**Introduction to web applications**

**Notes:**

1. **Websites are static pages that is the same for every user (Web 1.0)**
2. **Web Apps are Interactive, dynamic pages the have functions and modular that can run on any platform without being optimized (Web 2.0)**
3. **Web Apps VS Native OS Apps**
4. **Open-Source Web Application (WordPress, OpenCart, Joomla)**
5. **Closed-Source Web Application (Wix, Shopify, DotNetNuke)**
6. **Common Web Apps Attacks:**
   * **SQL Injection**
   * **File Inclusion**
   * **Unrestricted File Upload**
   * **Insecure Direct Object Referencing**
   * **Broken Access Control**
7. **Web Application Layouts:**
   * **Infrastructure (Client-Server, 1 Server, n-Server 1-DB, n-Server n-DB)**
   * **Components (Client, Server, Services, Functions)**
   * **Architecture (Presentation Layer, Application Layer, Data Layer)**
8. **Back End Components (Back End Servers, Web Servers, DB, Frameworks)**
9. **URL Encoding (Percent Encoding)**
10. **DOM Standard Parts (Core DOM, XML DOM, HTML DOM)**
11. **Relational Databases (MySQL, MSSQL, Oracle, PostgreSQL)**
12. **Non-Relational Databases (MongoDB, Elasticsearch, Apache Cassandra)**
13. **Development Frameworks (Laravel, Express, Django, Rails)**
14. **API Standards (Simple Objects Access “SOAP”, Rep. State Transfer “REST”)**
15. **Common Web Vulnerabilities:**
    * **Broken Authentication / Access Control**
    * **Malicious File Upload**
    * **Command Injection**
    * **SQL Injection**