**1주차 학습내용 정리**

|  |  |
| --- | --- |
| **학습주제** | OAuth |
| **학습정리목차** | |
| 1. OAuth란 무엇인가? 2. OAuth는 왜 필요한가? 3. OAuth의 주요 4가지 객체는 무엇인가? 4. 다른 인증방법과 OAuth의 차이점은 무엇인가? 5. OAuth 용어 정리 6. OAuth의 프로세스는 어떻게 진행되는가?  * 실습 참고사항 | |
| **내용** | |
| ㅁ OAuth란 무엇인가.  OAuth는 인터넷 사용자들이 비밀번호를 제공하지 않고 다른 웹사이트 상의 자신들의 정보에 대해 웹사이트나 애플리케이션의 접근 권한을 부여할 수 있는 공통적인 수단으로서 사용되는, 접근 위임을 위한 개방형 표준이다. 아마존이나 구글 등의 기업 계정을 가지고 있으면, 사용자들이 타사 어플리케이션이나 웹사이트 계정에 관한 정보를 공유할 수 있다. OAuth는 서버와 클라이언트 사이에 인증을 완료하면 서버는 권한부여의 결과로써 access token을 전송한다. 클라이언트는 access token을 이용해서 접근 및 서비스를 요청할 수 있다. 서버는 access token기반으로 서비스와 권한을 확인하여 접근을 허용할지 말지를 결정하고, 결과 데이터를 클라이언트에게 보내준다. 서버는 access token을 기반으로 클라이언트를 확인하여 서비스하기 때문에, 세션(session)이나 쿠키 (cookie)를 이용해 클라이언트의 상태정보를 유지할 필요가 없다.  ㅁ OAuth는 왜 필요한가?  OAuth가 사용되기 전에는 인증방식의 표준이 없었기 때문에 기존의 기본인증인 아이디와 비밀번호를 사용하였는데, 이는 보안상 취약한 구조이다. 기본인증이 아닐 경우는 각 애플리케이션들이 각자의 개발한 회사의 방법대로 사용자를 확인하였다. OAuth는 이렇게 제각각인 인증방식을 표준화한 인증방식이다. OAuth를 이용하면 이 인증을 공유하는 애플리케이션끼리는 별도의 인증이 필요없다. 따라서 여러 애플리케이션을 통합하여 사용하는 것이 가능하게 된다.  ㅁ 주요 4가지 객체  resource owner (자원 소유자)는 protected resource (보호된 자원)에 접근하는 권한을 제공합니다.  resource server (자원 서버)는 access token을 사용해서 요청 (request)을 수신할 때, 권한을 검증한 후 적절한 결과를 응답합니다.  Client (클라이언트)는 resource owner (자원 소유자)의 protected resource (보호된 자원)에 접근을 요청을 하는 애플리케이션 (application)입니다.  authorization Server (권한 서버)는 client (클라이언트)가 성공적으로 access token을 발급받은 이후에 resource owner (자원 소유자)를 인증하고 obtaining authorization (권한 부여)를 합니다.  ㅁ 다른 인증방법과 OAuth의 차이점  OpenID같은 인증 프로토콜도 http방식을 쓰는 것까지는 동일하지만, 다른 것과 다르게 OAuth는 인증목적이 아니라 “허가”목적이다. 네이버 문서에 따르면 OAuth도 인증절차가 있지만 목적은 인증이 아니라 허가이며, API를 호출하는 권한이 있는 사용자인지 확인하는 목적이 주 목적이다.  ㅁ OAuth 용어 정리 (공식문서보다 네이버 문서가 더 보기 편하게 설명되어 있어 참고함.)  - User : Service Provider에 계정을 가지고 있으면서, Consumer를 이용하려는 사용자.  - Service Provider : OAuth를 사용하는 Open API를 제공하는 서비스  - Consumer : OAuth 인증을 사용해 Service Provider의 기능을 사용하려는 애플리케이션이나 웹 서비스  - RequestToken : Consumer가 Service Provider에게 접근 권한을 인증받기 위해 사용하는 값. 인증이 완료된 후에는 Access Token으로 교환한다.  - Access Token : 인증 후 Consumer가 Service Provider의 자원에 접근하기 위한 키를 포함한 값  ㅁ OAuth의 프로세스    <네이버에서 설명한 인증과정 비유>  ㅇㅇ    <위키백과에 설명된 OpenID와 OAuth의 차이>    ㅁ 실습 중 참고사항    <구글 로그인 인증관련 창을 띄우고 성공여부에 따라 처리하는 결과처리함수 : 리퀘스트 코드와 결과를 전달받은 account코드> | |