Static Analysis with PyLint

Ben Straub and Jason Poppler

PyLint

- Static analyzer for Python (similar to FlawFinder)
- Output is a list of warnings to the developer
- Open source, support plugins
- Astroid - Abstract Syntax tree
    - supporting library
    - allows navigation of the source code

PyLint for CWEs!

The most common CVEs for Python are around input sanitization. So we chose:

- CWE-78
  - Ban Arbitrary Execution of a Subprocess
  - Ban OS Created Subprocess
- CWE-755
  - Pass only except blocks
- CWE-552
  - File Read sanitization
- CWE-20
  - input() sanitization