TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

BÀI TẬP LỚN 2:

Tìm hiểu về OpenID Connect, OAuth 2.0 và xây dựng triển khai hệ thống IAM dựa trên WSO2

Đỗ Minh Đức
Duc.dm200158@sis.hust.edu.vn

Giảng viên hướng dẫn: TS. Trần Quang Đức

Chữ ký của GVHD

Bộ môn: Khoa học máy tính
Trường: Công nghệ Thông tin và Truyền thông

HÀ NỘI, 8/2023

Lời cảm ơn

Đầu tiên và trên hết, em xin gửi lời cảm ơn chân thành tới giáo viên hướng dẫn , thầy Trần Quang Đức, với sự kiên nhẫn và sự hướng dẫn tận tâm đã giúp em đi sâu vào chủ đề và phát triển khả năng nghiên cứu cũng như tư duy phân tích. Những lời khuyên và góp ý của thầy đã góp phần quan trọng để đưa đề tài này đến một tầm cao mới.

Em cũng xin bày tỏ lòng biết ơn đến tất cả những nguồn tài liệu và nguồn thông tin mà em đã sử dụng trong quá trình nghiên cứu. Sự đa dạng và phong phú của các nguồn tài liệu này đã giúp chúng tôi có cái nhìn toàn diện và chi tiết về đề tài.

Một lần nữa, em xin chân thành cảm ơn tất cả những người đã đồng hành cùng em trong hành trình này. Những lời cảm ơn này không thể nào bày tỏ hết lòng biết ơn chân thành của em.

Xin chân thành cảm ơn và kính chúc mọi điều tốt lành đến tất cả mọi người.

Trân trọng,

Đức

Đỗ Minh Đức

Tóm tắt nội dung đồ án

Đồ án tập trung vào nghiên cứu và triển khai một hệ thống quản lý xác thực và ủy quyền dựa trên các giao thức OpenID Connect và OAuth 2.0. Nội dung đồ án tập trung vào các khía cạnh quan trọng của việc xây dựng hệ thống quản lý danh mục người dùng và ứng dụng, đồng thời cung cấp tính năng Single Sign On (SSO), Single Sign Out (SSO) và xác thực đa nhân tố.

Một số điểm chính trong nội dung đồ án gồm:

1. Tìm hiểu về OpenID Connect và OAuth 2.0: Đồ án bắt đầu với việc nghiên cứu sâu về hai giao thức quan trọng trong việc xây dựng hệ thống xác thực và ủy quyền - OpenID Connect và OAuth 2.0. Điều này bao gồm hiểu rõ về cách các giao thức này hoạt động, các phương thức xác thực và cách thức cung cấp quyền truy cập an toàn cho người dùng và ứng dụng.
2. Triển khai hệ thống IAM (Quản lý Danh mục người dùng và ứng dụng): Đồ án tập trung vào việc triển khai một hệ thống quản lý danh mục người dùng và danh mục ứng dụng bằng cách sử dụng các công cụ như WSO2 và Keycloak. Việc này đảm bảo rằng hệ thống có khả năng quản lý thông tin người dùng và ứng dụng một cách hiệu quả và an toàn.
3. Single Sign On (SSO) và Single Sign Out (SSO): Đồ án mô tả cách triển khai tính năng SSO và SSO trong hệ thống. SSO cho phép người dùng đăng nhập một lần và truy cập vào nhiều ứng dụng mà không cần phải đăng nhập lại. SSO cũng đồng thời hỗ trợ tính năng SSO để người dùng có thể thoát khỏi tất cả các ứng dụng khi họ đăng xuất khỏi một ứng dụng cụ thể.
4. Xác thực đa nhân tố: Một phần quan trọng trong đồ án là xây dựng khả năng xác thực đa nhân tố. Điều này đảm bảo rằng việc xác thực của người dùng không chỉ dựa trên một yếu tố như mật khẩu, mà còn sử dụng các yếu tố bổ sung như mã OTP, xác thực dấu vân tay, hoặc xác thực khuôn mặt.

Tóm lại, đồ án tập trung vào việc nghiên cứu và triển khai một hệ thống quản lý xác thực và ủy quyền, đặc biệt là sử dụng OpenID Connect và OAuth 2.0, cung cấp tính năng Single Sign On, quản lý danh mục người dùng và ứng dụng, cũng như xác thực đa nhân tố. Các công cụ như WSO2 và Keycloak được sử dụng để thực hiện triển khai hệ thống này.

MỤC LỤC

CHƯƠNG 1. GIỚI THIỆU ĐỀ TÀI

1.1 Đặt vấn đề

Trong thời đại số hóa và kết nối mạng ngày nay, việc bảo vệ thông tin và quản lý quyền truy cập đã trở thành một trong những thách thức quan trọng nhất mà các tổ chức phải đối mặt. Đặc biệt, trong môi trường công nghệ thông tin ngày càng phức tạp và đa dạng, việc đảm bảo rằng chỉ người dùng có quyền truy cập vào thông tin và tài nguyên cần thiết đã trở thành một nhiệm vụ phức tạp và quan trọng.

Hệ thống quản lý xác thực và ủy quyền là một phần quan trọng trong việc đảm bảo an ninh thông tin và quản lý quyền truy cập hiệu quả. Từ việc xác thực người dùng đến việc quản lý danh mục ứng dụng và đảm bảo tính năng Single Sign On, những yếu tố này đóng vai trò quan trọng trong việc đảm bảo tính bảo mật và tiện ích cho người dùng.

Trong bối cảnh này, giao thức OpenID Connect và OAuth 2.0 đã trở thành các tiêu chuẩn quan trọng trong việc xây dựng hệ thống xác thực và ủy quyền. Sự phổ biến của những giao thức này đã đánh dấu sự tiến bộ trong việc giải quyết các vấn đề liên quan đến xác thực an toàn, quản lý quyền truy cập hiệu quả và tạo ra trải nghiệm người dùng liền mạch.

Tuy nhiên, việc triển khai và quản lý hệ thống quản lý xác thực và ủy quyền không phải lúc nào cũng dễ dàng. Việc tích hợp các tính năng như Single Sign On, quản lý danh mục người dùng và ứng dụng, cũng như xác thực đa nhân tố đòi hỏi kiến thức sâu rộng về các giao thức và công cụ tương ứng.

Chính vì vậy, trong đồ án này, em tập trung vào việc nghiên cứu và triển khai một hệ thống quản lý xác thực và ủy quyền dựa trên giao thức OpenID Connect và OAuth 2.0. Em cũng xây dựng tính năng Single Sign On, quản lý danh mục người dùng và ứng dụng, cũng như tích hợp xác thực đa nhân tố. Mục tiêu của đồ án là đưa ra một giải pháp thực tế và hiệu quả để giúp tổ chức tăng cường an ninh thông tin và quản lý quyền truy cập một cách tốt nhất trong môi trường ngày càng kết nối và phức tạp của ngày nay.

1.2 Mục tiêu và phạm vi đề tài

Mục Tiêu:

Mục tiêu chính của đồ án là nghiên cứu, triển khai và đánh giá hiệu quả của một hệ thống quản lý xác thực và ủy quyền dựa trên giao thức OpenID Connect và OAuth 2.0. Cụ thể, các mục tiêu cụ thể của đồ án bao gồm:

1. **Nghiên cứu về OpenID Connect và OAuth 2.0:** Hiểu rõ cách hoạt động, các phương thức xác thực và quyền truy cập của OpenID Connect và OAuth 2.0.
2. **Triển khai hệ thống quản lý danh mục người dùng và ứng dụng:** Xây dựng khả năng quản lý thông tin người dùng và danh mục ứng dụng, bao gồm tạo, cập nhật và xóa thông tin, quản lý quyền truy cập.
3. **Triển khai tính năng Single Sign On (SSO) và Single Sign Out (SSO):** Xây dựng tính năng SSO để người dùng có thể đăng nhập một lần và truy cập vào nhiều ứng dụng mà không cần đăng nhập lại. Triển khai tính năng SSO để người dùng có thể thoát khỏi tất cả các ứng dụng khi đăng xuất khỏi một ứng dụng cụ thể.
4. **Xây dựng tính năng xác thực đa nhân tố:** Tích hợp các yếu tố xác thực bổ sung như mã OTP, xác thực dấu vân tay, hay xác thực khuôn mặt để tăng cường tính bảo mật trong việc xác thực người dùng.

Phạm Vi:

Phạm vi của đồ án sẽ tập trung vào các khía cạnh quan trọng sau đây:

1. **Triển khai hệ thống:** Đồ án sẽ triển khai hệ thống quản lý xác thực và ủy quyền dựa trên OpenID Connect và OAuth 2.0 bằng cách sử dụng các công cụ như WSO2 và Keycloak.
2. **Single Sign On (SSO) và Single Sign Out (SSO):** Đồ án sẽ triển khai tính năng SSO và SSO để cung cấp trải nghiệm người dùng liền mạch khi truy cập nhiều ứng dụng.
3. **Quản lý danh mục người dùng và ứng dụng:** Đồ án sẽ xây dựng khả năng quản lý thông tin người dùng và danh mục ứng dụng, bao gồm việc thêm, sửa, xóa thông tin và quyền truy cập.
4. **Xác thực đa nhân tố:** Đồ án sẽ tích hợp các yếu tố xác thực bổ sung như mã OTP và xác thực dấu vân tay để tăng cường tính bảo mật.

Phạm vi không bao gồm: Đồ án sẽ không đi sâu vào triển khai toàn bộ hệ thống xác thực và ủy quyền cho mọi tình huống. Các khía cạnh như quản lý token, cơ chế refresh token và các yếu tố xác thực tùy chỉnh sẽ được đề cập một cách cơ bản.

1.3 Định hướng giải pháp

Để thực hiện mục tiêu và phạm vi của đồ án, em đề xuất một giải pháp tổng thể để triển khai hệ thống quản lý xác thực và ủy quyền dựa trên giao thức OpenID Connect và OAuth 2.0. Dưới đây là định hướng giải pháp chi tiết:

1. Lựa chọn Công Cụ Triển Khai: Em sẽ lựa chọn một trong những công cụ phổ biến như WSO2 hoặc Keycloak để triển khai hệ thống. Sự lựa chọn này sẽ dựa trên khả năng tích hợp, hiệu suất và tính năng mà công cụ cung cấp.

2. Triển Khai Hệ Thống IAM (Quản lý Danh Mục Người Dùng và Ứng Dụng): Em sẽ bắt đầu bằng việc triển khai hệ thống quản lý danh mục người dùng và danh mục ứng dụng. Điều này bao gồm việc xây dựng giao diện quản lý để thêm, sửa, xóa thông tin người dùng và ứng dụng, cũng như quản lý quyền truy cập.

3. Triển Khai Single Sign On (SSO) và Single Sign Out (SSO): Em sẽ tích hợp tính năng SSO và SSO vào hệ thống. Điều này đòi hỏi việc cấu hình hợp lý và tích hợp với các ứng dụng khác nhau. Việc này sẽ giúp người dùng có trải nghiệm đăng nhập một lần và truy cập nhiều ứng dụng một cách dễ dàng.

4. Xây Dựng Tính Năng Xác Thực Đa Nhân Tố: Em sẽ triển khai tích hợp các yếu tố xác thực bổ sung như mã OTP, xác thực dấu vân tay và xác thực khuôn mặt. Điều này đảm bảo rằng quá trình xác thực người dùng không chỉ dựa trên một yếu tố duy nhất.

5. Kiểm Thử và Đánh Giá Hiệu Quả: Sau khi triển khai, em sẽ tiến hành kiểm thử hệ thống để đảm bảo tính bảo mật và tính ổn định của các tính năng đã triển khai. em cũng sẽ thực hiện đánh giá hiệu quả của hệ thống bằng cách so sánh trước và sau khi triển khai.

6. Tài Liệu Hóa và Báo Cáo Đồ Án: Cuối cùng, em sẽ viết báo cáo đồ án bao gồm các phần mô tả về giải pháp, quá trình triển khai, kết quả kiểm thử và đánh giá hiệu quả, cùng với hướng dẫn sử dụng hệ thống. Tài liệu này sẽ giúp người đọc hiểu rõ về quy trình triển khai và cách sử dụng hệ thống.

Tổng cộng, định hướng giải pháp trên đề xuất một quá trình chi tiết để triển khai hệ thống quản lý xác thực và ủy quyền với các tính năng quan trọng như SSO, quản lý danh mục người dùng và ứng dụng, cũng như xác thực đa nhân tố.

1.4 Bố cục bài báo cáo

Bài báo cáo được chia thành 7 chương như sau:

- **CHƯƠNG 1. GIỚI THIỆU ĐỀ TÀI:** Chương này giới thiệu tổng quan về đề tài, đặt vấn đề cần giải quyết, mục tiêu và phạm vi của đồ án, cùng với định hướng giải pháp được chọn. Cuối chương, được trình bày bố cục chi tiết của bài báo cáo.

- **CHƯƠNG 2. TÌM HIỂU VỀ OPENID CONNECT, OAUTH 2.0:** Chương này đi sâu vào nghiên cứu về OpenID Connect và OAuth 2.0, hai

giao thức quan trọng trong việc xây dựng hệ thống quản lý xác thực và ủy quyền. Nội dung bao gồm xác thực người dùng, hệ thống IAM, JSON Web Token (JWT), OAuth 2.0, OpenID Connect và các cơ chế xác thực đa nhân tố.

- **CHƯƠNG 3. TÌM HIỂU VỀ WSO 2:** Chương này trình bày về công nghệ WSO 2 và giới thiệu về Asgardeo Identity Server, một giải pháp quản lý danh mục và xác thực đa chức năng. Nội dung còn bao gồm WSO2 Identity Server, cách cài đặt và cấu hình OAuth2 bằng WSO2 Identity Server.

- **CHƯƠNG 4. CÔNG NGHỆ SỬ DỤNG:** Chương này giới thiệu các công nghệ cơ bản được sử dụng trong việc xây dựng hệ thống, bao gồm HTML, Javascript, CSS và C#.

- **CHƯƠNG 5. THIẾT KẾ, TRIỂN KHAI VÀ ĐÁNH GIÁ HỆ THỐNG:** Chương này mô tả quá trình thiết kế, triển khai và đánh giá hệ thống quản lý xác thực và ủy quyền. Từ việc xây dựng giao diện trang chủ, tích hợp Single Sign On và Single Sign Out, quản lý danh mục người dùng, quản lý danh mục ứng dụng, xây dựng module xác thực đa nhân tố.

- **CHƯƠNG 6. HƯỚNG DẪN SỬ DỤNG VÀ CÀI ĐẶT:** Chương này cung cấp hướng dẫn về yêu cầu hệ thống, cách cài đặt và sử dụng hệ thống quản lý xác thực và ủy quyền.

- **CHƯƠNG 7. KẾT LUẬN:** Chương này tổng kết kết quả đạt được từ đồ án, nhấn mạnh những thành tựu quan trọng và những học thuật từ quá trình thực hiện.

- **TÀI LIỆU THAM KHẢO:** Chương này liệt kê các tài liệu, nguồn tham khảo mà đồ án dựa vào.

- **PHỤ LỤC:** Chương này chứa các phụ lục, tài liệu bổ sung liên quan đến đồ án.

CHƯƠNG 2. TÌM HIỂU VỀ OPENID CONNECT, OAUTH 2.0

2.1 Xác thực người dùng (Authentication)

Với lượng dữ liệu khổng lồ đang tăng nhanh, người dùng cần phải có cách để bảo vệ dữ liệu của chính họ. Một cách đơn giản để bảo vệ dữ liệu là việc tạo ra mật khẩu hoặc mã PIN, thứ mà định danh người dùng có quyền sử dụng các nguồn dữ liệu thuộc khả năng của họ.

Xác thực (Authentication) người dùng là xem xét xem người dùng có phải đúng người mà họ khai báo hay không. Đó là quá trình xác nhận danh tính của một người dùng hoặc một hệ thống để đảm bảo rằng người dùng hoặc hệ thống đó có quyền truy cập vào tài nguyên hoặc thông tin được yêu cầu. Trong lĩnh vực an ninh mạng, xác thực là một phương thức để đảm bảo rằng người dùng đăng nhập vào hệ thống là người đúng và có quyền truy cập vào các tài nguyên được yêu cầu.

Các phương thức xác thực thông thường bao gồm xác thực bằng tên người dùng và mật khẩu, xác thực bằng giấy chứng nhận số (certificate-based authentication), xác thực bằng vân tay, khuôn mặt, hoặc các phương thức xác thực hai yếu tố (two-factor authentication) để đảm bảo rằng người dùng phải cung cấp ít nhất hai thông tin xác thực khác nhau để đăng nhập. Xác thực là một phần quan trọng trong bảo mật thông tin và đảm bảo tính toàn vẹn của hệ thống.

2.2 Hệ thống IAM

Hệ thống IAM (Identity and Access Management) là một hệ thống quản lý và kiểm soát quyền truy cập của người dùng đến các tài nguyên của một hệ thống thông tin. IAM có vai trò quan trọng trong việc đảm bảo an toàn và bảo mật thông tin trong hệ thống, đồng thời cũng giúp cho việc quản lý người dùng và phân quyền truy cập trở nên dễ dàng và hiệu quả hơn.

Một hệ thống IAM bao gồm các thành phần sau:

- Authentication: xác thực người dùng, đảm bảo rằng người dùng đăng nhập vào hệ thống là người thật, bằng cách yêu cầu nhập tên đăng nhập và mật khẩu hoặc sử dụng các phương thức xác thực khác như OAuth, OpenID Connect, ...
- Authorization: phân quyền truy cập, quyết định người dùng được phép truy cập những tài nguyên nào trong hệ thống và những hành động gì được thực hiện trên tài nguyên đó.
- User Management: quản lý thông tin của người dùng, bao gồm thông tin cá nhân, vai trò và quyền hạn của người dùng.
- Access Control: kiểm soát quyền truy cập, đảm bảo rằng chỉ những người dùng được cấp quyền mới có thể truy cập vào tài nguyên trong hệ thống.

- Audit and Reporting: giám sát và báo cáo hoạt động của người dùng, đảm bảo tính minh bạch và tuân thủ các quy định liên quan đến bảo mật thông tin.

Các công nghệ thường được sử dụng để xây dựng hệ thống IAM bao gồm các công nghệ và giao thức như OAuth, OpenID Connect, SAML, LDAP, ... Hiện nay, có nhiều giải pháp IAM như WSO2 Identity Server, Keycloak, Azure AD, Okta, AWS IAM, Google Identity Platform,... được sử dụng rộng rãi trong các ứng dụng và hệ thống thông tin.

2.3 JWT(JSON Web Token)

Token là một đoạn mã được sinh ra ngẫu nhiên bởi Authorization server khi có yêu cầu được gửi đến từ Client.

Có 2 loại token:

- Access token
- Refresh token

Access token

Là một đoạn mã dùng để xác thực quyền truy cập, cho phép ứng dụng bên thứ 3 có thể truy cập vào những dữ liệu của người dùng trong một phạm vi nhất định mà nó cho phép. Token này được gửi bởi Client như một tham số được truyền vào header trong mỗi request khi cần truy cập đến tài nguyên trong Resource server.

Nếu để lộ mất access token thì cũng có thể coi như bị lộ password bởi có thể lợi dụng nó để lấy được những tài nguyên mà nó đang bảo vệ. Vì vậy, access token có một thời gian sử dụng nhất định (2 giờ, 2 tháng...) tùy thuộc vào nhu cầu sử dụng cũng như yêu cầu về tính bảo mật. Access token chỉ được sử dụng một lần duy nhất, khi nó hết hiệu lực Client sẽ phải gửi lại yêu cầu đến Authorization server để lấy một mã access token mới.

Refresh token

Được sinh ra bởi Authorization server, cùng lúc với access token nhưng lại khác nhau về chức năng. Refresh token sẽ được gửi đi để lấy về một access token mới khi nó hết hạn, cũng chính vì vậy nó có thời gian hiệu lực lâu hơn access token. Với access token thời gian hiệu lực có thể là 2 giờ thì refresh token có thể lên đến 10 giờ.

Việc có mặt của refresh token giúp cho Client có thể lấy lại được access token mà không cần phải nhận xác thực lại từ phía người dùng. Nếu người dùng đăng xuất, refresh token cũng sẽ bị xóa theo.

JSON Web Token (JWT) là một tiêu chuẩn mở (RFC 7519) nhằm xác minh thông tin an toàn giữa các bên Client-Server dưới dạng JSON object. Thông tin này có thể được xác minh và tin cậy vì nó được ký điện tử - digitally signed. JWT có thể được ký bằng cách sử dụng một secret (với thuật toán HMAC) hoặc cặp public/private key dùng chuẩn RSA hoặc ECDSA.

Dưới đây là các lợi ích của việc sử dụng JWT:

- Ủy quyền - Authorization: Đây là trường hợp nên sử dụng JWT. Khi người dùng đã đăng nhập, mỗi request tiếp theo được gởi từ Client sẽ bao gồm JWT, cho phép người dùng access vào routes, services, and resources được phép với token đó. Single Sign ON là tính năng sử dung JWT rộng rãi hiện nay, vì chi phí thấp và dễ dàng sử dụng trên các domains khác nhau.
- Trao đổi thông tin - Information Exchange: JSON Web Tokens là một cách tốt để truyền thông tin an toàn giữa các bên Client và Server. Vì JWT có thể signed. Ví dụ, sử dụng các cặp public/private key, bạn có thể biết chắc người gửi. Ngoài ra, vì signature được xác định dựa vào header và payload, bạn cũng có thể xác minh rằng nội dung chưa bị giả mạo.

JSON Web Tokens bao gồm 3 phần được phân tách bằng dấu chấm (.):

Header.Payload.Signature

Do đó, JWT thường trông như sau:

xxxxx.yyyyy.zzzzz

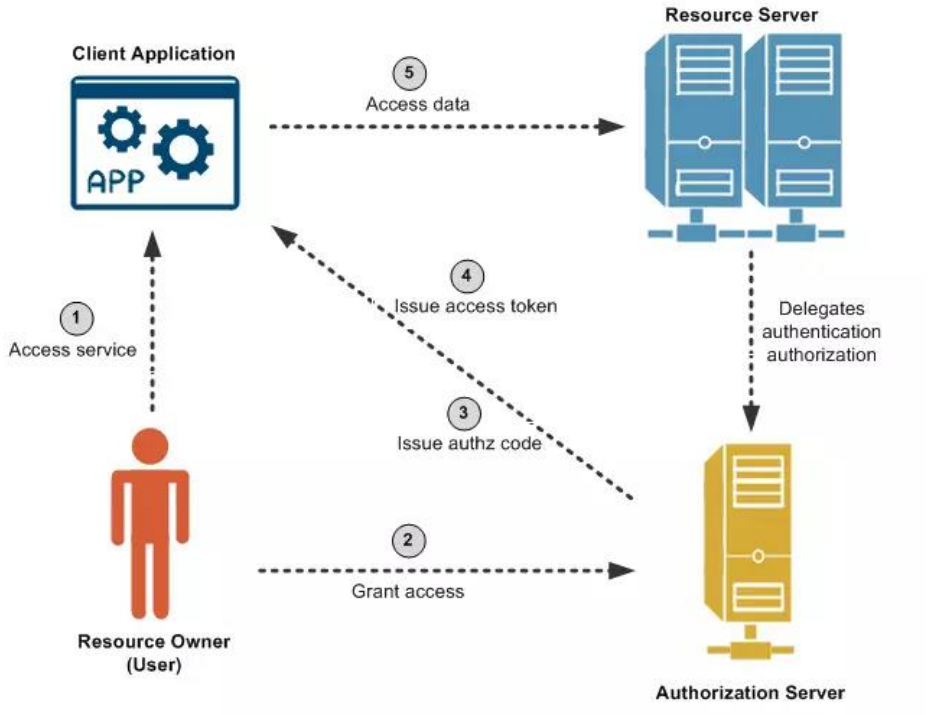
2.4 Oauth 2.0

OAuth (Open Authorization) 2.0 là tiêu chuẩn được thiết kế cho phép website hoặc ứng dụng thay mặt người dùng truy cập vào resources của website hoặc ứng dụng khác. OAuth 2.0 cung cấp quyền truy cập được đồng ý bởi người dùng và hạn chế các hành động của những ứng dụng khác có thể thực hiện mà không cần chia sẻ thông tin đăng nhập. OAuth 2.0 là giao thức ủy quyền, không phải là giao thức xác thực, do đó nó được thiết kế để truy cập vào các tài nguyên như API hoặc dữ liệu người dùng. Vậy nên người dùng phải có tài khoản và quyền truy cập vào tài nguyên, API trước đó.

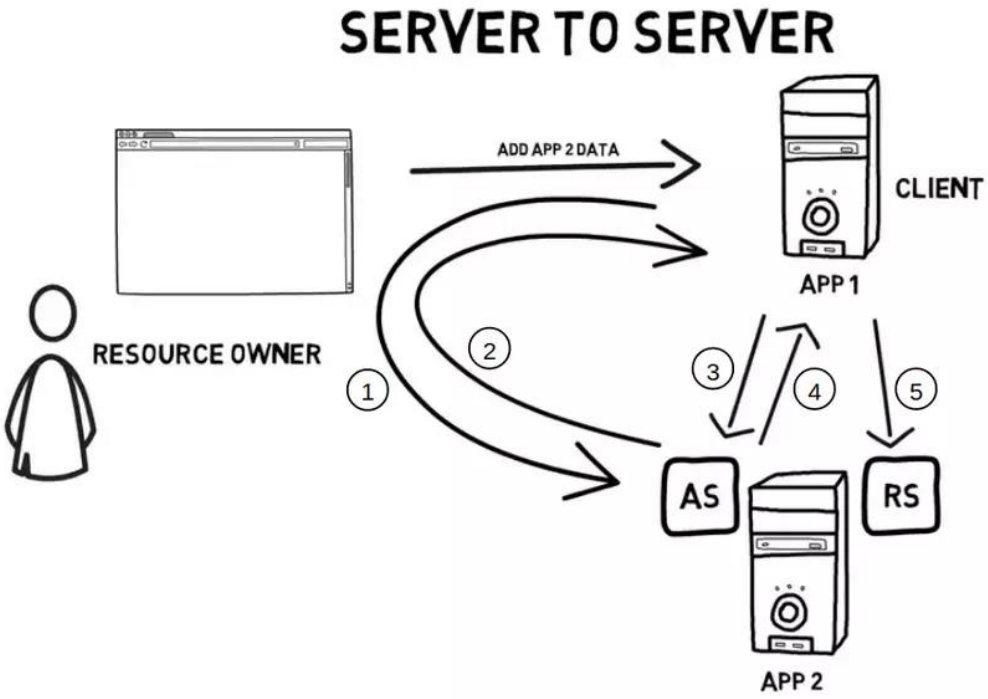
OAuth 2.0 có 4 thành phần quan trọng:

- Client: Client là hệ thống yêu cầu truy cập vào resources được bảo vệ.
- Resource Owner: Người/hệ thống nắm giữ resources được bảo vệ.
- Authorization Server: Server chuyên nhận request từ client và cấp phát access token khi nhận được sự chấp thuận Resource Owner. Authorization Server thường sẽ có hai endpoints
    - Authorization Endpoint: dùng để xác thực, cấp phát authorization code
    - Token endpoint: dùng để xác thực authorization code và trả về access token. Kiểu access token hay được sử dụng phổ biến là JSON web token(JWT).

- Resource Server: Server chứa resources của user, server này sẽ nhận request yêu cầu truy cập resources từ client, sau đó xác thực access token và trả về resources tương ứng.



Hình 1. Cách hoạt động của OAuth 2.0 ở mô hình native client to server



Hình 2. Cách hoạt động của OAuth 2.0 ở mô hình Server to Server

OAuth2 có 4 loại grant type:

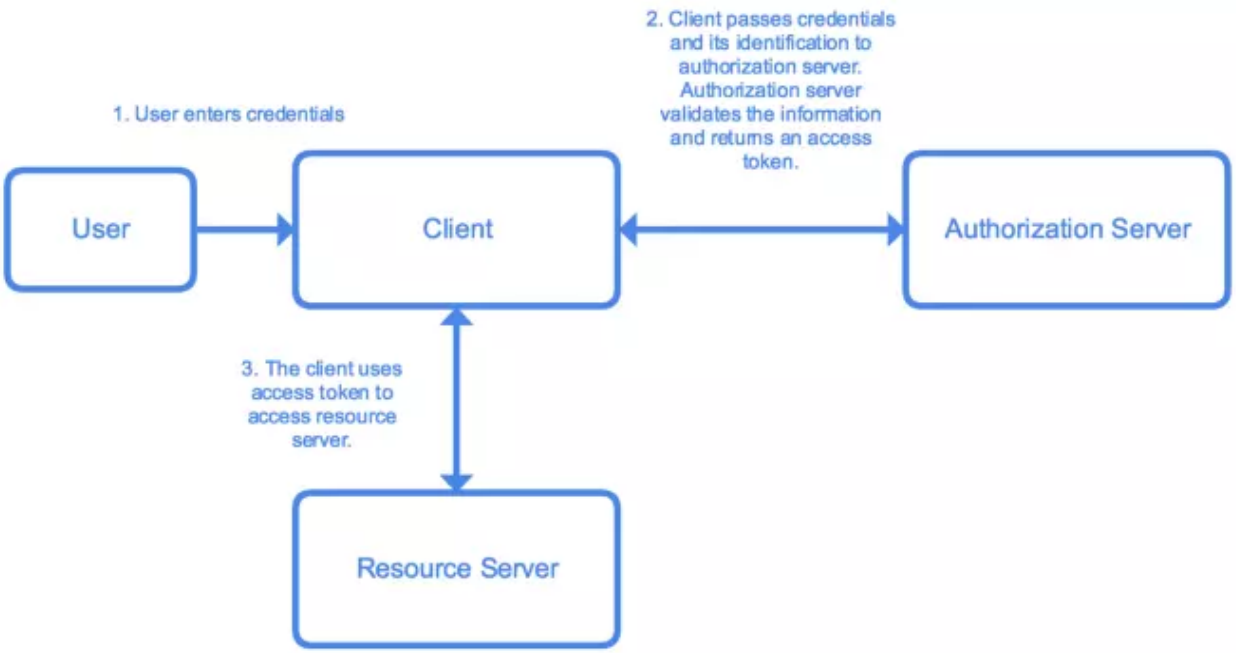
- Resource Owner Password Credentials
- Authorization Code

- Implicit
- Client Credentials

2. Resource Owner Password Credentials

Quy trình bao gồm các bước sau:

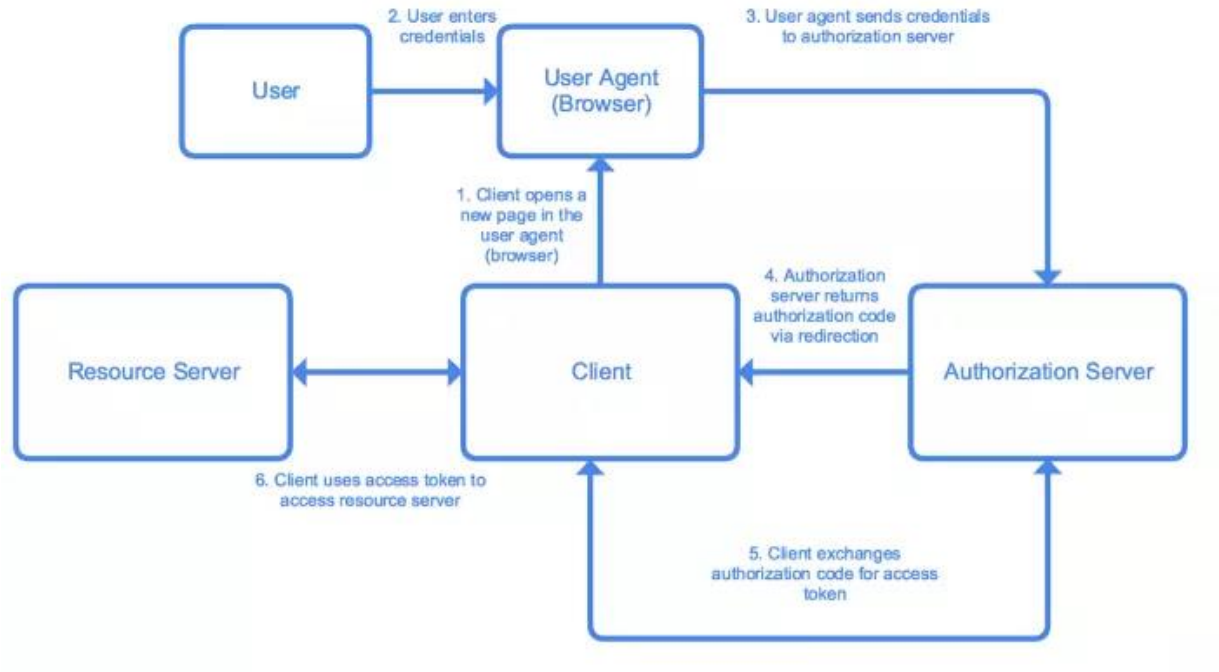
- Ứng dụng đưa ra một form cho phép người dùng nhập thông tin đăng nhập (ví dụ: username/password).
- Ứng dụng gửi thông tin đăng nhập cùng thông tin định danh của mình lên authorization server. Authorizaion server xác thực thông tin, trả lại access token và refresh token (nếu có).
- Ứng dụng sử dụng access token truy cập tài nguyên trên resource server.



3. Authorization Code

Quy trình bao gồm các bước sau:

- Ứng dụng gửi một link đến authorization server cho người dùng để bắt đầu quá trình nhận authorization_code. Link này bao gồm các thông tin cho phép authorization server định danh và response lại cho ứng dụng.
- Người dụng điền thông tin đăng nhập.
- Thông tin đăng nhập được gửi đến authorization server.
- Authorization server xác thực thông tin của đăng nhập và redirects người dùng đến redirect_uri của ứng dụng cùng với một authorization_code.
- Ứng dụng request đến authorization server cùng authorization_code để nhận access token cùng refresh token (nếu có).
- Ứng dụng sử dụng access token truy cập tài nguyên trên resource server.



3. Implicit và Client Credentials

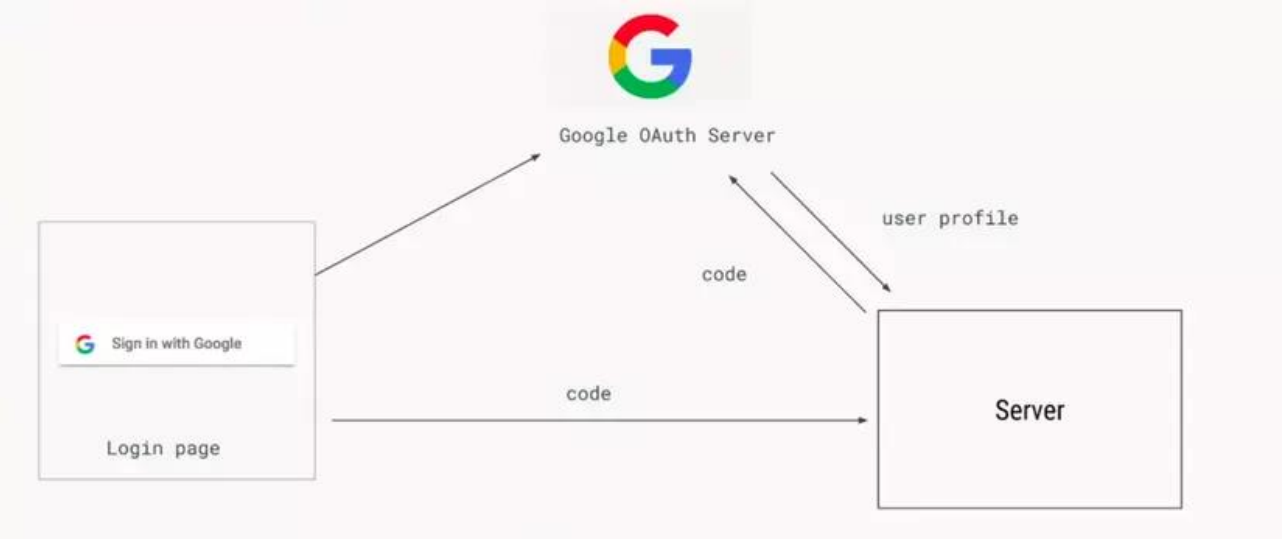
Flow của grant này rất giống với Authorization Code ngoại trừ phần liên quan đến authorization_code. Do lo ngại bảo mật, trong flow này, ứng dụng sẽ không nhận authorization_code từ Authorization server, thay vào đó, Authorization server sẽ trả trực tiếp access token cho ứng dụng. Loại grant này không hỗ trợ refresh_token.

2.5 OpenID Connect

OpenID Connect là một giao thức xác thực (authentication) dựa trên OAuth 2.0. Nó cung cấp cho người dùng một cách để xác minh danh tính của họ cho các ứng dụng web, mà không cần phải chia sẻ tên người dùng và mật khẩu giống như trong các hệ thống xác thực truyền thống.

OpenID Connect sử dụng JSON Web Tokens (JWTs) để cung cấp cho các ứng dụng thông tin xác thực của người dùng. Khi người dùng đăng nhập vào một ứng dụng, OpenID Connect sẽ cung cấp cho ứng dụng một mã truy cập (access token), chứa thông tin xác thực của người dùng dưới dạng JWT. Ứng dụng sẽ sử dụng mã truy cập này để truy cập vào các tài nguyên của người dùng trên các dịch vụ khác, mà không cần phải yêu cầu người dùng đăng nhập lại.

OpenID Connect cung cấp cho các nhà phát triển các cơ chế bảo mật mạnh mẽ để đảm bảo rằng các thông tin xác thực của người dùng được bảo vệ an toàn. Nó cũng cho phép các ứng dụng cung cấp một trải nghiệm người dùng tốt hơn, bằng cách cho phép người dùng đăng nhập một lần và truy cập vào nhiều ứng dụng khác nhau mà không cần phải đăng nhập lại.



1. Khi end-user click vào sign-in button trên trang web hoặc ứng dụng của bạn, browser/ứng dụng sẽ redirect end-user tới OpenID Provider(trang Google OAuth server)
2. OpenID Provider tiến hành xác thực user.
3. Sau khi xác thực thành công. OpenID Provider(Google OAuth Server) sẽ gửi code dùng một lần lại browser thông qua redirect url
4. Mã code mà browser nhận sẽ được chia sẻ tạm thời cho server
5. Server gửi mã code đó tới Google OAuth Server. Sau đó server có thể truy cập vào thông tin profile từ Google OAuth Server

2.6 Các cơ chế xác thực đa nhân tố

Một nhân tố thực chất là một kiểu xác thực. Khi tuyên bố danh tính của ai đó cần cung cấp thông tin hoặc bằng chứng để chứng tỏ đúng là thực thể với

danh tính đó. Nhân tố có thể là mật khẩu hoặc cũng có thể là một thẻ tín dụng ATM.

- Nhân tố thứ nhất: Mật khẩu, số nhận diện cá nhân (PIN). Tất nhiên phải lựa chọn mật khẩu hay số PIN sao cho khó đoán được đối với các thực thể khác.
- Nhân tố thứ hai: Chọn một vật mà chỉ thực thể hợp pháp mới có, thường mang theo mình và không thể nhân bản, ví dụ như thẻ thông minh.
- Nhân tố thứ ba: Đặc tính sinh trắc của người dùng, gắn liền với bản thân người dùng. Đó là vân tay, võng mạc mắt, giọng nói hay khuôn mặt.
- Nhân tố thứ tư: Vị trí của người dùng được xác định chính xác không nhầm lẫn. Đối với máy tính đó chính là địa chỉ IP.
- Nhân tố thứ năm: Nhân tố này ít được sử dụng và ít người biết đến. Đó là quan sát các hành động của người dùng như: Các cử động và tiếp xúc, ví dụ mật khẩu hình vẽ.

CHƯƠNG 3. TÌM HIỂU VỀ WSO 2

3.1 WSO2

WSO2 là một công ty công nghệ phần mềm cung cấp các giải pháp tích hợp doanh nghiệp (Enterprise Integration Solutions) và các dịch vụ đám mây (Cloud Services) cho các doanh nghiệp. WSO2 cũng cung cấp nền tảng phát triển ứng dụng (Application Development Platform) để giúp các nhà phát triển xây dựng các ứng dụng theo mô hình đám mây và hỗ trợ các chuẩn mở như Apache, Java và OSGi. Công ty này có trụ sở tại Sri Lanka và các văn phòng tại Mỹ, Anh, Đức, Ấn Độ và Úc.

3.2 Asgardeo

Asgardeo là một nền tảng quản lý đăng nhập và quản lý danh tính (Identity and Access Management platform) được xây dựng trên nền tảng mã nguồn mở WSO2 Identity Server. Asgardeo cung cấp các giải pháp quản lý đăng nhập, quản lý danh tính và các giải pháp bảo mật cho các doanh nghiệp và tổ chức. Nó cung cấp các tính năng như đăng nhập đơn giản, quản lý danh tính, ủy quyền và phân quyền, xác thực đa yếu tố và giải pháp bảo mật thông tin cá nhân (Personal Data Protection) để giúp các tổ chức bảo vệ thông tin của khách hàng và người dùng. Asgardeo là một sản phẩm của công ty WSO2.

3.3 WSO2 Identity Server

Trong đồ án này, em định hướng sử dụng WSO2 Identity Server để triển khai hệ thống quản lý xác thực và ủy quyền dựa trên giao thức OpenID Connect và OAuth 2.0. WSO2 Identity Server là một giải pháp quản lý danh mục và xác thực mạnh mẽ, cung cấp khả năng xác thực, ủy quyền và quản lý danh mục người dùng cũng như ứng dụng.

Ưu điểm của việc sử dụng WSO2 Identity Server:

1. **Hỗ trợ đầy đủ OpenID Connect và OAuth 2.0:** WSO2 Identity Server hỗ trợ đầy đủ các giao thức quan trọng cho việc xây dựng hệ thống xác thực và ủy quyền an toàn và linh hoạt.
2. **Tích hợp dễ dàng:** WSO2 Identity Server cho phép tích hợp dễ dàng với các ứng dụng và dịch vụ khác thông qua API và tương thích với nhiều ngôn ngữ lập trình và khung làm việc.
3. **Quản lý danh mục người dùng và ứng dụng:** WSO2 Identity Server cung cấp khả năng quản lý thông tin người dùng và ứng dụng một cách hiệu quả và an toàn.
4. **Single Sign On (SSO) và Single Sign Out (SSO):** WSO2 Identity Server hỗ trợ tính năng SSO và SSO, giúp người dùng có trải nghiệm liền mạch khi truy cập vào nhiều ứng dụng.

5. **Xác thực đa nhân tố:** WSO2 Identity Server cho phép tích hợp các yếu tố xác thực bổ sung như mã OTP, xác thực dấu vân tay và xác thực khuôn mặt.

Phạm vi sử dụng WSO2 Identity Server trong đồ án:

Em sẽ triển khai hệ thống quản lý xác thực và ủy quyền bằng cách sử dụng WSO2 Identity Server. Cụ thể, chúng tôi sẽ thực hiện các bước sau:

1. **Triển khai WSO2 Identity Server:** Cài đặt và triển khai WSO2 Identity Server trên môi trường phát triển.
2. **Quản lý Danh Mục Người Dùng và Ứng Dụng:** Xây dựng khả năng quản lý thông tin người dùng và danh mục ứng dụng bằng cách sử dụng tính năng có sẵn của WSO2 Identity Server.
3. **Triển khai Single Sign On (SSO) và Single Sign Out (SSO):** Cấu hình tính năng SSO và SSO để người dùng có trải nghiệm đăng nhập và đăng xuất thuận tiện.
4. **Xây Dựng Tính Năng Xác Thực Đa Nhân Tố:** Tích hợp các yếu tố xác thực bổ sung vào WSO2 Identity Server để cung cấp tính năng xác thực đa nhân tố.

3.4 Cài đặt WSO2 Identity Server

Sau đây là các bước cơ bản để cài đặt WSO2 Identity Server trên hệ điều hành Window:

1. Tải xuống phiên bản phù hợp của WSO2 Identity Server từ trang web chính thức của WSO2.
2. Giải nén tệp tin tải về vào thư mục mong muốn.
3. Mở Terminal và di chuyển đến thư mục chứa WSO2 Identity Server.
4. Chạy lệnh "wso2server.bat" để khởi động WSO2 Identity Server.
5. Nếu WSO2 Identity Server khởi động thành công, bạn có thể truy cập vào giao diện quản trị trên trình duyệt bằng cách nhập địa chỉ IP của máy chủ cùng với cổng 9443 (ví dụ: https://192.168.0.100:9443) và đăng nhập với tên người dùng và mật khẩu mặc định là admin/admin.

Lưu ý: Bạn cần cài đặt Java và thiết lập biến môi trường JAVA_HOME trước khi cài đặt WSO2 Identity Server.

3.5 Cấu hình Oauth2 bằng WSO2 Identity Server

Để cấu hình OAuth trong WSO2 Identity Server, bạn có thể làm theo các bước sau:

1. Đăng nhập vào giao diện quản trị của WSO2 Identity Server bằng tài khoản quản trị.

2. Tạo một ứng dụng trong WSO2 Identity Server. Điều này sẽ tạo một Client ID và Client Secret để sử dụng cho quá trình xác thực OAuth. Bạn có thể tạo ứng dụng bằng cách đi đến "Applications" -> "Add" và nhập các thông tin cần thiết.
3. Cấu hình OAuth trong WSO2 Identity Server bằng cách chọn "OAuth2/OpenID Connect Configuration" từ menu bên trái và cấu hình các thông số như sau:
    - OAuth2/OIDC Enabled: Bật OAuth2/OIDC lên.
    - Application Callback URL: Địa chỉ URL để ứng dụng của bạn nhận phản hồi từ OAuth2/OIDC.
    - Allowed Grant Types: Chọn các loại phép cấp quyền (grant types) được phép sử dụng trong ứng dụng của bạn.
    - Token Issuer: Chọn "Internal" hoặc "External" để cấu hình trình phát Token.
    - OAuth2/OIDC Scopes: Chọn các phạm vi OAuth2/OIDC bạn muốn sử dụng trong ứng dụng của bạn.
4. Lưu cấu hình của bạn và khởi động lại WSO2 Identity Server.

Sau khi hoàn tất các bước trên, bạn có thể sử dụng OAuth2/OIDC để xác thực trong ứng dụng của mình bằng cách yêu cầu mã truy cập (access token) từ WSO2 Identity Server. Với mã truy cập này, ứng dụng của bạn có thể truy cập các tài nguyên được bảo vệ thông qua API hoặc các dịch vụ khác.

CHƯƠNG 4. CÔNG NGHỆ SỬ DỤNG

4.1 HTML

HTML, HyperText Markup Language, cung cấp cấu trúc nội dung và ý nghĩa bằng cách xác định nội dung đó. Ví dụ như tiêu đề, đoạn văn hoặc hình ảnh… Các lợi ích chính của việc sử dụng HTML:

1. Nguồn tài nguyên hỗ trợ lớn, được sử dụng rộng rãi với rất nhiều nguồn tài nguyên cùng một cộng đồng sử dụng vô cùng lớn.

2. Hoạt động mượt mà trên phần lớn các trình duyệt phổ biến hiện nay.

3. Cách sử dụng dễ dàng.

4. Mã nguồn mở và hoàn toàn miễn phí.

5. Là một chuẩn web do W3C vận hành.

6. Dễ dàng tích hợp với nhiều loại ngôn ngữ như PHP, Node.js …

4.2 Javascript

JavaScript là một ngôn ngữ lập trình web rất phổ biến ngày nay. JavaScript được tích hợp đồng thời nhúng vào HTML để hỗ trợ cho website trở nên sống động hơn. Chúng cũng đóng vai trò tương tự như một phần của website, cho phép Client-side Script từ người dùng tương tự máy chủ (Nodejs) để tạo ra những website động. Một số ưu điểm nổi bật của ngôn ngữ lập trình JavaScript như sau:

1. Chương trình và code rất dễ đọc.

2. Có thể hoạt động ở trên nhiều nền tảng và các trình duyệt web khác nhau.

3. Là loại ngôn ngữ lập trình nhẹ và nhanh hơn nhiều so với các ngôn ngữ lập trình khác.

4. Giúp cho trang web có sự tương tác.

5. Giao diện phong phú với nhiều thành phần.

6. Giúp thao tác với người dùng phía Client và tách biệt giữa các Client với nhau

4.3 CSS

CSS, Cascading Style Sheets, là một loại ngôn ngữ lập trình được sử dụng phổ biến để có thể tìm và thực hiện định dạng lại cho những phần tử được tạo ra bởi các ngôn ngữ đánh dấu. Ví dụ như phông chữ, cỡ chữ, căn lề hoặc màu sắc… Các lợi ích chính của việc sử dụng CSS:

1. Giúp thực hiện định kiểu mọi thứ mình muốn lên một file khác.

2. Giúp ta không cần thực hiện lặp lại các mô tả cho từng thành phần. Từ đó, ta có thể tiết kiệm được tối đa thời gian làm việc, làm code ngắn lại giúp kiểm soát dễ dàng hơn các lỗi không đáng có.

3. Giúp người dùng nhiều styles trên một trang web HTML nên khả năng điều chỉnh trang trở nên vô hạn.

4. Mã nguồn của trang web sẽ được tổ chức gọn dàng hơn, trật tự hơn, nội dung trang web sẽ được tách bạch hơn trong việc định dạng hiển thị.

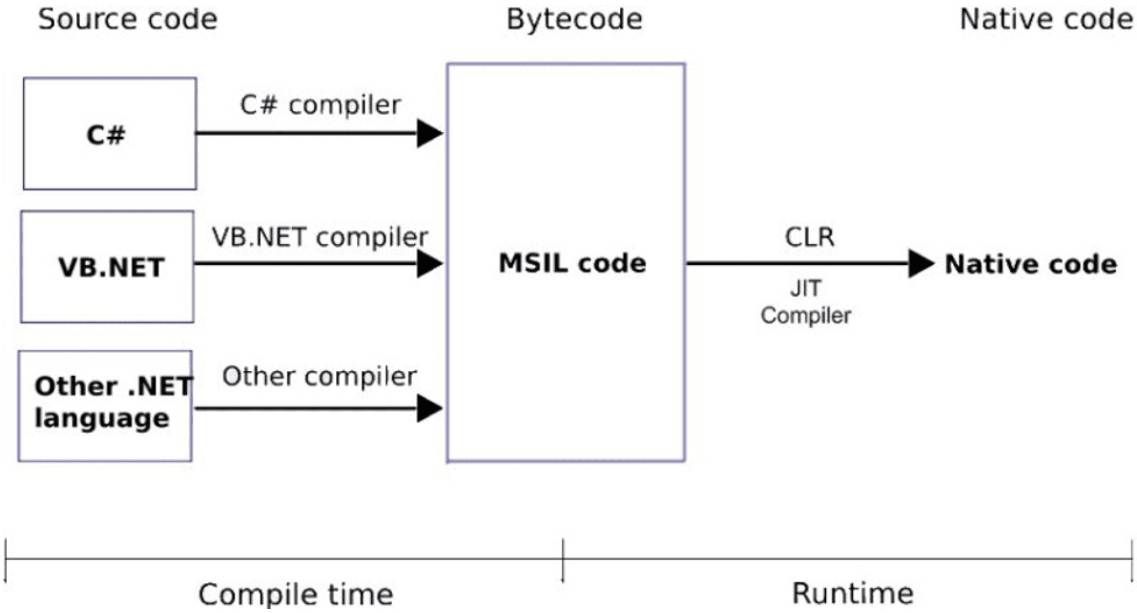
5. CSS tạo ra nhiều kiểu dáng nên có thể được áp dụng với nhiều trang web. Từ đó giảm tránh việc lặp lại các định dạng của các trang web giống nhau

4.4 C#

C# (hay C sharp) là một ngôn ngữ lập trình đơn giản, được phát triển bởi đội ngũ kỹ sư của Microsoft vào năm 2000. C# là ngôn ngữ lập trình hiện đại, hướng đối tượng và được xây dựng trên nền tảng của hai ngôn ngữ mạnh nhất là C++ và Java.

Trong các ứng dụng Windows truyền thống, mã nguồn chương trình được biên dịch trực tiếp thành mã thực thi của hệ điều hành. Trong các ứng dụng sử dụng .NET Framework, mã nguồn chương trình (C#, VB.NET) được biên dịch thành mã ngôn ngữ trung gian MSIL (Microsoft intermediate language). Sau đó mã này được biên dịch bởi Common Language Runtime (CLR) để trở thành mã thực thi của hệ điều hành.

Hình bên dưới thể hiện quá trình chuyển đổi MSIL code thành native code.

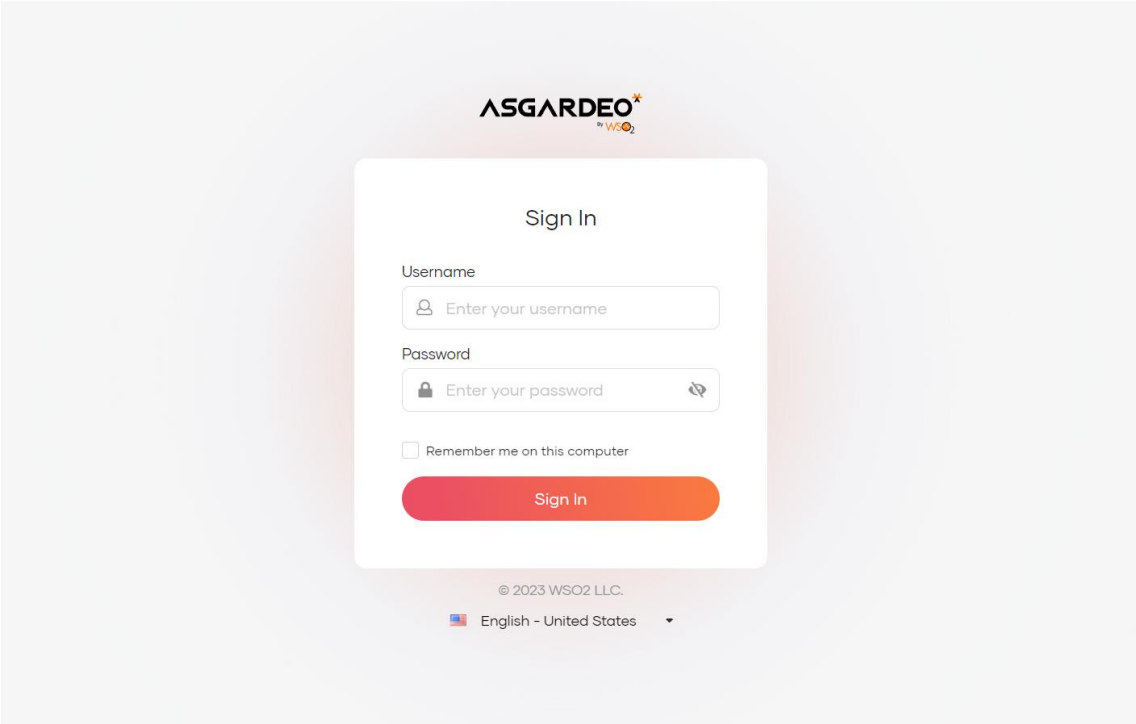


C# với sự hỗ trợ mạnh mẽ của .NET Framework giúp cho việc tạo một ứng dụng Windows Forms hay WPF (Windows Presentation Foundation), phát triển game, ứng dụng Web, ứng dụng Mobile trở nên rất dễ dàng.

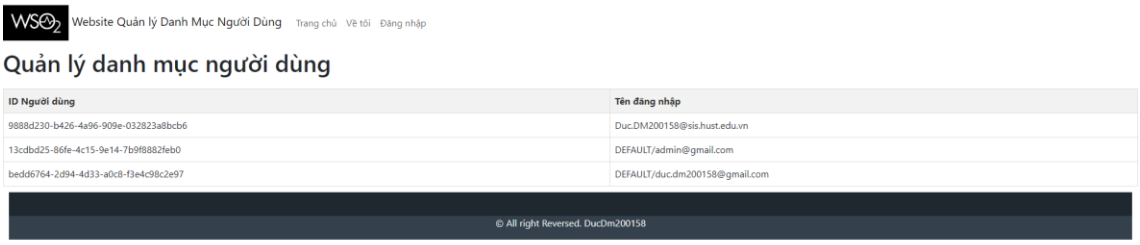
CHƯƠNG 5. THIẾT KẾ, TRIỂN KHAI VÀ ĐÁNH GIÁ HỆ THỐNG

5.1 Xây dựng giao diện trang chủ

5.2 Xây dựng Module đăng nhập tích hợp Single Sign On, Single Sign Out

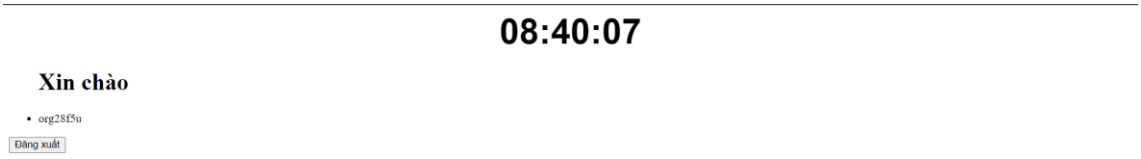


5.3 Xây dựng Module quản lý danh mục người dùng



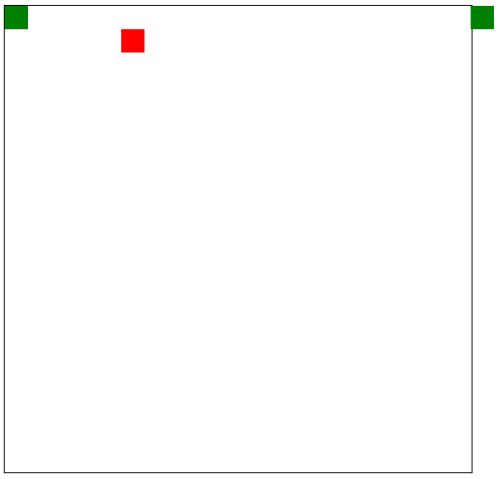
5.4 Xây dựng Module quản lý danh mục ứng dụng

5.4.1 Xây dựng ứng dụng đếm thời gian



5.4.2 Xây dựng ứng dụng rắn săn mồi

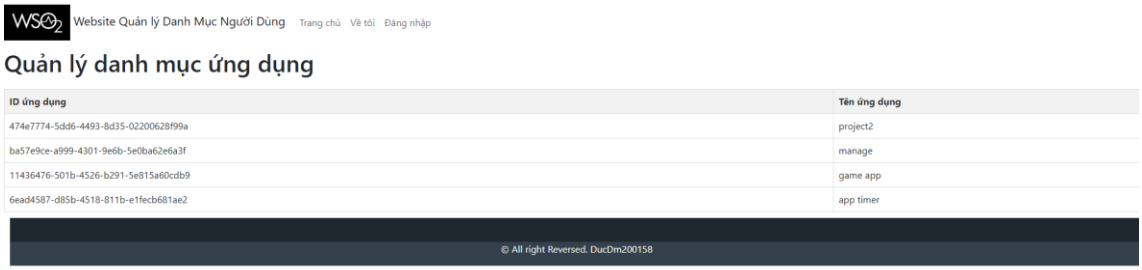
Snake Game



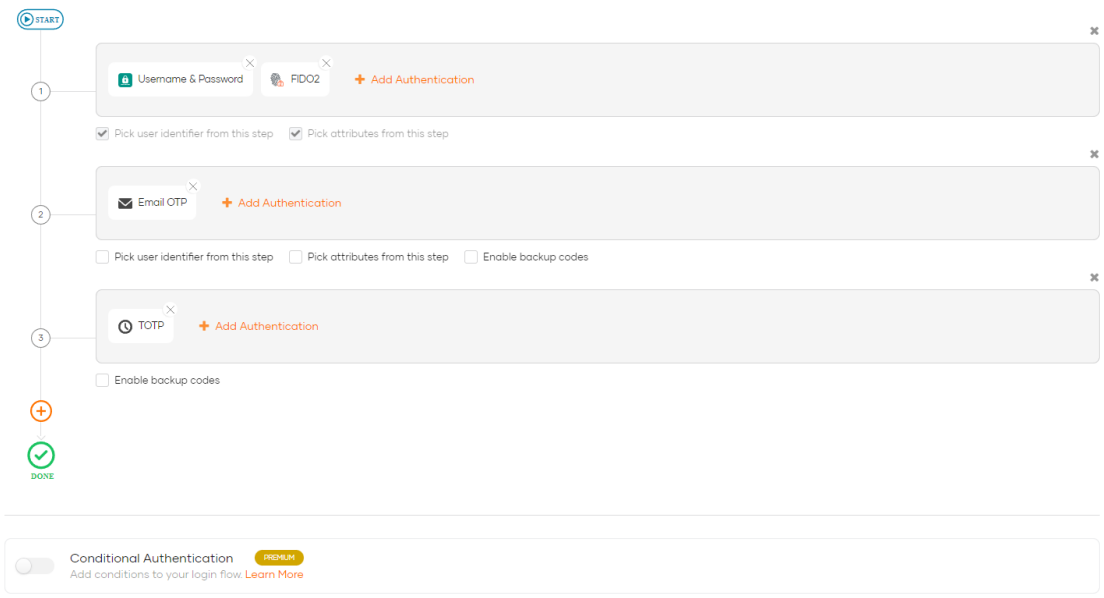
- duc.dm200158@gmail.com

Đăng xuất

5.4.3 Xây dựng module quản lý danh mục ứng dụng



5.5 Xây dựng Module xác thực đa nhân tố



CHƯƠNG 6. HƯỚNG DẪN SỬ DỤNG VÀ CÀI ĐẶT

6.1 Yêu cầu hệ thống

Yêu cầu phần cứng
- CPU: 1.1 GHz trở lên;
- Bộ nhớ trong (RAM): tối thiểu 2 GB;

Yêu cầu phần mềm
- Hệ điều hành: Windows 7 trở lên;

6.2 Hướng dẫn cài đặt

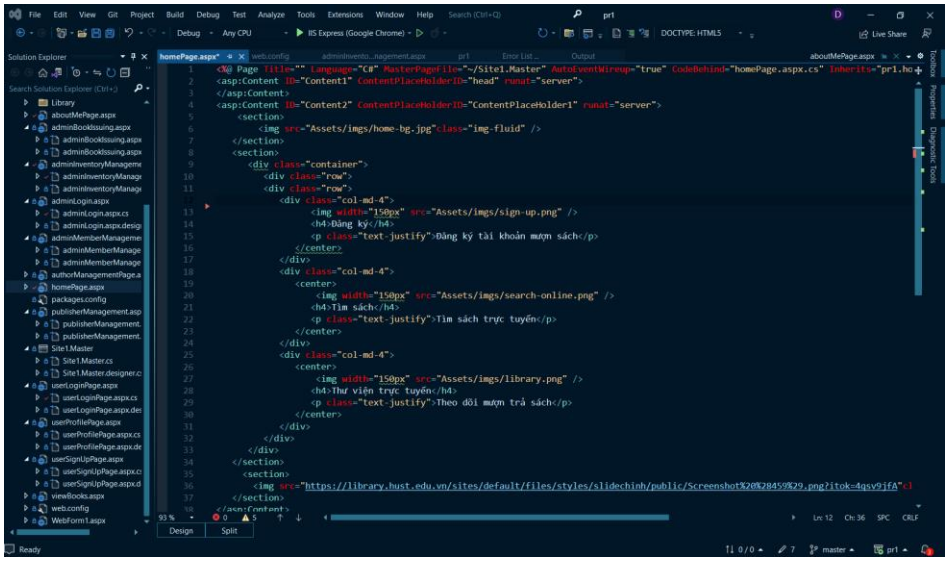
- Truy cập vào link github

  https://github.com/minhducdo050702/project2.git để clone về .

- Tải Visual Studio (https://visualstudio.microsoft.com)

6.3 Hướng dẫn sử dụng

Tại cửa sổ Visual Studio Code chọn folder chứa Project đã clone, mở file homePage.aspx như trong hình. Chọn nút "Run".



CHƯƠNG 7. KẾT LUẬN

Trong quá trình thực hiện đồ án, em đã nghiên cứu, triển khai và đánh giá hiệu quả của hệ thống quản lý xác thực và ủy quyền dựa trên giao thức OpenID Connect và OAuth 2.0. Việc xây dựng hệ thống này đã mang lại những kết quả quan trọng và đáng giá, cùng với những học thuật và trải nghiệm thực tế quý báu.

Trong phạm vi đề tài, em đã lựa chọn WSO2 Identity Server làm nền tảng triển khai hệ thống. Em đã thành công trong việc triển khai tính năng Single Sign On và Single Sign Out, quản lý danh mục người dùng và ứng dụng, cũng như tích hợp xác thực đa nhân tố. Những tính năng này cùng nhau tạo ra một hệ thống quản lý xác thực và ủy quyền an toàn, linh hoạt và hiệu quả.

Trong quá trình thực hiện đồ án, em đã gặp phải những thách thức và khó khăn, như việc hiểu rõ về các giao thức và tích hợp các tính năng phức tạp. Tuy nhiên, những khó khăn này đã thúc đẩy em phải nỗ lực, tìm hiểu sâu hơn và tìm cách giải quyết, giúp chúng tôi tích luỹ kiến thức và kỹ năng quý báu.

Kết quả đạt được từ đồ án không chỉ là sự hoàn thành một sản phẩm thực tế mà còn là sự tích luỹ kiến thức, kỹ năng và kinh nghiệm quý báu cho chúng tôi trong lĩnh vực quản lý xác thực và ủy quyền. Đồng thời, đồ án cũng mở ra cơ hội để tìm hiểu thêm về các công nghệ mới và thách thức trong bảo mật thông tin và quản lý quyền truy cập.

Em hy vọng rằng đồ án này có thể đóng góp một phần nhỏ trong việc nâng cao hiểu biết về các giao thức quản lý xác thực và ủy quyền, và đưa ra một giải pháp thực tế cho việc xây dựng hệ thống an toàn và hiệu quả.

Trong tương lai, em mong muốn có cơ hội tiếp tục phát triển và mở rộng nghiên cứu về các chủ đề liên quan đến an ninh thông tin và quản lý quyền truy cập.

Xin chân thành cảm ơn thầy Trần Quang Đức đã đồng hành và hỗ trợ em trong suốt quá trình thực hiện đồ án này.

Trân trọng,

Đức,

Đỗ Minh Đức

TÀI LIỆU THAM KHẢO

Baker, M. (2023) 'OAuth2, OpenID Connect and Keycloak', *OAuth2 for Securing Web Applications: Part 2* [Preprint]. doi:10.1007/978-1-4842-9763-6_1.

Home (no date) *Asgardeo Docs*. Available at: https://wso2.com/asgardeo/docs/ (Accessed: 15 August 2023).

Indrasiri, K. (2016) 'Fundamentals of WSO2 ESB', *Beginning WSO2 ESB*, pp. 29–58. doi:10.1007/978-1-4842-2343-7_3.

OAuth 2.0 (no date) *OAuth*. Available at: https://oauth.net/2/ (Accessed: 15 August 2023).

Teravainen, T. (2022) *What is single sign-on (SSO) and how does it work?*, *Security*. Available at: https://www.techtarget.com/searchsecurity/definition/single-sign-on (Accessed: 15 August 2023).

'Types of authentication' (2020) *Hacking Multifactor Authentication*, pp. 59–99. doi:10.1002/9781119672357.ch3.

PHỤ LỤC