an authentication layer built on top of OAuth 2.0. OAuth is also distinct from XACML, which is an authorization policy standard. OAuth can be used in conjunction with XACML where OAuth is used for ownership consent and access delegation whereas XACML is used to define the authorization policies (e.g. managers can view documents in their region).

Doing this thesis, I have investigated protocol of autentication OAuth2, and developed an application based on this protocol that could serve as good start for an enterprize application.

## Cuprins