

BSIS 2

SCENARIO 1

The bug happens kasi the code is expecting a POST variable, pero ang value kasi is sent via GET sa URL. Using `$_GET` ensures na ma-read ng script yung tamang parameter.

SCENARIO 2

SQL needs string values to be inside quotes. Kung wala quotes, MySQL thinks na column name siya, kaya lalabas yung "Unknown column" error

SCENARIO 3

Pag direct mong in-insert yung GET values sa SQL, pwede ka ma-expose sa SQL injection. Using prepared statements makes sure safe yung input at hindi maka-inject yung hacker.

SCENARIO 4

Blank data sa database can mess things up or cause errors. Validation ensures na may laman yung required fields bago mo i-INSERT sa SQL.

SCENARIO 5

Kung may typo yung POST key, PHP won't read the input, tapos lalabas yung undefined index error. Correcting the key ensures na ma-capture yung email properly.

SCENARIO 6

Using raw GET values sa DELETE query is super dangerous—pwede ma-delete lahat ng records. Casting to int limits deletion sa specific ID lang at prevents SQL injection.

SCENARIO 7

Even pag SQL fails, script pa rin nagsasabi ng "Updated!" kasi walang error checking. Adding proper error handling makes sure na hindi ka nag-fe-fake ng success.

SCENARIO 8

`mysqli_fetch_assoc` only reads one row per call. Kailangan mo siya i-loop para ma-output lahat ng records from the query.

SCENARIO 9

The link triggers GET, pero script was reading POST. Change script to \$_GET para match sa actual request method.

SCENARIO 10

Undefined variable = PHP warning at broken SQL query. Fix yung variable name para ma-access ng tama yung user input.

SCENARIO 11

Form sends GET pero PHP reads POST, kaya nawawala yung data. Make sure both sides are either GET or POST para ma-receive yung variable

SCENARIO 12

IDs are numeric—dapat hindi naka-quote sa SQL. Remove quotes or cast to int for better performance at to prevent type confusion.

SCENARIO 13

Walang WHERE clause sa UPDATE, lahat ng rows maa-affect. Add WHERE para only yung intended record lang yung ma-update.

SCENARIO 14

Array keys need proper quotes at string values din. Fix both para valid at safe yung SQL query.

SCENARIO 15

Users can input crazy page numbers, tapos ang offset magiging sobrang huge—pwede ma-slow or crash database. Validate at restrict page number para safe.