Introduction to Structured Query Language (SQL). Database Security

UMKC

School of Medicine

Database Security

- Keep security controls of database server on maximum
  - Run the most up-to-date version of your database software to remove vulnerabilities.
  - Turn on all security protocols and controls of your database and website server
    - unless there is a specific and necessary reason that one should be turned off.
  - Delete or disable any features you are not using and do not need.
  - Change all default passwords to prevent unauthorized users from logging in.

Database Security

- Update patches
  - If your database or website uses widgets, plugins and other third-party apps, cyber criminals will often target these in order to bypass your database security
  - Especially if they haven’t been patched or updated on a regular basis.
  - Even if your internal defenses are strong, these third-party additions can create weaknesses.
  - Update patches as soon as they become available to keep all of the defenses strong.
  - Audit your database to check security

Database Security

- Separate servers and web servers
    - It is best practice to separate your database server from your website server.
    - Keeping your servers separate will increase the cyber security of your database server and website
    - If a hacker cracks your web server admin account, they won’t be able to access your database.
    - While database servers may need to communicate with web servers at times, ensure that their permissions are confined to the lowest level of privilege needed in order for them to operate successfully.
    - This will limit the scope of damage an attacker can implement.

Database Security

- Encrypt all files and backups
  - Cyber criminals aren’t the only threat to your database security.
  - Employees could be a significant risk too. There is always the chance that an employee will access a file they don’t have permission to.
  - Encrypting your data makes it unreadable to both hackers, and employees without an encryption key.
  - Encryption is a final line of defense against unwanted intrusions.
  - Encrypt all important documents, files, and backups to keep your critical data unreadable to unauthorized users.

Database Security

- Configure a database firewall and web application firewall in place
  - Firewalls enhance database security by denying traffic by default to minimize the entrance of threats.
  - Firewall should only allow traffic from specific applications and web servers that need to access the data
  - Prevent your database from initiating outbound connections (aside from those that are necessary).
  - Web application firewall helps protect web servers and increases database security.
  - Without one, web application attacks could be used to delete or collect data from the database.

Database Security

- **Questions**