PHP Security-2

Jupiter Zhuo

What is possibly the most basic threat to the safety of your users' data, input abuse

- Input Metacharacters
- Input Wrong type
- Input Wrong Length
- Input containing unexpected command
- Entry data into hidden Interfaces

What Should we do

- Turning off Global Variable
- Declare Variable
- Anticipate expected input meet your expectation
- check length, type, and format
- Sanitize & Validation user input

Filtering,Validation and output escaping

- What is Filtering => Filtering is transform value ex : strip_tag()
- What is Validation => Validation Verifies value and performed against a set of rules ex : str_len()
- What is output escaping => Make information safe to display & can involve literally escaping value (ex : Quotes)

Why Filtering,Validation and output escaping (Golden Rule)

- Important component in protecting against common Attack
- Prevent Break in strings
- Help to keep data “clean”
- Note : Sometimes validation is more appropriate than filtering

What are the most common PHP filtering function and Techniques ?

- Changing Data Type
- Strip_tags function
- str_replace function
- preg_replace function

What are the most common PHP Validation function and Techniques ?

- ctype function
- stripos function
  - strpos case sensitive
- preg_match function
- validation by lookup

What are the most common PHP output escaping function and Techniques ?

- html_entities function
- html_specialchars function

Sanitize Data Using Fiter_var

- Common validation filters
  - filter_var() with validation return true false
    - FILTER_VALIDATE_EMAIL
    - FILTER_VALIDATE_INT
    - FILTER_VALIDATE_IP
- Common sanitization filters
  - filter_var() with "sanitize" filters cause filtering to take place
    - FILTER_SANITIZE_EMAIL
    - FILTER_SANITIZE_NUMBER_INT

Lab

- Filtering and validating POSTED FORM DATA
  - Modify add member
  - add validation for all field
  - add filtering for appropriate fields
  - Add appropriate validation message for each field
  - Make sure invalid entries are not added to database
  - Test against attack