

# Injection

- SQL Injection
  - Input passes to SQL query
  - Passes SQL query and manipulate the outcome of queries
- Command Injection
  - Input is passed to system commands
  - Able to execute arbitrary system commands

# Defense

- Use Allow List
  - If characters not in allow list > throw error
- Strip input
  - If input has dangerous characters, remove them process

# In PHP

- Use `$ pass thru ($CMD);`