CS 576 – Systems Security
Command Injection and Similar Attacks

Georgios (George) Portokalidis

Command Injection Attacks

- Command injection is an attack where an attacker can insert arbitrary commands on the host operating system via a vulnerable application
- They are possible when an application passes unsafe user supplied data to a system shell
  - E.g., through system(), exec(), or similar APIs

https://bitbucket.org/gportoka/cs576-22s/src/main/lectures/01-command_injection/

Prevent Command Injection Attacks

- Do not make assumptions about input
- Strict input validation
  - Data type (string, integer, real, filename, etc.)
  - Allowed character set, minimum and maximum length
  - Patterns (e.g., SSN, email, URL, etc.)
- Avoid filtering specific characters (e.g., ‘;’ or ‘&&’) as it is frequently not as effective
- Use libraries Faster and reusable
  - For example: https://www.yeahhub.com/7-best-python-libraries-validating-data/

Path Traversal Attacks

- A path traversal attack is when an attacker supplies input that gets used in a path to access a file that was intended to be accessed

https://bitbucket.org/gportoka/cs576-22s/src/main/lectures/01-path_traversal/

Prevent Path Traversal

- Do not make assumptions about input
- Do not allow user input into paths
- Input validation
- Avoid filtering specific characters (e.g., ‘..’) as it is frequently not as effective