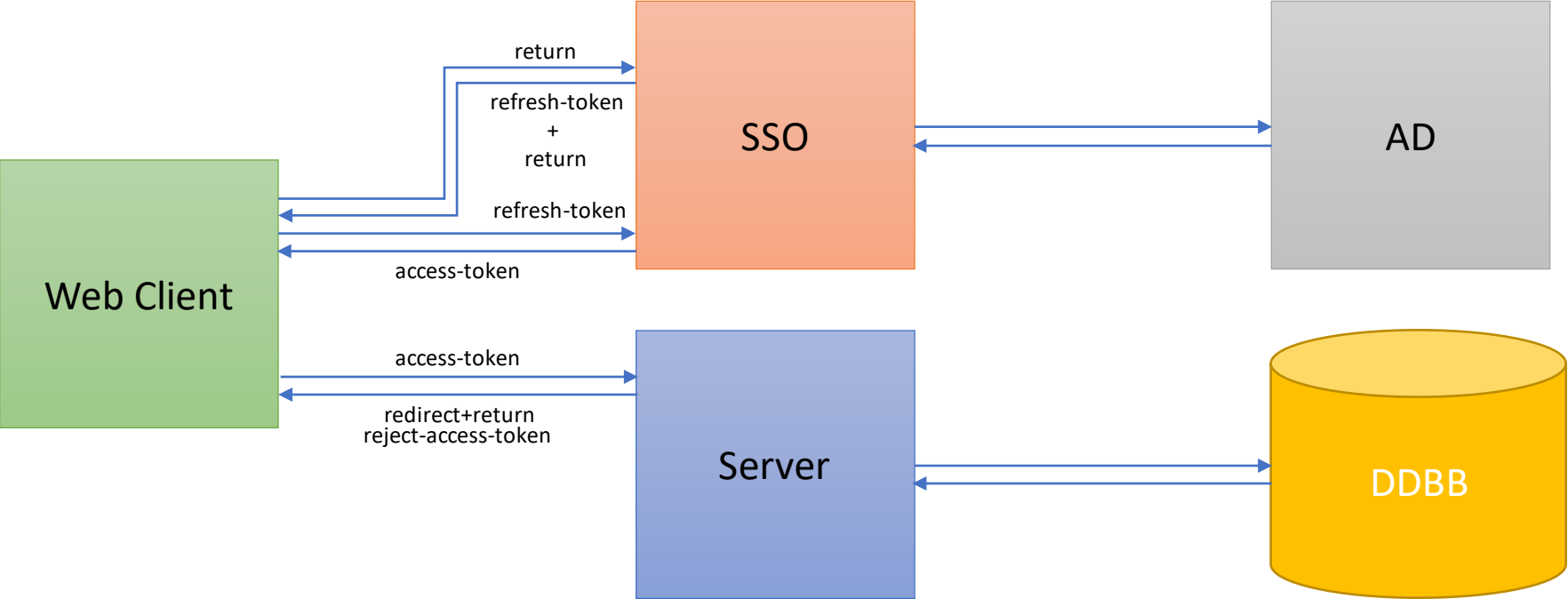


# SSO Flow



# En esta primera sesión

- Threat Model
- Implicaciones
- Conocemos nuestras herramientas:
  - WebGoat
  - Firefox
  - Zap
- Entendiendo los protocolos
- Un ejemplo simple de ataque: 2017 - A2 Broken authentication
- Mejores prácticas:
  - [https://docs.microsoft.com/en-us/previous-versions/ms178194\(v=vs.140\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/ms178194(v=vs.140)?redirectedfrom=MSDN)
  - [https://docs.microsoft.com/en-us/previous-versions/aspnet/zdh19h94\(v=vs.100\)](https://docs.microsoft.com/en-us/previous-versions/aspnet/zdh19h94(v=vs.100)) Antiguo

# Ejemplo práctico

A2 - Broken Authentication

Authentication Bypasses - 2FA Password  
Reset

Recordamos comprobar:

- Cheatsheet
  - ASVS
  - Contramedidas
  - Top 10
- Security Knowledge Framework

# 5. Verificación del control de acceso

# Ejemplo práctico

A5 - Broken Access Control

Missing Function Level Access Control -  
Gathering User Info

## 6. Verificación de entrada maliciosa

# Ejemplo práctico

A1 - Injection

Sql Injection (Intro) - Numeric SQL  
injection