Keycloak實現網頁Single Sign-On的登入機制
Using Keycloak as User federation to implement Single Sign-On login flow

呂威劭
政治大學資訊科學系
neolu2001@gmail.com

廖峻鋒
政治大學資訊科學系
cfliao@nccu.edu.tw

ABSTRACT(摘要)

挑戰：

- 傳統的帳號/密碼存在安全漏洞：如果攻擊者成功破解密碼，整個系統可能會被入侵。
- 處理系統停機和維護變得困難（例如資料庫維護）。

解決方案：

- 引入身份驗證和授權服務（例如 Keycloak）
  - 身份驗證：使用 LDAP（Lightweight Directory Access Protocol）伺服器
  - 授權：使用 Keycloak 作為身份和訪問管理解決方案

好處： Keycloak 作為開源身份提供者，提供單一登入、多因素驗證和集中式使用者管理等功能。 使用者憑證和相關信息得到安全儲存。這不僅提高了安全性，還簡化了使用者管理任務。

結果：

- 在安全事件發生時更迅速的響應
- 提供額外的安全層
- 使整體身份驗證和授權更具擴展性和可維護性

1. INTRODUCTION(介紹內容)

OpenLDAP: 一種儲存使用者資訊的目錄，更適用於組織目錄信息，管理用戶身份和訪問控制。

Keycloak: Keycloak 提供了單一登入 (Single Sign-On, SSO)，由 redhat 開發。

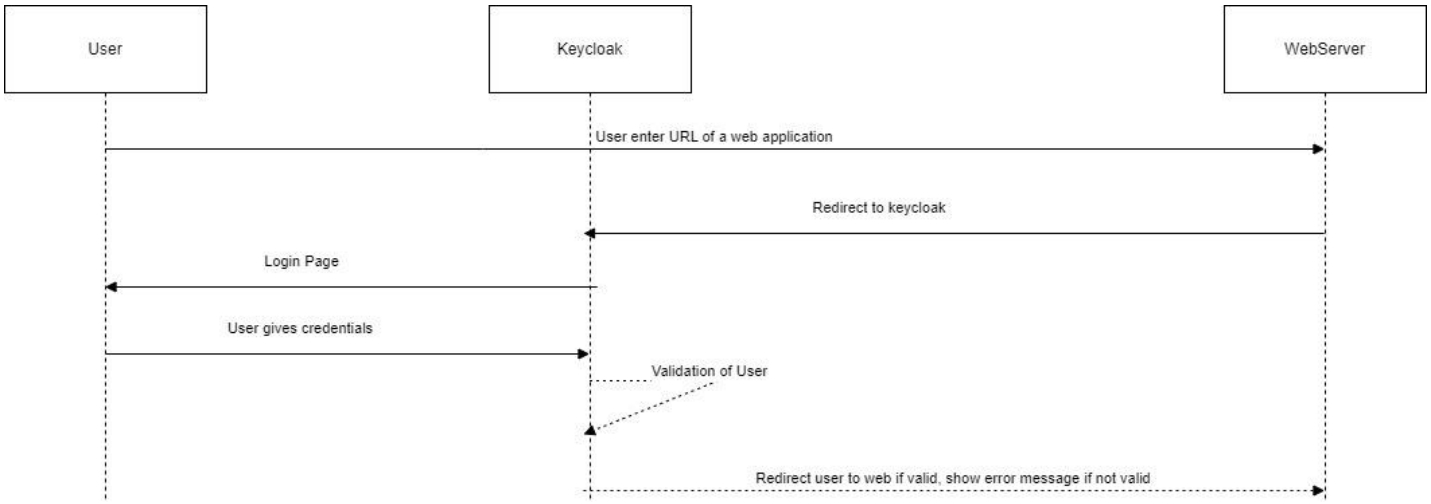
2. RELATED WORK (相關工作)

軟體技術: OpenLDAP, phpLDAPadmin, Keycloak, flask

資安協定:Oauth2, Openidconnect

在 flask 專案中 import flask_oidc 並且將設定檔(.json)寫入，在 login 函式中加入 oidc.require_login 的 decorator。可以導致登入跳轉至 keycloak 登入頁面。

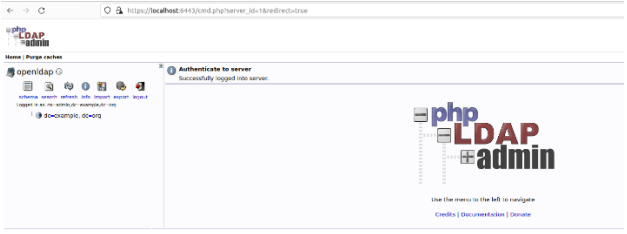
3. RESEARCH METHODS AND PROCEDURES (研究方法及步驟)



圖一、整個應用程式的登入架構

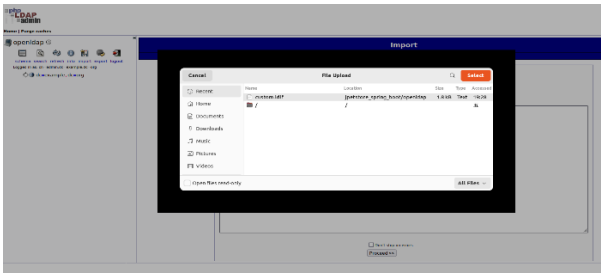
架設 OpenLDAP

use phpldapadmin to manipulate openldap



login into the openldap

click import to import the ldif file(custom.ldif)




after imported

這樣就把我們的 LDAP 架好了

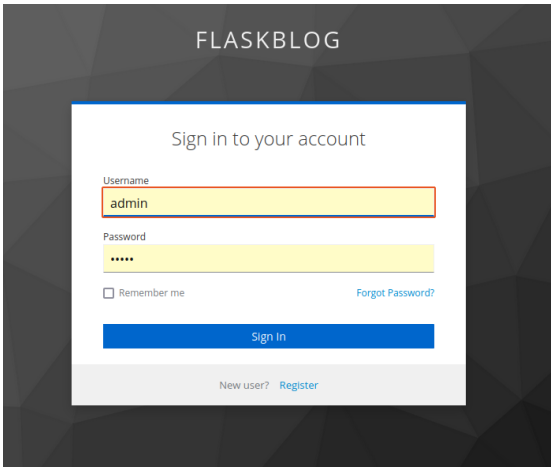
架設 Keycloak

架設時，需要先建置一個 realm，這個 realm 存放我們的登入資訊。接下來要在 realm 中創建 client id 是專門給我們的應用程式所使用，並且在 client id 中要定義使用者的權限(是 user 還是 admin)。要在 user federation 中引入 LDAP server 中的使用者資料。並且引入完成後，要將每一個使用者分配權限。這樣就完成 keycloak 設定。

4.EXPERIMENTAL RESULTS(預期實驗結果)

使用keycloak後，網頁的功能完全運作成功，登入時會跳轉至keycloak的登入頁面。登入後，網頁會顯示登入的使用者資料。並且其他網頁服務如果也鑲嵌keycloak就可以實現SSO的服務。

還沒登入前的網頁



點擊右上角 login 按鈕

登入後會在右上角顯示使用者資訊

5.CONCLUSIONS(結論)

傳統的帳號密碼登入系統，依賴使用者名稱和密碼的驗證方式，面臨著固有的安全風險。為了解決這些問題，我成功實施了一個基於網頁的系統，並採用了 LDAP 和 Keycloak 技術。Keycloak 作為開源身份提供者，與 LDAP 整合，確保了登入數據的安全存儲，顯著提升了系統的整體安全性。這種組合不僅提供了更強大的身份驗證機制，還為使用者管理和系統維護帶來了更簡便的解決方案。在這樣的系統中，我們能更快速地應對安全事件，同時為整個身份驗證和授權過程增加了額外的安全層，使系統更具擴展性和可維護性。

REFERANCE(參考文獻)

https://github.com/puiterwijk/flask-oidc/issues/5

https://blog.twjoin.com/%E7%AD%86%E8%A8%98-openldap-

%E5%BB%BA%E7%BD%AE%E8%88%87%E4%BB%8B%E6%8E%A5-3e16175b6c3c

https://medium.com/@ivangfr/setting-up-openldap-with-keycloak-for-user-federation-82c643b3a0e6