

# Security

The security landscape is a bit of a \$\*1tshow

# Some best practices

- Keep python and dependencies up to date
- Always sanitize external data
- Scan
  - Bandit
  - Type annotations
- Be careful with external packages
- Be careful with pickle/java serializable
- Sandboxing
- Use UUIDs
- Know your algorithms - secure hashing, RNG