Project information

Organization name

Python Software Foundation

Sub-organization name

MSS - Mission Support System

Project Idea

mscolab: Implement a SAML 2.0 service provider (SP) into mscolab

Project Abstract

A collaboration server is owned by MSS. Local users can be created for using this server. The existing identity providers are intended to be used by SAML 2.0. A service provider (SP) needs to be implemented for the project on the server site within the existing WSGI application, and authentication needs to be implemented in the QT client application. When a login is initiated on the QT client, a browser is triggered for the login process. The QT client user can authenticate afterwards by exchanging a one-time token. For testing purposes, a local identity provider (IdP) is configured, and a few tests are added.

Detailed description

The statement describes a project that involves setting up a collaboration server owned by MSS. Local users can be created to access the server. The project intends to use existing identity providers for SAML 2.0, which is a protocol used for exchanging authentication and authorization data between parties.

To implement this project, a service provider (SP) needs to be created on the server site within the existing WSGI application. The SP is responsible for validating the identity of the users and allowing them access to the server's resources.

Additionally, authentication needs to be implemented in the QT client application, which is a cross-platform application development framework. When a user initiates a login on the QT client, a browser is triggered for the login process. The user can then authenticate themselves by exchanging a one-time token. This process is designed to ensure the user's credentials are secure while providing a seamless login experience.

For testing purposes, a local identity provider (IdP) is configured. The IdP allows users to authenticate themselves locally without the need for an external authentication provider. A few tests are added to ensure the IdP is working correctly.

Overall, this project aims to create a secure and efficient authentication process for local users to access the collaboration server. By using SAML 2.0 and implementing an SP on the server side, the project ensures that user identity is validated, and access to the server is granted only to authorized users. The use of a one-time token and a local IdP further enhances the security and testing of the authentication process.

Weekly timeline

- This timeline is flexible and is changing according to mentor requirements.

Time Period	Milestone
May 4 - May 8	Project Initiation
May 9 - May 15	Requirement refinement with mentor
May 16 - May 22	Designing the architecture
May 23 - May 28	Creating the base structure for project
May 29 - July 31	Developing the project
May 29 - June 11 *(Week 1,2)*	Setup own IdP and test it with an existing service provider (SP) • To ensure proper functioning of the Service Provider (SP), it is necessary to have an Identity Provider (IdP) under our control. The process can begin by creating our own IdP and testing it with an existing Service Provider from another project. Valuable insights can be gained through this process, which would help ensure similarity of our SP

	implementation to that of the other project. Further tests can be added based on the results obtained to improve the system. ● Obtain the metadata file from the identity provider (IdP) that needs to use for SSO.
June 12 - June 25 *(Week 3,4)*	Configure the MSS collaboration server ● Install a SAML service provider (SP) library on a local server. ● Create an SSL/TLS certificate and key for the server. ● Configure the SP library with the metadata file and SSL/TLS certificate. ● Utilize a template for generating the data within the metadata file owned by the Service Provider. ● Test the SSO integration with the IdP.
June 26 - July 9 *(Week 5,6)*	Implement authentication into the QT client application ● On the QT client a login, login will trigger a browser for the login process. ● If the server successfully authenticates the user, return a one time token to the client application. ● Existing MSColab is an application based on requests and socket io events. In brief, upon successful request-based authentication, a JWT token is issued for event-based communication, and it remains valid until the user logs out. With SAML, the request-based login is replaced. ● Implement appropriate error handling and logout functionality in the client application. Start Documenting ● A gdoc will be used to provide documentation so that mentors are aware of what is required to answer questions. This is a kind of developer documentation, from which a user documentation can be derived later.

July 10 - July 23 *(Week 7,8)* *(July 14 - Midterm evaluation deadline)*	Use an existing identity provider (like keycloak) with SAML 2.0 ● Identify the IdP that can use and obtain their SAML metadata file. ● Configure service provider (SP) to trust the IdP by importing their metadata file. ● Configure SP to send SAML requests to the IdP, specifying the required parameters such as the assertion consumer service URL. ● Test the SAML integration with the IdP by initiating SSO and verifying that the user is correctly authenticated and redirected back to application. ● Once the integration is confirmed to be working, customize the user experience by modifying the login page and any error pages.
July 24 - Aug 6 *(Week 9,10)*	Test the implemented Project ● Verify the project requirements. ● Write functional test cases. ● Conduct functional testing.
Aug 7 - Aug 20	Finalizing project
Aug 7 - Aug 13 *(Week 11)*	Refine and improve features with mentor feedback + additional features
Aug 14 - Aug 20 *(Week 12)*	Finalize documentation ● Complete the current developer and user documentation, ensuring that all necessary information is included and presented in a clear and engaging manner.

Other commitments

Over the next eight months, I will have a combination of college lectures and research work to focus on, particularly with regard to my final year project.