An toàn dữ liệu

Bởi:

unknown

Ngôn ngữ SQL cho phép người sử dụng kiểm tra dữ liệu của mình khi cập nhật và tuyên bố quyền truy nhập tới cơ sở dữ liệu để đảm bảo cho tính nhất quán và toàn vẹn dữ liệu. Đặc biệt trong trường hợp có nhiều người cùng sử dụng hệ thống, nhất là cùng truy nhập tới cùng một tệp (bảng) của CSDL.

Vì vậy cần phải có những biện pháp phòng ngừa để ngăn ngừa cac nguy cơ

- Vô tình sử dụng sai
- Sự cố trong quá trình xử lý giao dịch
- Dị thường gây ra bởi truy cập đồng thời vào CSDL
- Dị thường gây ra bưởi sự phân tán của dữ liệu trên một số máy tính
- Cố tình sử dụng sai
- Đọc dữ liệu một cách trái phép (đánh cắp thông tin)
- Sửa đổi dữ liệu trái phép
- Phá hoại dữ liệu trong CSDL
- …

Bảo vệ dữ liệu trên hai phương diện:

- An toàn dữ liệu: Chỉ việc bảo vệ CSDL tránh khỏi những hiện tượng cố tình sử dụng sai dữ liệu
- Toàn vẹn dữ liệu: Chỉ việc tránh khỏi những hiện tượng vô tình hay cố ý làm mất tính nhất quán cua dữ liệu.

Sau đây là một số biện pháp:

Biện pháp : Sự cấp quyền

Nói một cách cụ thể người sử dụng có thể có một số quyền truy cập sau:

Quyền đọc: được phép đọc dữ liểu trong CSDL

Quyền chèn thêm dữ liệu: Được phép chèn thêm dữ liệu mới vào trong CSDL có sẵn nhưng không được thay đổi bất kỳ dữ liệu có sẵn nào.

Quyền cập nhật: Được phép sửa đổi dữ liệu nhưng không được xoá dữ liệu

Quyền xoá: Được phép xoá dữ liệu trong CSLD

Ngoài quyêng truy cập, người sử dụng còn có thể được phép sửa đổi lược đồ CSDL:

Quyền tạo chỉ mục: Được phép tạo các chỉ mục

Quyền quản lý tài nguyên: Được phép tạo các quan hệ mới

Quyền thay đổi: Được phép thêm hoặc xoá các thuộc tính trong quan hệ

Quyền loại bỏ: Loại bỏ một quan hệ

Biện pháp 2: Quyền tạo và sử dụng khung nhìn (Views)

Khung nhìn là một phương thức cho phép:

+ Che dấu những dữ liệu mà người sử dụng cụ thể nào đó không cần thiết phải "nhìn" thấy

+ Làm đơn giản hoá việc sử dụng hệ thống

+ Làm tăng cường an toàn dữ liệu

+ …

Biện pháp 3: Sự cấp đặc quyền luân chuyển dữ liệu

Một người sử dụng có thể chuyển quyền cho những người sử dụng khác và cần phải kiểm tra cẩn thận những đặc quyền này.

Sơ đồ chuyển quyền:

Những câu lệnh cấp và thu hồi quyền trong SQL:

- Lệnh cấp quyền: Việc tuyên bố và kiểm tra quyền truy nhập CSDL được thực hiện qua mệnh đề GRANT. Cú pháp như sau:

```
GRANT danh_sách_quyền ON đối_tượng TO danh_sách_người_sử
_dụng [WITH GRANT OPTION];
```

trong đó:

+ *danh_sách_quyền truy nhập:* trong SQL bao gồm: read, select, write, insert, update, delete và run.

+ *đối_tượng:* là tên bảng hoặc tên khung hoặc tên chương trình

+ *danh_sách_người_sử _dụng*: là tên người hoặc một nhóm người

+ Từ khoá WITH GRANT OPTION đảm bảo cho người sử dụng có thể tiếp tục trao quyền cho người khác khi cần.

Ví dụ: Trao quyền đọc bảng S cho cô Hồng và khi cần thì cô Hồng có thể trao quyền cho người khác

GRANT read ON S TO Hong GRANT OPTION ;

- Lệnh thu hồi quyền: REVOKE, cú pháp như sau:

```
REVOKE danh_sách_quyền ON tên_bảng/tên_khung_nhìn/
tên_chương_trình/ FROM danh_sách_người_sử_dụng;
```

Chú ý: Việc huỷ bỏ quyền của một người sử dụng kéo theo việc huỷ bỏ quyền của những người sử dụng được uỷ quyền.

Biện pháp 4: Mã hoá dữ liệu