МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧОРНОМОРСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ПЕТРА МОГИЛИ

Григор'єв Даниїл Олександрович

УДК 004.42

Розробка відкритої авторизації в сучасних web-системах.

122 – Комп'ютерні науки

Автореферат
магістерської кваліфікаційної роботи на здобуття освітньої кваліфікації
«Магістр комп'ютерних наук»

Миколаїв – 2021

Магістерська кваліфікаційна робота є рукопис.

Робота виконана в Чорноморському національному університеті імені Петра Могили Міністерства освіти і науки України на кафедрі інтелектуальних інформаційних систем

Науковий керівник: кандидат технічних наук, доцент кафедри інженерії програмного Давиденко Євген Олександрович.

Рецензент: канд. техн. наук, доцент, доцент кафедри інженерії програмного забезпечення Швед Альона Володимирівна

Захист відбудеться «22» лютого 2021 р. о $9^{\underline{30}}$ год. на засіданні екзаменаційної комісії (ауд. 2-403) у Чорноморському національному університеті імені Петра Могили за адресою: 54003, м. Миколаїв, вул. 68-ми Десантників, 10.

З магістерською роботою можна ознайомитися в бібліотеці Чорноморського національного університету імені Петра Могили за адресою: 54003, м. Миколаїв, вул. 68-ми Десантників, 10.

Автореферат представлений «16» лютого 2021 р.

Секретар
екзаменаційної комісії,
ст.викл. Н. М. Болюбаш

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми.

Більша частина веб-додатків потребують ідентифікації користувача, але з різних причин користувач не хоче надавати логін та пароль маловідомому сервісу, що ставить під загрозу конфіденційність його даних. Також зручно знати лише один логін та пароль від одного сервісу, якому користувач довіряє, наприклад Google, Facebook або особистий кабінет веб-банкінгу. Однак, було зафіксовано ряд атак на вразливості існуючих протоколів авторизації. З цих причин постає необхідність пошуку й розробки більш надійного та швидкого способу авторизації.

Метою даної роботи є аналіх протоколів авторизації та вибору безпечного протоколу для авторизації.

Практичне значення отриманих результатів.

Отримання навичок розробки web-систем з використанням відкритої авторизації.

Структура магістерської кваліфікаційної роботи. Пояснювальна записка до магістерська кваліфікаційна роботи складається із вступу, 4 розділів, висновків. Загальний обсяг роботи складає 72 сторінки, 5 рисунків, 1 таблиць та 39 посилань на літературні джерела.

Публікації. Результати даної магістерської кваліфікаційної роботи було надруковано у тезах Всеукраїнської науково-методичної конференції молодих вчених, аспірантів і студентів «Могилянські читання – 2021» у секції Комп’ютерні науки.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі магістерської кваліфікаційної роботи обґрунтовано актуальність обраної теми, сформульовано мету і задачі дослідження, визначено предмет та об’єкт дослідження.

У першому розділі було розглянуто предметну сферу кваліфікаційної роботи. Було розлянуто поняття протоколу для авторизації, було описано проблематику стандартних підходів та протоколів.

Розглянуто основні протоколи такі як:

- SAML 2.0;
- OpenID Connect 1.0;
- OAuth 2.0.

Кожен з протоколів було розглянуто окремо для вибору протоколу для авторизації в проекті роботи.

SAML підтримує єдиний вхід, а також підтримує авторизацію за маршрутом запиту атрибутів. OAuth орієнтований на авторизацію, навіть якщо її часто примушують виконувати роль автентифікації, наприклад, коли використовується соціальний логін, такий як «вхід за допомогою облікового запису Facebook». З технічної точки зору SAML визначає формат маркера, його шифрування ускладнюється, а розмір обмінюваних повідомлень є значним. На відміну від цього, OAuth2 не використовує жодного шифрування повідомлень (він покладається на HTTPS) і не визначає формат маркера.

Привабливість OAuth2 полягає у простоті використання та гнучкості: його можна використовувати на мобільних пристроях, смарт-пристроях (наприклад, смарт-телевізорах), веб-програмах, односторінкових програмах тощо. Багато бібліотек доступні для полегшення процесу інтеграції з різними типами клієнтів та постачальниками послуг. SAML, навпаки, не був розроблений з урахуванням цих сучасних програм, що ускладнювало використання в цих системах. Він зазвичай використовується з традиційними веб-програмами.

У другому розділі було розглянуто протокол OAuth в деталях для використання в кваліфікаційній роботі.

OAuth вирішує проблеми стандартної авторизації за допомогою логіну та паролю, вводячи рівень авторизації та відокремлення ролі клієнта від ролі власника ресурсу. В OAuth клієнт запитує доступ до контрольованих ресурсів власником ресурсу та розміщується на сервері ресурсів, і отримує набір облікових даних, відмінних від даних ресурсу власника.

Замість використання облікових даних власника ресурсу для доступу захищений ресурсів, клієнт отримує маркер доступу - рядок, що позначає а конкретний обсяг, термін служби та інші атрибути доступу. Маркери доступу видаються стороннім клієнтам сервером авторизації з схвалення власника ресурсу. Клієнт використовує маркер доступу ддя отримати доступ до захищених ресурсів, розміщених на сервері ресурсів.

Наприклад, кінцевий користувач (власник ресурсу) може надати доступ службі друку доступ до його захищених фотографій, що зберігаються на фото-сервісі спільного використання (сервер ресурсів), без надання спільного доступу до її імені користувача та пароль для служби друку. Натомість вона автентифікується безпосередньо із сервером, якому довіряє служба обміну фотографіями (сервер авторизації), який видає делегування послуги друку конкретні облікові дані (маркер доступу).

Також було розглянуто частини та параметри протоколу, його взаємодію з HTTPS та методи авторизації. Було розглянуто та взято до уваги вразливості протоколу OAuth, такі як:

- Неправильна реалізація неявного типу
- Порушено захист CSRF
- Витоки кодів авторизації та маркерів
- Неправильна перевірка redirect_uri

В третьому розділі детально описано процес створення застосунку. Було обрано і описано оптимальні методи авторизації. Реалізовано більшість із них. Описано структуру системи з використанням цих методів.

Описано модифікацію методу коду авторизації – PKCE.

PKCE - це розширення безпеки OAuth 2.0 для загальнодоступних клієнтів на мобільних пристроях, призначене для того, щоб уникнути зловмисної програми, яка проникає на той самий комп'ютер від перехоплення коду авторизації. У вступі RFC 7636 розглядаються механізми такої атаки.

PKCE має власну іншу специфікацію. Це дозволяє програмам використовувати найнадійніші потоки OAuth 2.0 у відкритих або ненадійних клієнтах - потік коду авторизації. Для того, щоб ефективно використовувати динамічно згенерований пароль, він досягає цього, виконуючи деякі налаштування перед потоком і деяку перевірку в кінці потоку.

Було розглянуто застарілі методи авторизації та не рекомедовані до розробки. У розділі було детально розглянуто використання та створення авторизації на базі OAuth, з реалізацією основних методів відкритої авторизації. Булу реалізовано майже всі актуальні потоки та методи авторизації використовуючи мову JavaScript.

У методичній частині розроблено практичні роботи на теми на теми «Введення в .NET Core» та «Знайомство з WebApi».

ЗАГАЛЬНІ ВИСНОВКИ

У данній роботи було розглянуто популярні протоколи авторизації, їх недоліки. Було досліджено та проаналізовано протоколи що можуть використовуватись для створення авторизації для веб-систем, описано алгортми роботи протоколі та обрано оптимальний протокол для створення авторизації у проекті.

Розглянуть деякі існуючі вразливості протоколу відкритої авторизації та описані метод для їх запобігання. В подальшому реалізовано для забезпечення більшої безпеки додатку.

Було розроблено модель авторизації на базі OAuth. Модель може бути масштабованою для подальшого використання у других проектах. Отриманий досвід під час аналізу допоміг реалізувати усі методи авторизації.

Отриманий під час дослідження та побудови моделі досвід допоміг реалізувати основні вимоги запропонованої моделі авторизації. Отримана модель може використовуватись розробниками для реалізації авторизації веб-застосунків, а також може бути надалі масштабована та розширена при появі нових загроз та атак на протокол авторизації OAuth 2.0.

АНОТАЦІЯ

Григор’єв Д. О.
Розробка відкритої авторизації в сучасних web-системах. – На правах рукопису.

Представлена магістерська кваліфікаційна робота складається з трьох розділів, загальний обсяг роботи – 72 сторінки. Містить 32 літературних посилань, 7 ілюстрацій, 2 таблиці. Основною метою роботи є підвищення захищеності способу авторизації вебзастосунків, які використовують протоколи авторизації. Для досягнення мети потрібно провести дослідження та аналіз існуючих протоколів авторизації, обрати найбільш безпечний для реалізації, виявити та дослідити існуючи атаки на обраний протокол авторизації – OAuth 2.0, та базуючись на складеному переліку атак побудувати модель безпечного способу авторизації на основі даного протоколу.

Об’єкт дослідження даної роботи – протоколи авторизації для веб-застосунків, що використовують API та OAuth 2.0.

Предметом дослідження виступає протокол авторизації OAuth 2.0.

Під час написання роботи були проведені аналіз, дослідження та узагальнення технічної і наукової літератури, запропоновано реалізацію моделі безпечного способу авторизації на основі протоколу OAuth 2.0 для веб-застосунків. Значення даної роботи зумовлено використанням розробниками запропонованої моделі для реалізації безпечного способу авторизації кінцевих користувачів, та побудови безпечних веб застосунків, що використовують протокол авторизації OAuth 2.0.

Ключові слова OAuth 2.0, протокол авторизації, маркери доступу, код авторизації, атака, модель, безпека, TLS, PKCE.

ABSTRACT

Hryhoriev D. O.

Developent of open authorization in modern web-systems. – On the rights of the manuscript.

The presented thesis consists of three sections, the total volume of work - 72 pages. Contains 32 literary references, 7 illustrations, 2 tables. The main purpose of this work is to increase the security of the method of authorization of web applications that use authorization protocols. To achieve this goal, you need to research and analyze existing authorization protocols, choose the most secure to implement, identify and investigate existing attacks on the selected authorization protocol - OAuth 2.0, and based on a list of attacks to build a model of secure authorization based on this protocol.

The object of this study is authorization protocols for web applications that use the API and OAuth 2.0.

The subject of the study is the authorization protocol OAuth 2.0.

During the writing of the work, the analysis, research and generalization of technical and scientific literature were carried out, the implementation of the model of a secure method of authorization based on the OAuth 2.0 protocol for web applications was proposed. The value of this work is due to the use of the proposed model by the developers to implement a secure way to authorize end users, and build secure web applications that use the authorization protocol OAuth 2.0.

Keywords OAuth 2.0, authorization protocol, access tokens, authorization code, attack, model, security, TLS, PKCE.