Mục tiêu

Thực hiện form Đăng ký và tạo tài khoản [hướng dẫn ghi password].

Nội dung

Với yêu cầu của bài tập tuần 06. Thực hiện ghi dữ liệu xuống database, khi đó vấn đề cần quan tâm là ghi password như thế nào để đảm bảo các yếu tố: privacy (ko bị lộ password với admin), thực hiện kiểm tra xác thực được.

Để đạt được mục tiêu đó thì phương pháp cơ bản là: thực hiện hash với salt trước khi ghi password.Thực hiện như sau:

- Tạo class User

```
public class User
{
    public string f_Username { get; set; }
    public string f_Name { get; set; }
    public string f_Password { get; set; }
    public  string f_Email { get; set; }
    public int f_Permission { get; set; }
    public DateTime f_DOB { get; set; }
}
```

- Xử lý password để lưu

```
// lấy password bản rõ
var strPw = txtPassword.Text;
// sử dụng hỗ trợ hash SHA1 của .NET
var sha = new SHA1CryptoServiceProvider();

// vì các thuật toán hash có săn làm việc với mảng byte
// nên cần chuyển sang mảng byte để xử lý
// sử dụng phương thức chuyển chuỗi sang mảng byte
// có sẵn trong các lớp Encoding
var arrBytePw = ASCIIEncoding.ASCII.GetBytes(strPw);
// sử dụng thời gian hiện tại làm đại lượng salt
// (để có được xác suất khác nhau cao)
var strTimeNow = DateTime.Now.Millisecond.ToString();

// ghép salt vào với password
var arrTimeNow = ASCIIEncoding.ASCII.GetBytes(strTimeNow);
var arrPwSalt = new byte[arrBytePw.Length + arrTimeNow.Length];
Array.Copy(arrBytePw, arrPwSalt, arrBytePw.Length);
Array.Copy(arrTimeNow, 0, arrPwSalt, arrBytePw.Length, arrTimeNow.Length);

// thực hiện hash
var arrPwHashed = sha.ComputeHash(arrPwSalt);

// ghép salt vào kết quả để lưu trữ salt xuống database
var arrPwSaltHashed = new byte[arrPwHashed.Length + arrTimeNow.Length];
Array.Copy(arrPwHashed, arrPwSaltHashed, arrPwHashed.Length);
Array.Copy(arrTimeNow, 0, arrPwSaltHashed, arrPwHashed.Length, arrTimeNow.Length);
// chuyển đổi mảng byte sang dạng chuỗi HEX để ghi xuống database
var strPwHashed = BitConverter.ToString(arrPwSaltHashed).Replace("-", "");
```

```
// có được dữ liệu User
var u = new User
{
    f_Username = txtName.Text,
    f_Password = strPwHashed,
    f_Email = "abc@gmail.com",
    f_Permission = 1,
    f_DOB = DateTime.Now,
    f_Name = "ABC",
};

// thực hiện ghi User xuống database
```

- Xử lý khi xác thực

```
var strPw = txtPassword.Text;
var sha = new SHA1CryptoServiceProvider();
var arrBytePw = ASCIIEncoding.ASCII.GetBytes(strPw);

// giá trị hash length ứng với giải thuật hash đã chọn
var hashLen = 20;
// sử dụng để chuyển đổi giá trị HEX đã lưu
List<char> lHex = new List<char> { '0', '1', '2', '3', '4', '5', '6', '7',
                                   '8', '9', 'A', 'B', 'C', 'D', 'E', 'F',};

// lấy user từ database dựa vào username
User uTemp = null; // thực hiện lấy từ database
if (uTemp == null)
{
    MessageBox.Show("fail");
    return;
}
// lấy giá trị salt đã lưu
var arrChar = uTemp.f_Password.ToCharArray();
var arrByte = new byte[uTemp.f_Password.Length / 2 - hashLen];
for (int i = hashLen * 2, j = 0; i < arrChar.Length; i += 2)
{
    arrByte[j++] = (byte)(lHex.IndexOf(arrChar[i]) * 16 + lHex.IndexOf(arrChar[i + 1]));
}

// ghép password với salt
var arrPwSalt = new byte[arrBytePw.Length + arrByte.Length];
Array.Copy(arrBytePw, arrPwSalt, arrBytePw.Length);
Array.Copy(arrByte, 0, arrPwSalt, arrBytePw.Length, arrByte.Length);

// thực hiện hash
var arrPwHashed = sha.ComputeHash(arrPwSalt);
var arrPwSaltHashed = new byte[arrPwHashed.Length + arrByte.Length];
Array.Copy(arrPwHashed, arrPwSaltHashed, arrPwHashed.Length);
Array.Copy(arrByte, 0, arrPwSaltHashed, arrPwHashed.Length, arrByte.Length);
var strPwHashed = BitConverter.ToString(arrPwSaltHashed).Replace("-", "");

// so sánh kết quả
if (strPwHashed == uTemp.f_Password)
{
    MessageBox.Show("success...");
}
else
{
    MessageBox.Show("pw error");
}
```