PHP Security-4

Jupiter Zhuo

Prevent The Most Common Form of Attacks

- Protecting Against Unplanned Information Disclosure
- Protecting Predictable Resource Location
- Insufficient Authorization
- Improper Access Control
- Avoiding Misconfiguration
- Protecting file Upload

Protecting Against Unplanned Information Disclosure

- Display of Error
- Error Handling
- Error Reporting and logging
- Exception handling
- Improving Code Efficiency

Display Errors

- PHP Setting display_errors
- display errors should be ON for development
- display errors should be OFF for Production

Error Handling

- Use if statement to anticipate error conditions
  - use ternary operator to test and set default
  - use set_error_handler() and Also set debug_print_backtrace function

Protecting Against Predictable Resource Location

- Dont use default folder name ex :uploads, admin or administrator and etc.
- use prefix on table name
- don't use Predictable field name
  Like :password, username and etc
- Change default sessionID using ini_set or session_name() function

PHP.ini should be set and shouldn't be set

- should be set
  - default timezone
  - default charset
- shouldn't be set
  - mysqli.default_user, mysqli.default_pwd, pdo.dns

Protecting against Insufficient Authorization

- Improper Access to secure areas of the website
  - Need Carefully examine program logic
  - Consider establishing Access control list (ACL)
- Improper Authority for low Level accounts
  - need to apply the principle of least privilege on database

Protecting against Improper Access Control

- Proper storage of password
  - Do Not Storage as plain text
  - One Way password
- password Control
  - min length
  - Mixture Char
- Create new and reset password
  - Security Question
  - Offline Confirmation
  - Extra Information when reset password

Avoid Misconfiguration

- File System right
  - please Aware directory permission
  - Protect files and directory off the document root
- php.ini security setting
  - https://www.cyberciti.biz/tips/php-security-best-practices-tutorial.html
- running php as CGI binary

Protecting file Upload

- PHP.Ini Setting
  - upload_max_filesize --> defaults to 2M and must be less than:
  - post_max_size --> defaults to 8M and must be less than:
  - memory_limit --> defaults to 128M
- Safety Check
  - $_FILES["field"]["error"]
  - is_upload_file()

Protecting file Upload

- Sanitize Filename
  - $_FILES["field"]["name"]
    - use basename() remove bad path info
    - Preg_replace()
- Move To Secure Location
  - Make own Directory with Unusual Directory name

Protecting file Upload

- Client Validation + Server Validation
- Other Safety Measurement
  - Save Directory With Anti Virus
  - Cron Jobs To Check