User Input

Books

- 19 Deadly Sins of Software Security: Programming Flaws and How to Fix Them – Hpward, LeBlanc, Viega – McGraw-Hill, 2005.
- Innocent Code: A Wake-up Call for Web Developers – Huseby, Wiley 2004.
- Writing Secure Code, Howard and Le Blanc, Microsoft Press 2003.
- The Web Application Hacker's Handbook, Stuttard, Pinto, Wiley 2008.

User Input - Example

- User input might be simply stored in a database.
- What harm can that do?
- But in order to be stored in a database, some SQL is probably executed.
- So user input becomes part of some SQL code.
- And if the programmer is not careful, the user can manipulate the SQL in ways not foreseen by the programmer.

User Input

- Such an attack is know as an SQL injection attack.
- It is a particular example of a general problem where user input becomes part of some text that is interpreted by a subsystem.
- Examples
  - SQL
  - Command interpreters (cmd, bash, sh, csh)
  - Javascript

Validating User Input

- Identify and Validate all Input
- Create Validation Functions
- Check Ranges
- Check Lengths
- Check for metacharacters, for example ; in SQL, as these can be used to alter the behavior of the SQL interpretor.
-

WhiteLists and BlackLists

- Whitelists – what is acceptable
- BlackLists – what is not.
- WhiteLists work well. Blacklists not so well.
- White lists implement “deny by default”.
- Whereas blacklists implement allow by default.

Logging

- Obviously useful for tracking down attacks and even legal proceedings.
- Web Server logs can store a certain amount of information.
  - IP address of client
  - Date/Time
  - The HTTP request.
  - Parameters of POST request will not normally be logged.

Logging (cont)

- The Web Application will have a lot more information than the Web Server.
  - Session information that identifies a user.
  - Operations
  - POST parameter values supplied
- So create application level logs.

Log Monitoring

- Log monitors are used to scan logs in real time and attempting to identify attempted intrusions.
- A critical part of Intrusion Detection Systems (IDS).

Logging APIs

- For example, Log4J.
- Has a number of Log Levels including
  - DEBUG
  - INFO
  - WARN
  - ERROR
  - FATAL
- Output can be directed to files as well as console obviously.

Logging

- Logging is a subsystem and has metacharacters.
- For example \n used to separate logged events.
- If logging user data, be aware that users can insert meta characters to confuse log monitoring software.