عنوان: **مقایسه نتایج الگوریتم‌های هش کردن اطلاعات در اس کیوال سرور و دات نت**
نویسنده: وحید نصیری
تاریخ: ۱۳۸۸/۰۲/۱۴ ۲۱:۵۴:۰۰
آدرس: www.dotnettips.info
برچسب‌ها: SQL Server

از اس کیوال سرور 2005 به بعد تابع HashBytes نیز به مجموعه توابع قابل استفاده در دستورات T-SQL اس کیوال سرور اضافه شده است که الگوریتم‌های SHA1 | SHA | MD5 | MD4 | MD2 را پشتیبانی می‌کند. برای مثال:

```
DECLARE @str1 VARCHAR(4),
    @str2 NVARCHAR(4)

--متن یونیکد اینجا ناقص ذخیره می‌شود
SET @str1 = 'وحید'

SET @str2 = N'وحید'

SELECT hashbytes('md5', @str1) --C82A7D721AAE517AD76EF1B871BC33CE

SELECT hashbytes('md5', @str2) --7D883091B80F3CD20B872CADBFDDACDF
```

اگر این نتایج را بخواهیم با استفاده از فضای نام استاندارد System.Security.Cryptography تولید کنیم، باید به encoding رشته دریافتی حتما دقت داشت؛ در غیر اینصورت نتایج یکسان نخواهند بود.
مهم‌ترین encoding های پشتیبانی شده در دات نت در جدول زیر برشمرده شده‌اند:

Encoding	تعداد بیت هر کاراکتر
ASCII	هر کاراکتر آن 7 بیت است
UTF7	هر کاراکتر آن 7 بیت است
UTF8	هر کاراکتر آن 8 بیت و یا یک بایت است
Unicode (UTF-16)	هر کاراکتر آن 16 بیت و یا دو بایت است
UTF32	هر کاراکتر آن 32 بیت و یا 4 بایت است

نوع nvarchar در اس کیوال سرور همانند حالت Encoding.Unicode دات نت است و هر کاراکتر آن 2 بایت می‌باشد.
این نکته هنگام استفاده از این توابع بسیار حائز اهمیت است. برای مثال اگر تابع HashBytes اس کیوال سرور را بخواهیم در دات نت پیاده سازی کنیم، به کلاس زیر خواهیم رسید:

```
using System.Text;
using System.Security.Cryptography;

class CHash
{
public static string GetMD5Hash(string input, Encoding encoding)
{
    byte[] bytes = new MD5CryptoServiceProvider().ComputeHash(encoding.GetBytes(input));
    StringBuilder chars = new StringBuilder();
    foreach (byte chr in bytes)
    {
        chars.Append(chr.ToString("x2"));
    }
    return chars.ToString();
}
}
```

در اینجا تنها حالت زیر با هش تولید شده یک فیلد یا متغیر از نوع nvarchar توسط تابع HashBytes اس کیوال سرور معادل است:

```
string result = CHash.GetMD5Hash("وحید", Encoding.Unicode);
```

پ.ن.
احتمالا عده‌ای را دیده‌اید که هر چقدر تلاش می‌کنند با سی شارپ متون ایران سیستم تحت داس را به نمونه‌های ویندوزی تبدیل کنند، کمتر موفق می‌شوند؛ علت را با توجه به جدول encoding فوق و عدم اطلاع از آن بهتر می‌توان بررسی کرد.

نظرات خوانندگان

نویسنده: Anonymous
تاریخ: ۱۳۸۸/۰۲/۱۵ ۰۰:۱۴:۰۰

با عرض سلام
آقای نصیری حدودا 2 3 سال پیش با خوندن کتاب شما و آقای هاشمیان با دات نت آشنا شدم بعد از مدتها وبلاگ شما رو بصورت اتفاقی پیدا کردم(ضمنا همچنا دنبال وبلاگ و یا... از آقای هاشمیان هستم) شما 2 نفر حق معلمی گزدن من دارید امیدوارم بتونم یه روز جبران کنم
قبل از هر چیز از شما بخاطر بروز نگه داشتن وبلاگتون تشکر میکنم
و اما سوال و درخواستی دارم
سوال
1:برای هش کردن پسورد از همین تابع ی که معرفی کردید (در قالب تریگر)استفاده کنم یا از توابع دات نت

پیشنهاد

2:اگه امکانش هست درباره وب سرویس ها هم تاپیک داشه باشید مخصوصا تکنولوژی جدید دات نت WCF

ممنون از توجهتون

نویسنده: وحید نصیری
تاریخ: ۱۳۸۸/۰۲/۱۵ ۰۰:۵۲:۰۰

سلام،
- شما لطف دارید.
- بر روی select نمی‌شود تریگر تعریف کرد بنابراین ...
و در کل فرقی نمی‌کند. یا یک رویه ذخیره شده بنویسید و کل عملیات را در آن پیاده کنید و سپس مثلا یک 0 یا 1 یا true یا false بازگشت دهید که شخص یوزر نیم و پسورد درستی وارد کرده (در این حالت می‌شود از روش اس کیوال سرور استفاده کرد برای هش کردن پسورد وارد شده و سپس مقایسه)
یا پسورد را هش کنید (توسط کلاینت دات نتی) و سپس با نمونه موجود در دیتابیس مقایسه کنید.
هر دو راه قابل انجام است و تفاوتی هم ندارد.
روش رویه ذخیره شده بهینه‌تر است و بدلیل کامپایل شدن سریعتر هم خواهد بود.

نویسنده: Mohammad Shams Javi
تاریخ: ۱۳۸۸/۰۲/۱۵ ۰۹:۰۹:۰۰

متشکرم
جالب بود

نویسنده: فاتحی
تاریخ: ۱۳۸۸/۰۲/۱۵ ۱۲:۱۲:۰۰

البته در استفاده از رویه ذخیره شده سمت sql این امکان وجود دارد که رمزعبور توسط SQL Profiler رصد شود!
و کلا پسورد هش نشده به دیتابیس پاس می شود.
جا داره منم از زحمات و مطالب شما تشکر و سپاس گذاری کنم.

نویسنده: وحید نصیری
تاریخ: ۱۳۸۸/۰۲/۱۵ ۱۴:۳۷:۰۰

البته کسی که دسترسی به SQL Profiler دارد یعنی دسترسی در حد برنامه نویس یا مدیر سیستم به او اعطاء شده و کلا باید به این دو اطمینان کرد چون در غیر اینصورت واقعا کارکردن مشکل خواهد شد.

نویسنده: حمیدرضا
تاریخ: ۱۳۸۸/۰۲/۱۵ ۱۷:۵۷:۰۰

اگه اشتباه نفهمیده باشم تعداد بایتهای یک کاراکتر توی استاندارد UTF-8 حداقل یک بایته (متغیره)، توی همون لینکی دادید نوشته 1 تا 4 بایت.

نویسنده: وحید نصیری
تاریخ: ۱۳۸۸/۰۲/۱۵ ۱۹:۴۸:۰۰

درسته. جدول حداقل و حداکثر رو میشه در سایت زیر هم دید:
http://unicode.org/faq/utf_bom.html
ولی برای این حداقل‌ها و حداکثرها، اما و اگرهای زیادی هست (در مورد عدم تداخل با یکدیگر) که در لینک‌های زیر توضیح داده شده:
http://en.wikipedia.org/wiki/UTF-8
http://tools.ietf.org/html/rfc3629

رشته‌ها در دات نت فریم ورک از نوع UTF-16 هستند و برای اینکه به صورت صحیحی تبدیل به آرایه‌ای از بایت‌ها شده و در الگوریتم‌های مورد نظر استفاده شوند باید به این نکته دقت داشت.