Vulnerability Name: SQL Injection.

Description:
SQL Injection is a code injection technique that might destroy a database. It is one of the most common web hacking techniques. This attack allows the execution of malicious SQL statements, potentially allowing unauthorized access to sensitive data.

Vulnerable URL: https://www.bishopwalsh.edu.hk/news_detail.php?id=59

Example Code:
```
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
```

Steps to Reproduce:
- Append a single quote (') to the end of the URL parameter.
- Observe any SQL-related error messages.
- Use a tool such as HAVIJ to further analyze the database structure:
  ➔ Analyze → Get Tables → Select Admin DB → Get Columns → Select Passwd → Get Data

Impact:
Successful exploitation can result in:
- Unauthorized access to database contents
- Data leakage, deletion, or modification
- Escalation of privileges

Mitigation:
- Use parameterized queries or prepared statements
- Avoid dynamic SQL using string concatenation
  Sanitize and validate all user inputs

Reference: https://www.w3schools.com/sql/sql_injection.asp

Proof of Concept (POC):