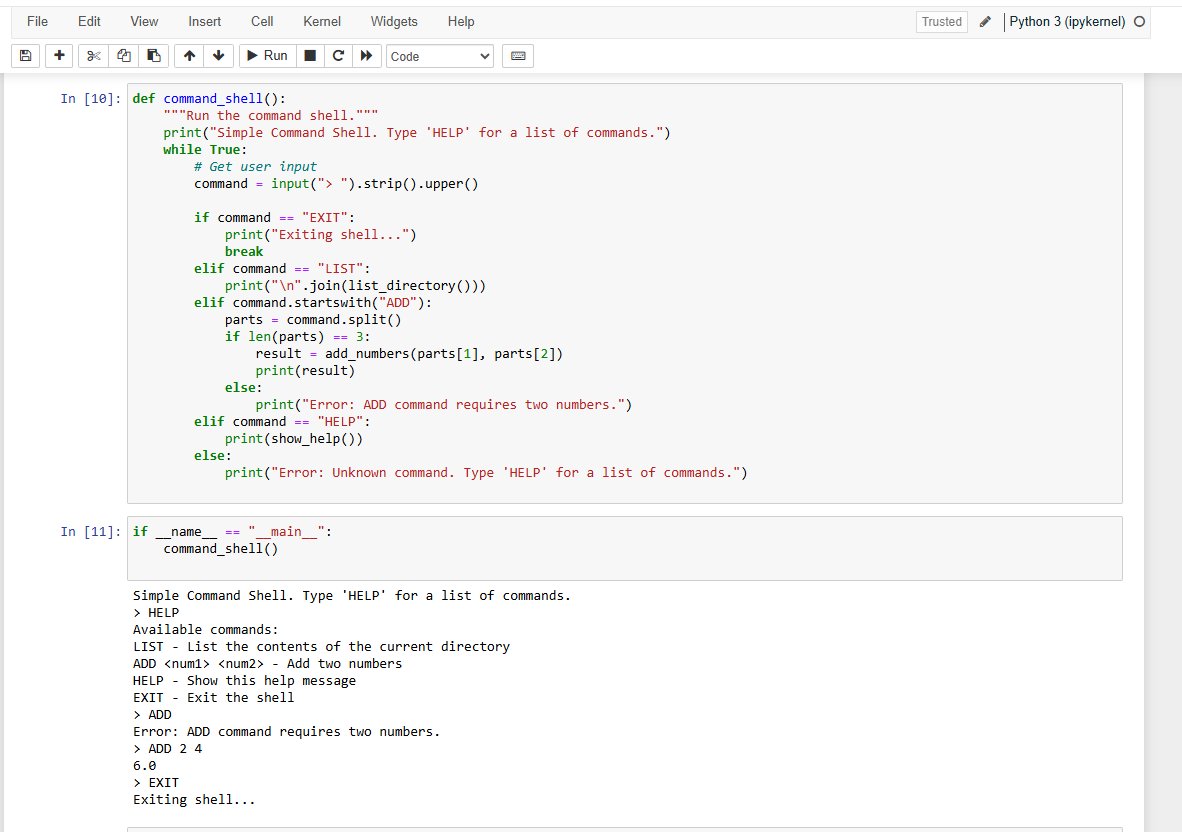
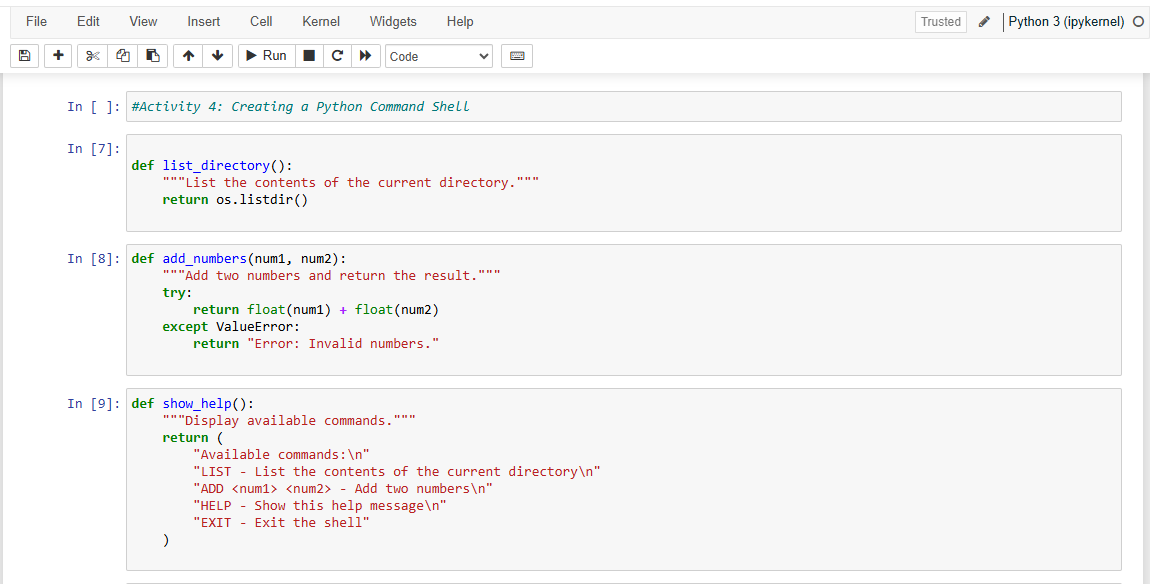
**Exploring a Simple Python Shell**



**Security Analysis**

**Security Vulnerabilities**

If the shell is extended, for example by using os.system(), to run system commands, then it could be subject to command injection attacks. Malicious input could then be executed on the host system.  
This is probably the most important point: with this shell, no validation or sanitization of input is performed. As a simple example, attempting to provide a non-number input for performing number addition will return an error message. This is not a direct vulnerability itself but helps explain that input should always be validated.

**Recommendation to Increase Security**

Always validate and sanitize user input, such as checking that commands and parameters have the expected format and are within the expected range. Never run system commands from user input without proper validation.