

CSCI 370 Final Report

[team name]

[author 1 name]  
[author 2 name]  
[author 3 name]  
[author 4 name]  
[author 5 name]

Revised May 23, 2023

[optional graphic or logo]

CSCI 370 [semester] [year]

Mr./Ms./Dr./Prof. [advisor name]

Table 1: Revision history

|  |  |  |
| --- | --- | --- |
| Revision | Date | Comments |
| New |  |  |
| Rev – 2 |  |  |
| Rev – 3 |  |  |

Table of Contents

[I. Introduction 3](#_Toc135746278)

[II. Functional Requirements 3](#_Toc135746279)

[III. Non-Functional Requirements 3](#_Toc135746280)

[IV. Risks 3](#_Toc135746281)

[V. Definition of Done 3](#_Toc135746282)

[VI. System Architecture 3](#_Toc135746283)

[VII. Software Test and Quality 3](#_Toc135746284)

[VIII. Project Ethical Considerations 3](#_Toc135746285)

[IX. Project Completion Status 3](#_Toc135746286)

[X. Future Work 3](#_Toc135746287)

[XI. Lessons Learned 3](#_Toc135746288)

[XII. Acknowledgments 3](#_Toc135746289)

[XIII. Team Profile 3](#_Toc135746290)

[References 3](#_Toc135746291)

[Appendix A – Key Terms 3](#_Toc135746292)

# I. Introduction

# II. Functional Requirements

# III. Non-Functional Requirements

# IV. Risks

# V. Definition of Done

# VI. System Architecture

There are two main components to our system architecture as discussed before. These are the Service Provider (SP) and the Identity Provider (IdP). These systems are technically independent from each other and are only coupled by the Single Sign On (SSO) protocol we use. The system we have chosen for this is OIDC which is an extension of OAuth 2.0, providing authentication on top of the base protocol. This is not a new design and is commonplace in the current internet ecosystem. Take for example, the Mines suite of services. Before you can access the protected views in Canvas, for example class views, grades, etc., you must first authenticate via the Mines MultiPass system. Here, Canvas is the Service Provider, the Mines login page is the Identity provider, and they use SAML, which is very similar to OIDC, to communicate with each other.

Usually, one would use a well-known social account as an IdP, for example, Facebook, Google, Spotify, etc. However, we want to have fine-grained control over how our IdP behaves to best demonstrate the vulnerability and mitigate it. To properly implement this system, it is vital that we understand the OIDC flow, particularly, we will use the *Authorization Code Flow.* Below is a diagram of the process:

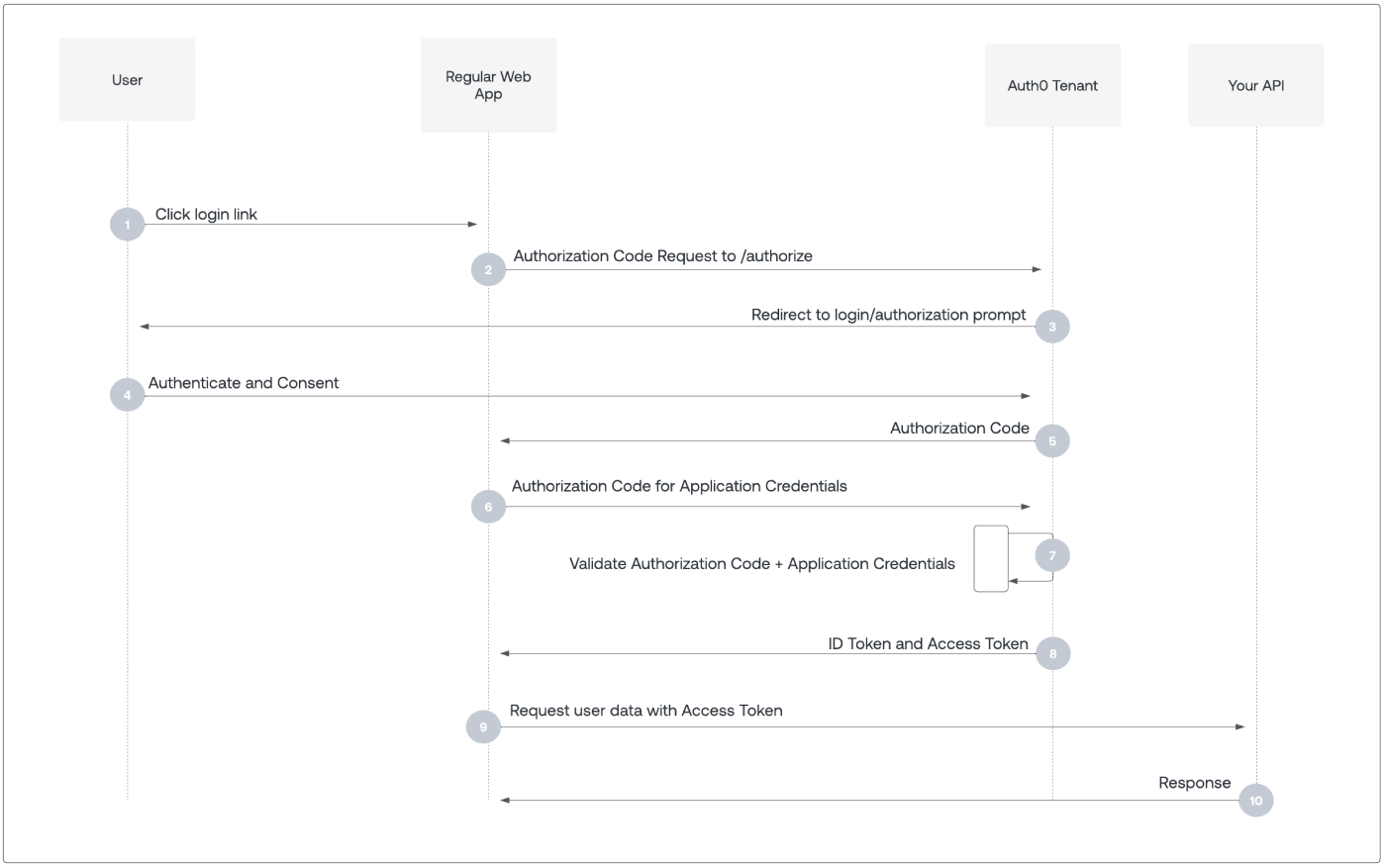


Figure 1 OIDC Authorization Code Flow. Source: [Auth0 by Okta](https://auth0.com/docs/get-started/authentication-and-authorization-flow/authorization-code-flow)

Here, the user begins by trying to log in to the web app which will end up redirecting the user to the IdP for authentication. After authorizing and allowing the web app to use your IdP account, the OAuth process begins. The web app asks for an authorization code which can then be exchanged for an access token to authenticate to the API or service you want to access.

The purpose of our service provider is only to act as the web application in the OIDC process, so it needs to provide the following:

* A login page with a link to sign in via our identity provider.
* A registration process via our identity provider.
* Protected views that cannot be accessed without credentials.
* Maintain a userpool database with client credentials for OIDC.

The last part is critical for mitigating the vulnerability since that is the way we will identify users based on something more than only their email address. The other part of our system, the identity provider, requires the following functionality:

* A login and registration page that can process URL parameters.
* Providing access to OAuth endpoints:
  + */authorize*
  + */token*
  + */revoke*
* Adherence to OIDC requirements.

By tailoring our two providers to these criteria, we can fully demonstrate the vulnerability and then mitigate it. The backends of both of our systems will be handled by Django. It is a framework that fully supports OIDC through libraries, is easily adaptable, and has a fantastic ORM. This brings us to how we store our data. Since the key functionality only requires user data, we will use a traditional relational database system, specifically Postgres. To make our service provider more dynamic, we will use a react webpage to interact with our Django backend. We could do the same for our IdP, but Django templates provide most of the functionality we require and would simplify and expedite our development process. This system can be summarized by the following diagram:

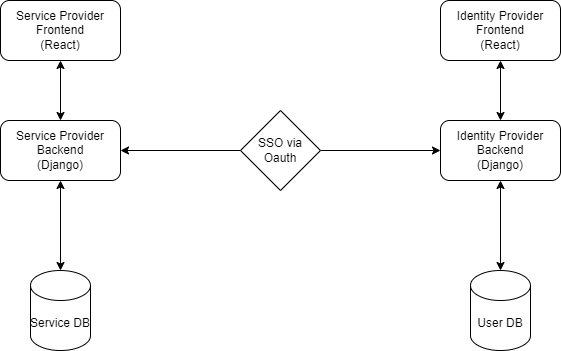


Figure 2 The Architecture of Our System

The arrows here represent direct lines of communication. For example, our frontend has no need to know of our database and will only interact with it through API calls. A key requirement from our client that has not been mentioned so far is that we want to host everything locally, and ideally through containers.

Each component of the service will have its own dedicated container. For example, our SP Postgres database and our IdP Postgres database are separate. For one, this makes sharing extremely simple and spinning up both services is only a matter of composing the containers through a Docker Compose file. Second, it makes publishing simple in case that is the direction the client wants to move forward with the project.

Finally, let’s examine a state diagram of how the vulnerability functions:

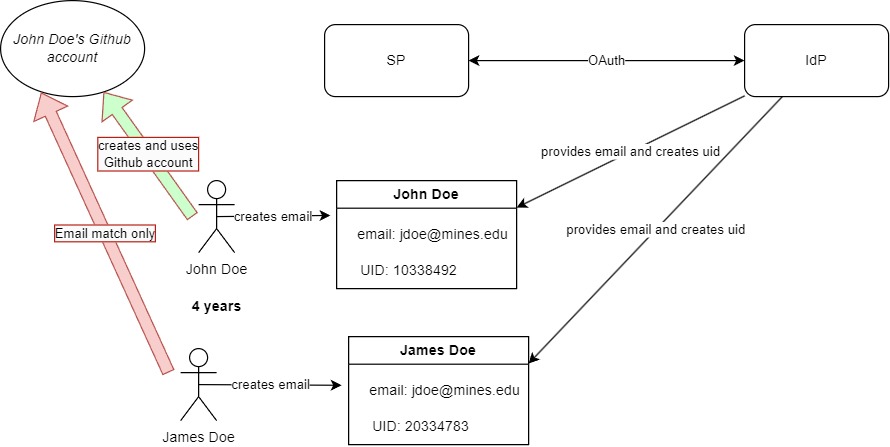


Figure State Diagram Demonstrating Vulnerability

First, a John Doe starts school at the Colorado School of Mines. In this hypothetical, Mines assigns their email address in the format {Initial of First Name}{Last Name}@mines.edu. This might seem strange, but the reality is that many institutions use this scheme or a similar one [1]. In his time at Mines, he creates many accounts, but one of them is a Github account. In this hypothetical, Github uses email addresses as the primary key for a user. Not using the unique ID is an unsafe choice, but many service providers do exactly that [1]. After four strenuous years of University, John Doe graduates. Along comes James Doe and gets assigned the same email as John Doe. For one of his classes, he tries to login to Github and is redirected to the Mines IdP. He signs in and since Github only considers the email address, he is granted access to John’s old account.

# VII. Software Test and Quality

# VIII. Project Ethical Considerations

# IX. Project Completion Status

# X. Future Work

# XI. Lessons Learned

# XII. Acknowledgments

# XIII. Team Profile

# References

[1] G. Liu, X. Gao, and H. Wang, “An investigation of identity-account inconsistency in single sign-on,” in *Proceedings of the Web Conference 2021*, 2021, pp. 105–117.

# Appendix A – Key Terms

Include descriptions of technical terms, abbreviations and acronyms

|  |  |
| --- | --- |
| **Term** | **Definition** |
| *[Insert Term]* | *[Provide definition of the term used in this document.]* |
| *[Insert Term]* | *[Provide definition of the term used in this document.]* |
| *[Insert Term]* | *[Provide definition of the term used in this document.]* |