1. **Which least amount of permissions granted will access the dynamic management**

**view.**

In MS SQL Server, the most basic permissions that are granted to the user by default while providing access to dynamic management views (DMVs) would be VIEW SERVER STATE authority. This permitter facilitates your ability to access the server's wide-area state information including viewing the DMVs. Issuing this authority helps users view this information as well as the life cycle of the data at the time, which will be useful for querying attribute data.

1. **Consider that you have a web site that connects to a sales database. Some of the SQL queries are embedded in the page. What security threat, if any, are you most likely to face?**

In the foregoing context, the greatest security threat might be SQL injection (SQLI). In code injection, attackers inject SQL code into text boxes and URL parameters which will result in exploitation of vulnerabilities, damages to the system. Through a vulnerability in the sales database, they may, by the queries they execute and the manipulations of these searches, attempt to obtain unauthorized access to the data in the sales database. SQL injection is a technical term that generally carries substantial outcomes, such as permissioned data access, data manipulation, and even service denial due to web application trying to carry out resource-demanding queries. The existing threat can be reduced by vigorous implementation of security measures like facilitating parameterized queries or prepared statements, executing input validations and sanitization, establishing the least privilege rule, and conducting security audits and penetration testing periodically so as to detect any vulnerabilities. Such preventive practices provide shield for getting SQL injection breaches and augmenting the total state of security in the website along with its related database.

1. Using GRANT/REVOKE for roles is the best option for efficient and consistent access control in databases.