Senparc 盛派®

盛派网络

微信公众号+小程序快速开发

Senparc 盛派®

第15节：OAuth 微信网页授权 - OAuth原理介绍

所需课时：1

延伸参考：《微信开发深度解析》第16章

Senparc 盛派®

学习目标：

1、学习 OAuth 2.0 技术原理。
2、学习微信在 Oauth 2.0 上的实现规则。
3、学习微信后台 OAuth 的设置。
4、延伸学习更多在微信网页安全方面的知识。

Senparc 盛派®

SDK 源代码：
https://github.com/JeffreySu/WeiXinMPSDK

参考 Sample 源代码：
Senparc.Weixin.MP.Sample

BookHelper：
https://book.weixin.senparc.com

课堂案例源代码下载：
https://github.com/JeffreySu/WechatVideoCourse

微信入群加个人微信：SenparcWechat（盛小嗨）
QQ学员群（14群）： 588231256

Senparc 盛派®

1、什么是OAuth?

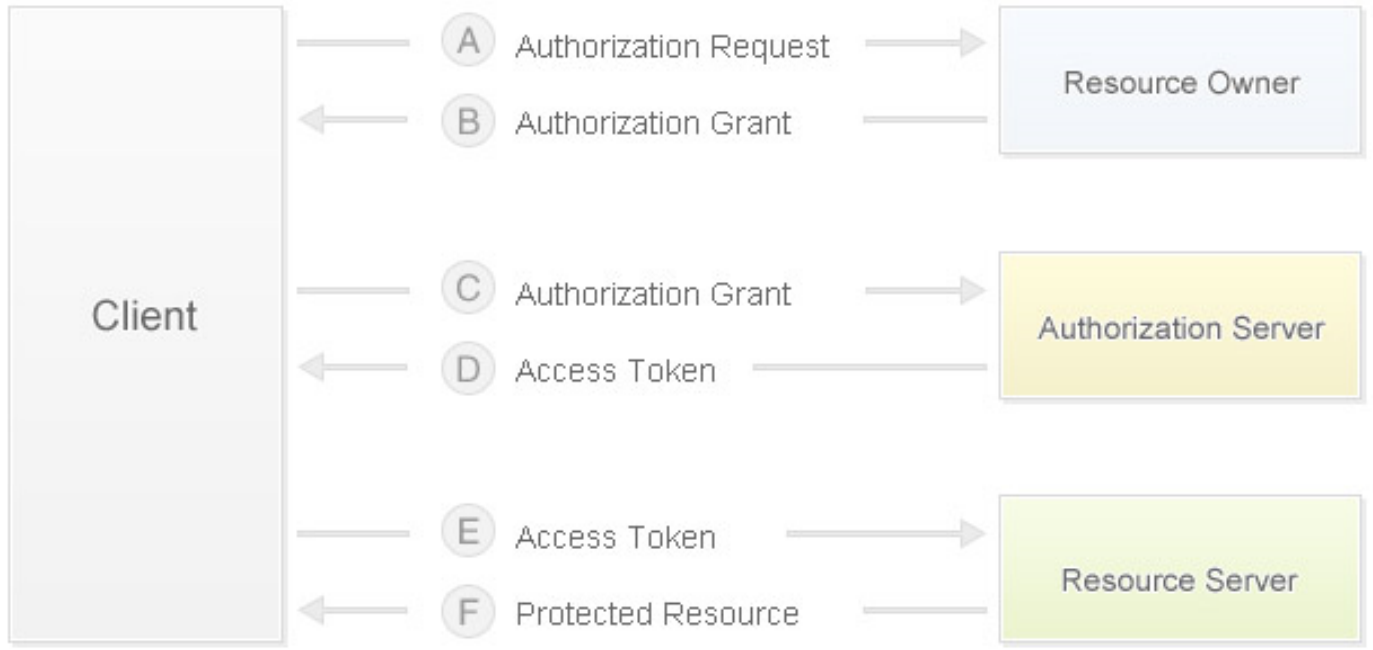
OAUTH 协议为用户资源的授权提供了一个安全的、开放而又简易的标准。与以往的授权方式不同之处是 OAUTH 的授权不会使第三方触及到用户的帐号信息（如用户名与密码），即第三方无需使用用户的用户名与密码就可以申请获得该用户资源的授权，因此 OAUTH 是安全的。oAuth 是 Open Authorization 的简写。

OAUTH 协议为用户资源的授权提供了一个安全的、开放而又简易的标准。同时，任何第三方都可以使用 OAUTH 认证服务，任何服务提供商都可以实现自身的 OAUTH 认证服务，因而 OAUTH 是开放的。

Senparc 盛派®

2、OAuth 2.0 的流程?

OAuth 2.0 的流程



例如：开发者服务器

例如：微信服务器

整个过程进行了 2 次“握手”，最终可以利用授权的 AccessToken 进行一系列的安全请求。相关的过程说明如下：

- A：由客户端（对应**应用服务器**）向服务器（对应**微信服务器**）发出验证请求，请求中一般会携带这些参数：
  - ID 标识，例如微信公众号的 AppId
  - 验证后跳转到的 URL（redirectUrl）
  - 状态参数（可选）
  - 授权作用域 scope（可选）
  - 响应类型（可选）
- B：服务器返回一个 grant 授权标识（微信默认情况下称之为 code），类似于一个一次性的临时字符串密钥。如果在A中提供了 redirectUrl，这里服务器会做一次跳转，带上 grant 和状态参数，访问 redirectUrl。
- C：客户端的 redirectUrl 对应页面，凭借 grant 再次发起请求，这次请求通常会携带一些敏感信息：
  - ID 标识
  - 密码
  - grant 字符串（code）
  - grant 类型（可选，微信中默认为 code）
- D：服务器验证 ID 标识、密码、grant 都正确之后，返回 AccessToken（注意，这里的 AccessToken 和之前通用接口、高级接口介绍的 AccessToken 没有关系，不能交叉使用）
- E：客户端凭借 AccessToken 请求一系列的 API，在此过程中不再会携带 AppId，Secret，grant 等敏感的信息。
- F：服务器返回请求结果。

Senparc 盛派®

3、加强账号/密码安全意识

账号和密码的安全性

1、客户端将密码加密之后再传输到服务器（如MD5）。
2、服务器端使用“加盐”的方式进行混淆加密，严谨明文存储密码！
3、尽量不要使用Cookie储存用户名，尤其是OpenId，更不要在Url中传输OpenId！
4、你必须知道：Session常规情况下也是依赖Cookie才能起作用的，所以不要以为Session和客户端安全无关！
3、HTTPS不能解决所有安全问题！