- ✓ Database management systems are nearly as complex as the operating systems on which they reside.
- ✓ As a security professional, there is need to assess and manage any potential security problems.
- ✓ Following are the Vulnerabilities in database management systems
  - ➢ **Loose access permissions.** Like applications and operating systems, database management systems have schemes of access controls that are often designed far too loosely, which permits more access to critical and sensitive information than is appropriate. This can also include failures to implement cryptography as an access control when appropriate.
  - ➢ **Excessive retention of sensitive data.** Keeping sensitive data longer than necessary increases the impact of a security breach.
  - ➢ **Aggregation of personally identifiable information.** The practice known as aggregation of data about citizens is a potentially risky undertaking that can result in an organization possessing sensitive personal information.

Sometimes, this happens when an organization deposits historic data from various sources into a data warehouse, where this disparate sensitive data is brought together for the first time. The result is a gold mine or a time bomb, depending on how you look at it.

Best practices for minimizing database security risks

- ✓ While some attackers still focus on denial of service attacks, cyber criminals often target the database because that is where the money is.
- ✓ The databases that power web sites hold a great deal of profitable information for someone looking to steal credit card information or personal identities.
- ✓ Database security on its own is an extremely in-depth topic that could never be covered in the course of one article; however there are a few best practices that can help even the smallest of businesses secure their database enough to make an attacker move on to an easier target.

Separate the Database and Web Servers

- Keep the database server separate from the web server.
- When installing most web software, the database is created for you. To make things easy, this database is created on the same server where the application itself is being installed, the web server. Unfortunately, this makes access to the data all too easy for an attacker to access.
- If they are able to crack the administrator account for the web server, the data is readily available to them.
- Instead, a database should reside on a separate database server located behind a firewall, not in the DMZ (Demiltarized Zone) with the web server. While this makes for a more complicated setup, the security benefits are well worth the effort.

Encrypt Stored Files

- Encrypt stored files.
- White Hat security estimates that 83 percent of all web sites are vulnerable to at least one form of attack.
- The stored files of a web application often contain information about the databases the software needs to connect to.
- This information, if stored in plain text like many default installations do, provide the keys an attacker needs to access sensitive data.

Encrypt Your Backups Too

- Encrypt back-up files.
- Not all data theft happens as a result of an outside attack. Sometimes, it's the people we trust most that are the attackers.

Use a WAF

- Employ web application firewalls.
- The misconception here might be that protecting the web server has nothing to do with the database.

Keep Patches Current

- Keep patches current. This is one area where administrators often come up short.
- Web sites that are rich with third-party applications, widgets, components and various other plug-ins and add-ons can easily find themselves a target to an exploit that should have been patched.

Minimize Use of 3rd Party Apps

- Keep third-party applications to a minimum.
- We all want our web site to be filled with interactive widgets and sidebars filled with cool content, but any app that pulls from the database is a potential threat.
- Many of these applications are created by hobbyists or programmers who discontinue support for them.

Don't Use a Shared Server

- Avoid using a shared web server if your database holds sensitive information.
- While it may be easier, and cheaper, to host your site with a hosting provider you are essentially placing the security of your information in the hands of someone else.
- If you have no other choice, make sure to review their security policies and speak with them about what their responsibilities are should your data become compromised.

Enable Security Controls

- Enable security controls on your database.
- While most databases nowadays will enable security controls by default, it never hurts for you to go through and make sure you check the security controls to see if this was done.
- Keep in mind that securing your database means you have to shift your focus from web developer to database administrator. In small businesses, this may mean added responsibilities and additional buy in from management.
- However, getting everyone on the same page when it comes to security can make a difference between preventing an attack and responding to an attack.