CHAPTER 10

WEBSITE RECON & EXPLOIT

Checkpoint

- *Done*
  - belajar dasar pemrograman
  - membuat program yang relevan dengan cybersecurity
- *What's next?*
  - praktik membuat program untuk cek kelemahan sistem
  - praktik lagi dan lagi.

Praktik

- Setup sistem yang akan diserang
  - DVNA (https://github.com/appsecco/dvna)
- Buat program untuk recon/exploit (lengkap dengan DRIVE framework)
  a. path/directory fuzzing
  b. brute force web login
  c. SQL injection
  d. XSS exploit
  e. CSRF exploit
- ⚠️ **Kode hanya untuk keperluan edukasi. Jangan dijalankan di mesin yang tidak kamu miliki *authorization*-nya.**

Recon: Path/Directory Fuzzing

- **Definisi**: melakukan brute force untuk menebak path web berisi informasi sensitif
  - /admin, /test
- **Dampak**: [Low]
  - exposure atas path yang tidak untuk umum
- **Mitigasi**:
  - sembunyikan path sensitif
  - disable indexing
  - set permission untuk akses path
- Library Python terkait:
  - `wfuzz`
  - `dirsearch`

Exploit: Brute Force Web Login

- **Definisi**: melakukan brute force untuk login dengan set credential yang telah ditentukan
- **Dampak**: [Medium]
  - *unauthorized access*
- **Mitigasi**:
  - rate-limiting
  - account lockout
  - 3rd party: CAPTCHA, Cloudflare
- Library Python terkait:
  - `request`
  - `hydra`
  - `mechanize`

Exploit: SQL Injection

- **Definisi**: memasukkan perintah SQL dari user yang nantinya dieksekusi oleh sistem target
- **Dampak**: [High]
  - kebocoran data DB
  - unauthorized *access* dengan manipulasi data user
  - merusak aplikasi jika struktur DB diubah (misal: Drop Table)
- **Mitigasi**:
  - sanitasi input
  - gunakan ORM atau safe query
- Library Python terkait:
  - `sqlmap`
  - `requests`

Exploit: Cross-site Scripting (XSS)

- **Definisi**: memasukkan malicious script ke dalam web app untuk eksekusi hal tertentu, dan berdampak ke pengguna lain.
- **Dampak**: [Medium]
  - pencurian cookies
  - redirect user
  - deface tampilan UI
- **Mitigasi**:
  - validasi input
  - escape HTML output
- Library Python terkait:
  - `selenium`
  - `requests`

Exploit: Cross-site Request Forgery (CSRF)

- **Definisi**: memaksa user yang terautentikasi untuk eksekusi hal di luar kehendak, misal change password, konfirmasi transaksi finansial, dll
- **Dampak**: [High]
  - hilang kontrol atas akun
  - infiltrasi attacker ke dalam sistem
- **Mitigasi**:
  - CSRF token
  - verifikasi referrer
  - SameSite cookies
- Library Python terkait:
  - `BeautifulSoup`
  - `requests`