Vulnerabilities & Exploits

Apa itu Vulnerabilities

- Kelemahan atau ralat dalam kod sesebuah sistem
- Jika disalahguna, integriti, confidentiality sesuatu data akan terjejas dan boleh mengakitkan kehilangan data penting

Salah siapa?

- PEBKAC
- Bugs dalam code
- Misconfiguration
- Kurang cakna dengan perihal keselamatan

Jenis Vulnerabilities

- SQL Injection
- Arbitary File Upload
- Local File Inclusion (LFI)
- Brute-force (Weak Password)
- Buffer Overflow
- .. dan banyak lagi

Kesan dari Vulnerabilities

- Kebocoran Data/Maklumat
- Defacement
- Hilang reputasi

Camana nak cari Vulnerabilities?

- Static Code Analysis
  - Debugging code
- SQL Injection
- Fuzzing
  - Automated tools untuk cari vulnerabilities
  - Macam QC people tapi auto. LOL

Apa itu Exploits?

- Code atau program yang ditulis untuk menyalahgunakan vulnerabilities

Demonstrasi Exploits

- DirtyCOW
  - https://youtu.be/KRMDCITEQuY
- PwnKit
  - https://youtu.be/V67GtBCHiJ0
- EternalBlue
  - https://youtu.be/5_zV0HZQn7g