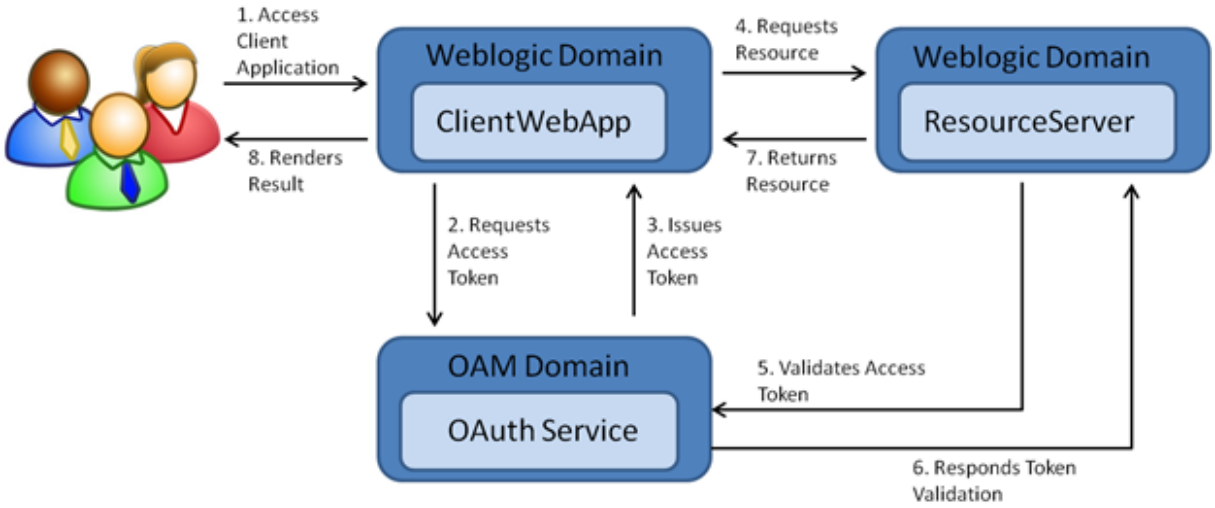
# Delegacja autoryzacji między aplikacjami

Marcel Piłatowski

# Cel Projektu

- Implementacja delegacji autoryzacji, dzięki której jedna aplikacja będzie w stanie ubiegać o dostęp do zasobów innej aplikacji z udziałem serwera autoryzującego
- Pomyślne przeprowadzenie procesu uzyskiwania tokenu i zweryfikowanie, czy odpowiednie zasoby zostały udostępnione
- Analiza i poprawa bezpieczeństwa przeprowadzonego procesu na podstawie bazy artykułów OWASPa




*Schemat przedstawiający infrastrukturę OAuth2.0*

# Założenia

- Klient, jako aplikacja ubiegająca się o token i dostęp do zasobów,
- Serwer autoryzujący, odpowiadający za udzielenie poświadczenia w imienia właściciela zasobu i definiowanie zakresu uprawnień,
- Serwer zasobu, jako aplikacja przechowująca chronione zasoby np. dane użytkowników
- Aplikacja przechowuje dane o wielu użytkownikach, użytkownicy mają dostęp tylko do swoich własnych danych, wyłączając dane upublicznione za zgodą użytkowników np. dane profili publicznych
- Wielu użytkowników aplikacji klienckiej może ubiegać się o token i dostęp do zasobów w tym samym czasie

# Narzędzia

Utworzenie aplikacji webowych:

- Framework Django
- MySQL
- Bootstrap

Implementacja OAuth 2.0:

- biblioteki OAuth dla Pythona

Wdrożenie do symulowania:

- Docker

Lista artykułów OWASPa, dotycząca OAuth2.0:

Testowanie podatności OAutha2.0:

https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/05-Authorization_Testing/05-Testing_for_OAuth_Weaknesses

https://owasp.org/www-pdf-archive/20151215-Top_X_OAuth_2_Hacks-asanso.pdf

Testowanie podatności serwera autoryzującego:
https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/05-Authorization_Testing/05.1-Testing_for_OAuth_Authorization_Server_Weaknesses