Assignment 1 Outline

1. Intoduction
   - NASA employee respository
     - OS, database, runtime requirements
     - Python libraries
   - Security concerns
   - Plan for secure repo
     - assumptions and limitations
     - recommendations

2. NASA repo requirements
   - Linux and Windows OS cross compatibility
     - Python libraries
       - pylint
       - pytest
       - pandas
       - logging
       - sqlite3
     - space station interface
     - HR interface
     - IT interface
     - local API
   - SQL database – relational
     - employee
     - department
     - project
     - assignment
   - scalability
   - Assumptions
     - Data download requirements – 8GB RAM, 2MB per min
     - CPU – quadcores
     - API – SOAP
     - Latest Windows/Linux OS distribution (compatibility)
     - Monolithic prototype

   - Limitations
     - Request/reply is limited to local ping
     - Open-source programs only
     - Limited CPU/storage for prototype
     - Command line based – No GUI/UI

3. Security concerns
- OWASP top ten
  - SQL injection
  - XSS
  - XML
  - login logic defeat
  - buffer overflow
  - cookie tampering
  - info leak
    - error messages
- Security Recommendations
  - Access controls
    - Custom error messages
      - 200 – 500 level
        - based on access ability
    - group/role controls
      - read, write, execute
    - boundary validation
      - general checks
        - approved charset for input
      - clean SQL
      - encode XML characters
      - encode HTML characters
    - 2FA
  - session mgmt
    - cookies
      - encryption
    - inactivity logout
- source code parsing
  - known weaknesses in strings/commands/classes etc.

4. Testing
- Code testing
  - Unit testing - each function/method/feature
  - Integration/end-to-end testing
- penetration testing
  - on the command line
    - common input commands for
      - SQLi
      - XSS
      - XML
      - login defeat
      - encryption defeat

- cookie tampering
- etc.

5. Conclusion
   - Recap of main points above