Advanced SQL Injection

Patch SQL Injection

Patch the SQL Injection !

- Patch the SQL Injection vulnerability in the code below

```php
<?php
if( isset( $_POST[ 'Submit' ] ) ) {

    // Get input

    $id = $_POST[ 'id' ];
    $con = mysqli_connect("localhost","my_user","my_password","my_db");
    $id = mysqli_real_escape_string($con, $id);
    $query  = "SELECT first_name, last_name FROM users WHERE user_id = $id;";
    $result = mysqli_query($con, $query) or die( '<pre>' . mysqli_error($con) . '</pre>' );

    // Get results

    while( $row = mysqli_fetch_assoc( $result ) ) {

        // Display values

        $first = $row["first_name"];
        $last  = $row["last_name"];

        // Feedback for end user

        echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
    }
}

// This is used later on in the index.php page
// Setting it here so we can close the database connection in here like in the rest of the source scripts

$query  = "SELECT COUNT(*) FROM users;";
$result = mysqli_query($con,  $query ) or die( '<pre>' . ((is_object($con)) ? mysqli_error($con) : (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );
$number_of_rows = mysqli_fetch_row( $result )[0];
mysqli_close($con);
?>
```


ZDResearch

Download Code

Patch the SQL Injection ! - Solution

- In this example preventing SQL Injection is straightforward
- We have to only allow an integer in the query

```php
<?php
if( isset( $_POST[ 'Submit' ] ) ) {
    // Get input
    $id = $_POST[ 'id' ];
    $con = mysqli_connect("localhost","my_user","my_password","my_db");

    $id = mysqli_real_escape_string($con, $id); // this is not enough, as we are not inside a string

    $id = $id*1; // only allow numbers, remove everything else.

    $query  = "SELECT first_name, last_name FROM users WHERE user_id = $id;";
    $result = mysqli_query($con, $query) or die( '<pre>' . mysqli_error($con) . '</pre>' );

    // Get results
    while( $row = mysqli_fetch_assoc( $result ) ) {
        // Display values
        $first = $row["first_name"];
        $last  = $row["last_name"];

        // Feedback for end user
        echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
    }

}

// This is used later on in the index.php page
// Setting it here so we can close the database connection in here like in the rest of the source scripts
$query  = "SELECT COUNT(*) FROM users;";
$result = mysqli_query($con,  $query ) or die( '<pre>' . ((is_object($con)) ? mysqli_error($con) : (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );
$number_of_rows = mysqli_fetch_row( $result )[0];

mysqli_close($con);
?>
```

[Download Code]

ZDResearch

ZDResearch Advanced Web Hacking

ZDResearch

www.zdresearch.com