





**- In the <body> :** echo "<article class=\"textblock2a\" contenteditable=\"true\" onBlur=\"saveToDatabase(this,'".$row[9]."','text1','tbl\_text')\">".stripslashes($row[3])."</article>\n";

**- On save it uses following javascript :**

function saveToDatabase(editableObj, textid, textfield, tbl) {

if (!String.prototype.trim) {

String.prototype.trim = function () {

return this.replace(/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g, '');

};

}

var edithtml = editableObj.innerHTML;

var edithtml = edithtml.trim();

var edithtml = encodeURIComponent(edithtml);

$.ajax({

scriptCharset: "utf-8" ,

contentType: "application/x-www-form-urlencoded; charset=UTF-8",

url: 'textsave.php',

type: "POST",

data: 'action=text&text='+edithtml + '&textid='+textid + '&textfield='+textfield + '&tbl='+tbl,

success: function(data) {

}

});

}

**- In the script textsave.php :**

<?php

include\_once('../incl/inc\_path.php');

include\_once('incl\_public/inc\_config.php');

// if(isset($\_POST["text"]) && !empty(trim($\_POST["text"]))){$vartext = htmlspecialchars(trim($\_POST["text"]));}else{$vartext="";}

if(isset($\_POST["text"]) && !empty(trim($\_POST["text"]))){$vartext = trim($\_POST["text"]); } else{$vartext="";}

if(isset($\_POST["textid"]) && !empty(trim($\_POST["textid"]))){$vartextid = htmlspecialchars(trim($\_POST["textid"]));}else{$vartextid="";}

if(isset($\_POST["textfield"]) && !empty(trim($\_POST["textfield"]))){$vartextfield = htmlspecialchars(trim($\_POST["textfield"]));}else{$vartextfield="";}

if(isset($\_POST["action"]) && !empty(trim($\_POST["action"]))){$varlinkaction = htmlspecialchars(trim($\_POST["action"]));}else{$varlinkaction="";}

if(isset($\_POST["tbl"]) && !empty(trim($\_POST["tbl"]))){$vartbl = htmlspecialchars(trim($\_POST["tbl"]));}else{$vartbl="";}

if (isset($varlinkaction) && ($varlinkaction == "text") && ($vartbl === "tbl\_text") ){

if( !empty($vartextid) && !empty($vartextfield) ){

include\_once('includes/inc\_db.php');

include\_once('includes/inc\_cms\_functions.php');

$vartext = mysqli\_real\_escape\_string($mysqli,$vartext);

$vartext = preg\_replace("/&amp;/", "&",$vartext);

$vartext = htmlentities($vartext, ENT\_NOQUOTES);

$vartext = preg\_replace("/&lt;/", "<",$vartext);

$vartext = preg\_replace("/&gt;/", ">",$vartext);

$vartext = ctrlSQLinject($vartext);

$sql = "UPDATE tbl\_text SET ".$vartextfield."=? WHERE textid=?";

$parameters = array($vartext, $vartextid);

InsertDelUpdateDB($mysqli, $sql, $parameters);

$mysqli->close();

}

}

if (isset($varlinkaction) && ($varlinkaction == "text") && ($vartbl === "tbl\_config") ){

if( !empty($vartextid) && !empty($vartextfield) ){

include\_once('includes/inc\_db.php');

include\_once('includes/inc\_cms\_functions.php');

$vartext = mysqli\_real\_escape\_string($mysqli,$vartext);

$vartext = preg\_replace("/&amp;/", "&",$vartext);

$vartext = htmlentities($vartext, ENT\_NOQUOTES);

$vartext = preg\_replace("/&lt;/", "<",$vartext);

$vartext = preg\_replace("/&gt;/", ">",$vartext);

$vartext = ctrlSQLinject($vartext); // -> changes <script> into script without <> ...

$sql = "UPDATE tbl\_config SET ".trim($vartextfield)."=? WHERE configid=?";

$parameters = array($vartext, $vartextid);

InsertDelUpdateDB($mysqli, $sql, $parameters);

$mysqli->close();

}

}

?>