Ryan Dean

Period: A

3/8/15

Oracle Database Presentation Outline

* Interaction
  + Information stored in server (database)
  + Information received and displayed through web page
  + Information processed through database scripting language
    - Through a database host such as a localhost server
* Creating a Database
  + Commonly helped with 3rd party software such as WebMatrix
    - Follow steps to set up an SQL database
    - Add columns, tables, etc.
  + Create user account details
    - Username, password (Oracle class members)
* Create Host
  + Localhost server
    - Serves as a web server running on local machine
    - Host to link web page to database
* Connect to Host
  + Add PHP to connect to host
* Query Data
  + Use SQL scripts to query(retrieve) your data
  + Output data to user through scripts with HTML structure
* Scripting Languages: Web
  + Web Page (User End):
    - HTML:
      * Standard markup language to create web pages.
      * Structure and content of the site.
      * Considered Secure
    - CSS:
      * Styling of the HTML content.
* Scripting Languages: Server
  + PHP:
    - Server side scripting language for web development
    - Most popular scripting language of its type
    - 240 million websites and 2.1 million servers.
* Scripting Languages: Database
  + SQL:
    - Commonly used and known for managing data
    - Known by classmates
    - Used for database management
* PHP
  + Runs on web server
  + Create dynamic web page content
    - Because code is executed in runtime
  + Used as a link between web and database server
* Why PHP?
  + Most widely recognized
  + Most resources available
    - Good for learning students
  + Solid and stable infrastructure
* Security Roadblocks
  + Web Page:
    - Need of a host server to connect between HTML and database.
    - Possible HTML code injection if live project.
      * Embed into project undetected.
    - Cross Site Scripting
      * Using code injection, causes a function to be executed undetected.
  + PHP:
    - Turn register globals off
      * Potential for admin to be a global variable with no code. Get all information from it.
    - Turn Magic quotes off
      * Makes PHP susceptible to code injection by using escape characters.
    - Error reporting will give hackers the upper hand as they know what to look for
  + SQL:
    - Physical Access to server
    - Network Security
    - More services and features enabled on server, higher risk of attack
    - Code Injection
    - Authorization
* Sources
  + http://www.w3schools.com/website/web\_database.asp
  + http://smallbusiness.chron.com/database-52268.html
  + http://en.wikipedia.org/wiki/HTML
  + http://www.technicalinfo.net/papers/CSS.html
  + http://en.wikipedia.org/wiki/PHP
  + http://stackoverflow.com/questions/1165040/what-security-issues-should-i-look-out-for-in-php
  + http://en.wikipedia.org/wiki/SQL
  + https://technet.microsoft.com/en-us/magazine/2009.05.sql.aspx