

Security level is medium.

This is how it looks like.

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

Sign Guestbook

Clear Guestbook

Name: test

Message: This is a test comment.

More Information

- <https://owasp.org/www-community/attacks/xss>
- <https://owasp.org/www-community/attacks/xss#filter-avoidance-cheat-sheet>

By reviewing the webpage, the length of the fields are 10 and 50 letters.

```
<table border="1">
  <tbody>
    <tr>
      <td width="100">Name *</td>
      <td>
        <input name="txtName" type="text" size="30" maxlength="10">
      </td>
    </tr>
    <tr>
      <td width="100">Message *</td>
      <td>
        <textarea name="mtxMessage" cols="50" rows="3" maxlength="50">
        </textarea>
      </td>
    </tr>
  </tbody>
</table>
```

We can simply change the size of the inputs.

```

        <td>
            <input name="txtName" type="text" size="30" maxlength="1000">
        </td>
    </tr>
    <tr>
        <td width="100">Message *</td>
        <td>
            <textarea name="mtxMessage" cols="50" rows="3" maxlength="5000">
            </textarea> == $0
        </td>
    </tr>
    <tr>...</tr>
</tbody>
</table>
// form

```

After we can try to insert our code here. I will put some script to redirect users to the bcit.ca page. But before that, as we see the source code of JS. We can see that Name field replaces <script> from our input.

```

<?php
if( isset( $_POST[ 'btnSign' ] ) ) {
    // Get input
    $message = trim( $_POST[ 'mtxMessage' ] );
    $name = trim( $_POST[ 'txtName' ] );

    // Sanitize message input
    $message = strip_tags( addslashes( $message ) );
    $message = ((isset($GLOBALS["__mysqli_ston"]) && is_object($GLOBALS["__mysqli_ston"])) ? mysqli_real_escape_string($GLOBALS["__mysqli_ston"], $message) : [MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.);
    $message = htmlspecialchars( $message );

    // Sanitize name input
    $name = str_replace( '<script>', '', $name );
    $name = ((isset($GLOBALS["__mysqli_ston"]) && is_object($GLOBALS["__mysqli_ston"])) ? mysqli_real_escape_string($GLOBALS["__mysqli_ston"], $name) : [MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.);

    // Update database
    $query = "INSERT INTO guestbook ( comment, name ) VALUES ( '$message', '$name' );";
    $result = mysqli_query($GLOBALS["__mysqli_ston"], $query ) or die( '<pre>' . ((isset($GLOBALS["__mysqli_ston"])) ? mysqli_error($GLOBALS["__mysqli_ston"]) : [MySQLConverterToo] Fix the mysql_error() call! This code does not work.) );

    //mysql_close();
}

```

Vulnerability: Stored Cross Site Scripting (XSS)


Name *

Message *

British Columbia Institute of Technology

https://www.bcit.ca

BCIT



Your studies, your way.

Flexible learning for a complex world.

Register now >

Welcome to BCIT

ENG

2:51 PM

2024-12-05