



ISO 9001: 2015
SOCOTEC SCP000722Q

REPUBLIC OF THE PHILIPPINES
BICOL UNIVERSITY
POLANGUI

Polangui, Albay

Email: bupc-dean@bicol-u.edu.ph



Name: Lozano, Eunice L

Course & Block: BSIS – 2

Subject: IS Elec 2 - Web Systems

Professor: Reymar Llagas

Troubleshooting Exercise

SCENARIO	PROBLEM	Correct Fix
1	Using \$_POST instead of \$_GET	Use GET because the ID is coming from the URL.
2	Missing quotes around a string value in SQL	Add single quotes around the first name since it is text.
3	SQL injection risk from direct user input	Use a prepared statement to safely filter by age.
4	Inserts data even when form fields are empty	Add input validation to check if fields are not empty before inserting.
5	Wrong POST key (emial instead of email)	Use the correct key name that matches the form field.
6	Unsafe delete using raw GET input	Use intval() or a prepared statement to sanitize the ID before deleting.
7	Update query fails but still prints “Updated!”	Add error checking and ensure the email is properly quoted.
8	Only one record prints because fetch is called once	Use a while loop to display all rows from the query.
9	Using POST even though the link sends GET	Change to GET since links always pass data through the URL.
10	Wrong variable name used in SQL (aeg instead of age)	Use the correct variable name in the query.
11	Form sends GET but PHP reads POST	Make the form method match the PHP superglobal being used.
12	Numeric ID placed inside quotes	Remove the quotes or convert the value to an integer before using it.
13	Missing WHERE clause in UPDATE (updates all rows)	Add a WHERE clause to update only the specific record.
14	Wrong formatting of POST array values in SQL	Use the correct array access and wrap text values in quotes.
15	GET page number not validated, causing huge offsets	Validate and limit the page number to prevent large or harmful values.

Explanation:	Scenario
<ul style="list-style-type: none"> - Kung galing sa URL yung data, GET talaga ang dapat gamitin. POST ginagamit lang kapag form ang nag-send. 	Scenario 1
<ul style="list-style-type: none"> - Yung name (like “Ana”) ay text, so dapat naka-quotes sa SQL. Pag walang quotes, iniisip ng database column name siya, kaya error. 	Scenario 2
<ul style="list-style-type: none"> - Diretsong nilalagay ang GET value sa query, kaya pwedeng magpasok ng harmful code (ex. 1 OR 1=1). Kaya kailangan prepared statement para safe. 	Scenario 3
<ul style="list-style-type: none"> - I-check muna kung may laman yung input. Para iwas sa blank or incomplete na data. 	Scenario 4
<ul style="list-style-type: none"> - Mali ang spelling ng key (emial), kaya hindi makuha yung value. Dapat eksaktong match sa name attribute ng form. 	Scenario 5
<ul style="list-style-type: none"> - intval() ensures number lang, so hindi pwedeng maglagay ng 1 OR 1=1. 	Scenario 6
<ul style="list-style-type: none"> - Kailangan i-check kung nag-succeed yung query bago mag-print ng success message. 	Scenario 7
<ul style="list-style-type: none"> - mysqli_fetch_assoc() gets only one row. Kung gusto lahat ng records, kailangan ng while loop para ma-loop bawat row.. 	Scenario 8
<ul style="list-style-type: none"> - Link (<a href>) always uses GET, kaya kung POST ang ginamit sa PHP, hindi niya makukuha yung id. Dapat GET ang gamitin. 	Scenario 9
<ul style="list-style-type: none"> - Mali yung variable (\$aeg). Dapat \$age. Kapag mali ang spelling, undefined siya at hindi gagana yung query. 	Scenario 10
<ul style="list-style-type: none"> - Form sends GET pero PHP naghahanap ng POST. Magkaka-undefined index. Dapat mag-match yung method at superglobal na ginagamit. 	Scenario 11
<ul style="list-style-type: none"> - Numbers don't need '' kasi di sila text. Mas efficient if walang quotes. 	Scenario 12
<ul style="list-style-type: none"> - Walang WHERE, kaya lahat ng rows maa-update. Dapat laging may WHERE para specific lang ang ma-update. 	Scenario 13
<ul style="list-style-type: none"> - Strings kailangan naka-quotes, at dapat tama ang syntax ng array keys. Without correct quotes, magiging invalid ang SQL. 	Scenario 14
<ul style="list-style-type: none"> - Nililimit ang allowed page number para hindi bumagsak ang system. 	Scenario 15