TUGAS

KEAMANAN JARINGAN

“INJECTION”

Nama : Mega Putri Rahmawati Darta

Kelas : D4 LJ IT B

NRP : 3122640038

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

TAHUN AJARAN 2022/2023

1. Apakah fungsi petik pada percobaan login dengan SQL Injeksi?
   Jawab :

   Select * from user where username = “bender@juice-sh.op” ‘-- and password=”password"

   Pada percobaan SQL injection digunakan untuk bisa masuk ke perintah SQL. Oleh karena itu setelah karakter petik diberikan karakter ‘—’ dikarenakan karakter tersebut digunakan untuk mengcomment dari perintah setelahnya. Dengan adanya karakter tersebut maka proses yang diajlankan pada perintah SQL hanya perintah berikut ini :

   Select * from user where username = “bender@juice-sh.op”

   Sehingga perintah tersebut membantu user untuk login tanpa menginputkan password yang sesuai dengan username yang tersimpan didatabase.

2. Apa itu input sanitation, berikan contohnya?
   Jawab :
   Apabila ada case sebuah username atau nama yang mengandung karakter backtick, maka diperlukan input sanitation untuk mengecek karakter tersebut. Dan karakter tersebut bisa diubah menjadi backslash.
   Pada input sanitation akan mefilter atau menghilangkan karakter yang dianggap tidak valid atau berbahaya. Tujuan utamanya adalah mencegah serangan keamanan seperti SQL injeksi.
   Contoh Input sanitation adalah form yang memeriksa apakah input tersebut memenuhi kriteria yang sudah ditentukan. Misalnya pada form login dimana untuk bagian username atau email tidak boleh mengandung karakter selain huruf dan angka.
   Selain itu sanitation input juga dapat berupa pembatasan escape karakter, parameterized queries, whitelist validation, dan input filtering.

3. Apa perbedaan injection dan sql injection ?
   Injection memiliki banyak jenis salah satunya adalah SQL Injection. Berikut merupakan macam-macam injection lainnya :
   1. XSS (Cross-Site Scripting) : injeksi dengan melibatkan penyisipan skrip atau kode yang berbahaya didalam web kemudian dieksekusi oleh browser pengguna.
   2. Command Injection : Terjadi ketika input yang diterima oleh sistem digunakan untuk membangun perintah shell yang kemudian dieksekusi oleh sistem.
   3. LDAP : Serangan ini terjadi ketika input yang diterima oleh aplikasi yang menggunakan Lightweight Directory Access Protocol (LDAP) digunakan dalam operasi pencarian atau autentikasi.
   4. XML Injection: Serangan XML Injection terjadi ketika input yang diterima oleh aplikasi yang memproses XML digunakan untuk memanipulasi struktur XML atau memasukkan entitas XML yang tidak valid.

5. OS Command Injection: Serangan ini serupa dengan command injection, tetapi terjadi pada tingkat sistem operasi.
6. Path Traversal: Serangan ini memanfaatkan kerentanan dalam pemrosesan jalur file oleh aplikasi.

4. Bagaimana mengamankan input form agar tidak terinjeksi ?
   Diberikan validasi karakter untuk menghindari kemungkinan terinjeksi, seperti dengan menerapkan input sanitation yang sudah dijelaskan diatas.