Investigate Database Architecture Issues

```
# Question 1
## What are cursors? Why are they useful in application architectures? What are some of the benefits? A
```

Cursors are pointers to a specific row in a database query. Cursors allow programmers to iterate the result of a query row by row instead of processing the entire resulting set all at once. [*Introduction to database systems.* Delhi: Pearson, 2010.] Benefits of using cursors: when making updates concurrency problems may occur if we use multiple SQL update statements. With a cursor, we are updating row by row and thus would avoid any potential concurrency problems. Drawbacks of using cursors: The use of cursors may require more memory from the computer than without. The utilization of cursors may also be slower than a simple SELECT statement. The syntax for cursors are embedded into MYSQL and SQLite.["MySQL 8.0 Reference Manual :: 13.6.6 cursors," *MySQL.* [Online]. Available: https://dev.mysql.com/doc/refman/8.0/en/cursors.html. [Accessed: 03-Dec-2022].] Cursors can be created using the "DECLARE" and "CURSOR" keyword. For example: "DECLARE CURSOR". It can then be opened using the "OPEN" keyword, and closed using the "CLOSE" keyword. [*Introduction to database systems.* Delhi: Pearson, 2010.]

```
# Question 2
## What are connection pools? Why are they useful in application architectures? What are some of the be
```

When utlizling a database, we usually have to open a connection to the database, perform a set of operations, and then close the connection to that database. Connection pools is a way to maintain a collection of open connections which can be used and reused. ["What is connection pooling, and why should you care," Cockroach Labs, 30-Nov-2021. [Online]. Available: https://www.cockroachlabs.com/blog/what-is-connection-pooling/. [Accessed: 03-Dec-2022].] The benefits of a connection pool is that we set it up once and we do not need to open a connection every time we want to connect to a database, this limits latency and storage space that would be needed to create a new connection. The drawback is that keeping idle connections open in the connection pool when they are not in use is also costly in terms of space and processing power. Thus, a balance is needed to find the right amount of connections to keep in the pool.

```
# Question 3
## 800 - 1000 word review of the two articles (combine the two reviews; do not write two separate revie
```

Both articles talk about the dangers of SQL injection attacks (SQLIAs) and the methods used to try to prevent them.

Some key take-aways that both articles list for prevention are "sensitive data should be encryptedin the database"[J. O. Atoum and A. J. Qaralleh , "A HYBRID TECHNIQUE FOR SQL INJECTION ATTACKS DETECTION AND PREVENTION ," International Journal of Database Management Systems (IJDMS), vol. 6, no. 1, Feb. 2014.] Things like passwords, user names, credit card account numbers, should be encrpyted.

Another take-away is to be mindful of error messages displayed to the user. Error messages can give attackers information on how the database schema was constructed, or what table names exist in the database, etc. As mentioned by Halfond, W. G., Viegas, J., & Orso, A., "In fact, the simple fact that an error messages is generated can often reveal vulnerable/injectable parameters to an attacker. Additional error information, originally intended to help programmers debug their applications, further helps attackers gain information about the schema of the back-end database."[J. O. Atoum and A. J. Qaralleh , "A HYBRID TECHNIQUE FOR SQL INJECTION ATTACKS DETECTION AND PREVENTION ," International Journal of Database Management Systems (IJDMS), vol. 6, no. 1, Feb. 2014.]

Some prevention of SQLIAs techniques mentioned by both articles is the thought of checking user input for

SQL keywords and reject it if it looks like an SQL command.

Both articles also mention taking a hybrid approach of "Static and Dynamic Analysis" where errors are first statically evaluated and then evaluated again during the runtime of the query. [Halfond, W. G., Viegas, J., & Orso, A. (2006, March). A classification of SQL-injection attacks and countermeasures. In Proceedings of the IEEE international symposium on secure software engineering (Vol. 1, pp. 13-15). IEEE.]

While both articles describe SQLIAs and how they work. the article by Halfond, W. G., Viegas, J., & Orso, A. gives a better overview of best methods to prevent them. J. O. Atoum and A. J. Qaralleh, offer their own method for SQLIA prevention. Their approach is to replicate the database and create and additional "database_Behaviors" database and redirect the SQL queries to that database prior to executing it on the main database. As I am unexprierienced in this field, I am uncertain if that is the best approach as it seems costly to replicate the entire database.