Security for the **Web**

Thanks again to Dave Levin for some slides

The Web

- Previously: **Applications written in C and C++**
  - Issues like *remote code injection* and *sensitive data theft* arise from **violations of memory safety**

- Now: **Security for the World-Wide Web** (**WWW**)
  - New vulnerabilities to consider: **SQL injection**, Cross-site Scripting (**XSS**), **Session Hijacking**, and Cross-site Request Forgery (**CSRF**)
  - These share some common causes with memory safety vulnerabilities; like **confusion of code and data**
    - **Defense** also similar: **validate untrusted input**
  - New wrinkle: **Web 2.0's use of mobile code**
    - How to protect your applications and other web resources?

Web Security Outline

- Web 1.0: the basics
  - **Attack**: SQL (“sequel”) injection
- The Web with state
  - **Attack**: Session Hijacking
  - **Attack**: Cross-site Request Forgery (CSRF)
- Web 2.0: The advent of Javascript
  - **Attack**: Cross-site Scripting (XSS)
- **Defenses throughout**
  - *Theme*: **validate or sanitize input**, then trust it