

Advanced SQL Injection

Patch SQL Injection



ZDResearch

www.zdresearch.com

ZDResearch Advanced Web Hacking

Patch the SQL Injection !

- Patch the SQL Injection vulnerability in the code below

```
1 <?php
2 if( isset( $_POST[ 'Submit' ] ) ) {
3
4     // Get input
5
6     $id = $_POST[ 'id' ];
7     $con = mysqli_connect("localhost","my_user","my_password","my_db");
8     $id = mysqli_real_escape_string($con, $id);
9     $query = "SELECT first_name, last_name FROM users WHERE user_id = $id;";
10    $result = mysqli_query($con, $query) or die( "<pre>' . mysqli_error($con) . '</pre>' );
11
12    // Get results
13
14    while( $row = mysqli_fetch_assoc( $result ) ) {
15
16        // Display values
17
18        $first = $row[ "first_name" ];
19        $last = $row[ "last_name" ];
20
21        // Feedback for end user
22
23        echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
24    }
25 }
26
27 // This is used later on in the index.php page
28 // Setting it here so we can close the database connection in here like in the rest of the source scripts
29
30 $query = "SELECT COUNT(*) FROM users;";
31 $result = mysqli_query($con, $query) or die( '<pre>' . ((is_object($con)) ? mysqli_error($con) : (($__mysqli_res = mysqli_connect_error()) ? $
    __mysqli_res : false)) . '</pre>' );
32 $number_of_rows = mysqli_fetch_row( $result )[0];
33 mysqli_close($con);
34 ?>
35
```

Patch the SQL Injection ! - Solution

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

```
1 <?php
2 if( isset( $_POST[ 'Submit' ] ) ) {
3     // Get input
4     $id = $_POST[ 'id' ];
5     $con = mysqli_connect("localhost","my_user","my_password","my_db");
6
7     $id = mysqli_real_escape_string($con, $id); // this is not enough, as we are not inside a string
8
9     $id = $id*1; // only allow numbers, remove everything else.
10
11     $query = "SELECT first_name, last_name FROM users WHERE user_id = $id;";
12     $result = mysqli_query($con, $query) or die( '<pre>' . mysqli_error($con) . '</pre>' );
13
14     // Get results
15     while( $row = mysqli_fetch_assoc( $result ) ) {
16         // Display values
17         $first = $row["first_name"];
18         $last = $row["last_name"];
19
20         // Feedback for end user
21         echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
22     }
23 }
24 }
25
26 // This is used later on in the index.php page
27 // Setting it here so we can close the database connection in here like in the rest of the source scripts
28 $query = "SELECT COUNT(*) FROM users;";
29 $result = mysqli_query($con, $query) or die( '<pre>' . ((is_object($con)) ? mysqli_error($con) : (( $__mysqli_res = mysqli_connect_error()) ? $
    __mysqli_res : false)) . '</pre>' );
30 $number_of_rows = mysqli_fetch_row( $result )[0];
31
32 mysqli_close($con);
33 ?>
34
```

[Download Code](#)

Exdemy.com
Personal property of Keith Samborski
_my69@yahoo.com



ZDRResearch Advanced Web Hacking

ZDRResearch

www.zdresearch.com

Copyright © Exdemy.com