Command Injection Prevention Guide

What is Command Injection?

Command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application.

It happens when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell.

Prevention Strategies

- **1. Avoid Calling OS Commands:** Use language-specific APIs instead of system calls whenever possible (e.g., use `os.mkdir` instead of `os.system("mkdir")`).
- **2. Input Validation:** Validate input against a rigorous allow-list. Ensure input contains only safe characters (alphanumeric).
- **3. Parameterization:** If you must use OS commands, use functions that support argument parameterization (e.g., `subprocess.run(["ls", dirname])` instead of `os.system("ls " + dirname)`).

```
import subprocess subprocess.run(["ls", "-l", user_input]) # Safe
```