

**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](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](https://www.w3schools.com/sql/sql_injection.asp)

## Proof of Concept (POC):

The screenshot displays the Havij application window. At the top, the 'Target' field is set to `http://www.bishopwalsh.edu.hk/news_detail.php?id=59`. The 'Keyword' and 'Syntax' fields are both set to 'Auto Detect'. The 'Data Base' is set to 'Auto Detect', the 'Method' is 'GET', and the 'Type' is 'Auto Detect'. The 'Analyze' button is visible on the right.

Below the configuration fields is a toolbar with icons for 'About', 'Info', 'Tables', 'Read Files', 'Cmd Shell', 'Query', 'Find Admin', 'MDS', and 'Settings'. The 'Tables' icon is selected, and the 'Get Tables' button is highlighted in the main toolbar.

The main workspace is divided into two panes. The left pane shows a tree view of the database schema with the following items checked:

- ☒ verse
- ☒ usr
- ☐ usr\_pwd\_mod\_usr\_id
- ☐ usr\_pwd\_mod\_ip
- ☐ usr\_pwd\_mod\_dt
- ☒ usr\_pwd
- ☐ usr\_email
- ☒ usr\_name
- ☐ usr\_login\_name
- ☐ usr\_st
- ☐ usr\_fixed
- ☐ usr\_sort\_id
- ☐ usr\_sort\_lv
- ☐ usr\_login\_fail\_ct

At the bottom of the left pane, the options 'Use Group\_Concat (MySQL Only)' and 'All in one request' are visible, with 'Use Group\_Concat (MySQL Only)' selected.

The right pane displays the results of the 'Get Tables' operation, showing a table with two columns: 'usr\_name' and 'usr\_pwd'. The data rows are:

| usr_name      | usr_pwd                                  |
|---------------|------------------------------------------|
| Administrator | 293453210e7f684714d3e1c92ed2ffff77400752 |
| EastTech      | 42971234f44b567813955235245b2497399d7a93 |
| SystemCreate  |                                          |
| UserModify    |                                          |
| Init          |                                          |

Below the panes is a status bar showing 'Status: I'm IDLE' and a 'Clear Log' button. A log window at the bottom displays the following messages:

```
Turning off 'bypass illegal union' and retrying!  
Data Found: usr_pwd=  
Data Found: usr_name=UserModify  
Turning on 'bypass illegal union' and retrying!  
Data Found: usr_pwd=  
Data Found: usr_name=Init  
Turning off 'bypass illegal union' and retrying!  
Data Found: usr_pwd=
```

The Windows taskbar at the bottom shows the system clock as 2:30 AM on 4/12/2025, with a temperature of 22°C and 'Mostly clear' weather.