

Re: protect passwords in database

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.languages.csharp/2006-08/msg01224.html>

- *From:* John B <jbngspam@xxxxxxxxxx>
 - *Date:* Fri, 04 Aug 2006 10:04:02 +1000
-

Jon Skeet [C# MVP] wrote:

John B <jbngspam@xxxxxxxxxx> wrote:

Out of curiosity, what weaknesses? My FreeBSD boxes use them to great effect.

md5 has been proven to have collisions. ie two values producing the same hash.

All hash codes will have collisions. That much is clear just from the pigeon-hole principle. The concern isn't that there **are** collisions – it's that they can be engineered deliberately.

Agreed, sorry.

From what I remember of the MD5 "hole", it wouldn't actually help anyone to break into such a system. Of course, it's worth researching what the hole actually is rather than just taking my word for it.

In an interesting side note, the md5 'weakness' was actually used in a defense against a traffic notice here in Australia recently.

A picture was taken, md5 hash generated for it and the person driving argued in court that since md5 was 'broken' it was invalid.

The traffic authority was given a period of time to produce expert witnesses to refute this claim and since they didn't, the case was thrown out. :)

JB

.