Tugas Pendahuluan
Praktikum - 3
SQL Injection dan XSS Scripting

BY
Wahyu Isya wantoro Adi
52151000023

Asisten 2017

Jawablah dengan detil dan terarah.

1. Coba jelaskan apa yang dimaksud dengan :
    a. Blind SQL Injection
    SQL Blind (Structured Query Language) injeksi adalah jenis serangan injeksi SQL yang meminta database pertanyaan benar atau salah dan menentukan jawaban berdasarkan respon aplikasi
    (https://www.owasp.org/index.php/Blind_SQL_Injection)

    b. SQL Injection
    Injeksi SQL atau SQL Injection memiliki makna dan arti yaitu sebuah teknik yang menyalahgunakan sebuah celah keamanan yang terjadi dalam lapisan basis data sebuah aplikasi
    (http://www.binushacker.net/pengertian-tutorial-tools-sql-injection-cara-kumpulan-software-sql-injection.html)

    c. XSS Scripting
    Scripting Cross-Site (XSS) serangan adalah jenis injeksi, di mana script berbahaya yang disuntikkan ke situs web lain jinak dan terpercaya. serangan XSS terjadi ketika seorang penyerang menggunakan aplikasi web untuk mengirim kode berbahaya, umumnya dalam bentuk script sisi browser, untuk pengguna akhir yang berbeda
    (https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))

2. Apa yang membedakan antara Blind SQL Injection dengan SQL Injection itu sendiri?
    Perbedaannnya adalah cara kerjanya, Standar SQL Injection bekerja seperti mengajukan pertanyaan-pertanyaan yang akan membingungkan aplikasi ke kembali jawaban dalam pesan kesalahan. Blind SQL Injection bekerja seperti mengajukan pertanyaan yang hanya bisa memiliki jawaban ya atau tidak. Dari sana Anda hanya iterate melalui semua pilihan Anda sampai semua ya dan tidak ada tanggapan membangun hasil yang diinginkan. (Blind SQL evolusi dari SQL injection)
    (https://danielmiessler.com/blog/a-fantasy-explanation-of-standard-vs-blind-sql-injection/#gs.5QAWhyI)

3. Coba jelaskan apa saja hal preventif yang dapat dilakukan untuk menghindari perlakukan SQL Injection pada suatu website !

    - Menggunakan mysql_real_escape_string().
    - Menggunakan addslashes()

- Menggunakan casting input. Misalnya nilai harus berupa integer, anda bisa melakukan casting dengan fungsi int()
- Memeriksa apakah inputan mengandung karakter terlarang dengan fungsi strpos().
  (http://harviacode.com/2015/01/28/cara-mencegah-sql-injection/)

4. Coba sebutkan tools yang dapat digunakan untuk melakukan SQL Injection.
   (Minimal 4)
   - Havij SQL Injection
   - Pangolin – Automated SQL Injection Test Tool
   - BSQL Hacker
   - Safe3 SQL Injector
   - The Mole
   - SQLNinja SQL injection
     (http://resources.infosecinstitute.com/best-free-and-open-source-sql-injection-tools/#gref)

5. Coba jelaskan hal preventif apa yang dapat dilakukan untuk menghindari XSS.
   - Mendowonload software Open Source Libraries mengenai pencegahan XSS attack seperti PHP AntiXSS , HTML Purifier , xssprotect , XSS HTML Filter
   - memakai fungsi *htmlspecialchars()*
   - menambahkan filter dengan str_replace
   - Untuk user solusi adalah mematikan semua bahasa script yang ada pada komputernya
   - memastikan bahwa halaman yang membangkitkan konten secara dinamis tidak mengandung tag yang tidak diinginkan.
   - Encoding

     (https://hayungku.wordpress.com/2012/05/28/xss-cross-site-scripting/)