Mục lục

[1. Cài đặt XAMPP 4](#_Toc531809031)

[1.1 Lưu ý trong file Php.ini 4](#_Toc531809032)

[Cách 1: tác động trực tiếp vào file Php.ini 4](#_Toc531809033)

[Cách 2: dùng lệnh trong php để cấu hình 4](#_Toc531809034)

[2. Echo – Print 4](#_Toc531809035)

[3. Comment trong PHP 5](#_Toc531809036)

[3.1 Comment dòng đơn // hoặc # 5](#_Toc531809037)

[3.2 Comment đoạn văn 5](#_Toc531809038)

[4. Biến số trong PHP 5](#_Toc531809039)

[5. Các kiểu string 5](#_Toc531809040)

[5.1 Chiều dài string: strlen($string1) 5](#_Toc531809041)

[5.2 In hoa tất cả string: strtoupper($string2) 5](#_Toc531809042)

[5.3 In thường tất cả string: strtolower($string2) 5](#_Toc531809043)

[5.4 In hoa chữ đầu: ucfirst($string1) 5](#_Toc531809044)

[5.5 In hoa tất cả chữ đầu: ucwords($string1) 6](#_Toc531809045)

[5.6 String thay thế: str\_replace('biên', 'song', $string3) 6](#_Toc531809046)

[5.7 Cắt kí tự trong chuỗi: Substr($chuỗi, từ đâu, SoKitu) 6](#_Toc531809047)

[5.8 Đếm số kí tự trước giá trị cuối cùng cần tìm: strrpos($text, ‘ ’) 6](#_Toc531809048)

[6. Biến Constance 6](#_Toc531809049)

[7. Mảng Array 6](#_Toc531809050)

[7.1 Khai báo mảng, truy xuất phần tử 6](#_Toc531809051)

[7.2 Đếm số lượng phần tử trong mảng 7](#_Toc531809052)

[7.3 Giá trị lớn nhất, bé nhất, sắp xếp trong mảng 7](#_Toc531809053)

[7.4 Tách, gộp các phần tử trong mảng 7](#_Toc531809054)

[7.5 Lấy phần tử ngẫu nhiên, hiện thị phần tử 7](#_Toc531809055)

[8. Numbers và các hàm tính 8](#_Toc531809056)

[9. Vòng lặp 8](#_Toc531809057)

[9.1 Vòng lặp if … else… 8](#_Toc531809058)

[9.2 Vòng lặp switch 9](#_Toc531809059)

[9.3 Vòng lặp For 9](#_Toc531809060)

[9.4 Vòng lặp While 9](#_Toc531809061)

[10. Function 10](#_Toc531809062)

[10.1 Function trả lại 1 giá trị 10](#_Toc531809063)

[10.2 Function trả lại nhiều giá trị 10](#_Toc531809064)

[11. Fuction biến toàn cục 10](#_Toc531809065)

[12. Biến $\_POST 10](#_Toc531809066)

[13. Biến $\_GET 11](#_Toc531809067)

[14. IZWEBZ 11](#_Toc531809068)

[14.1 Query đếm số page trong CSDL để hiện trong <option> 11](#_Toc531809069)

[14.2 Query truy xuất Category trong CSDL để hiện trong <option> 11](#_Toc531809070)

[14.3 Query thêm dữ liệu vào CSDL và báo kết quả 11](#_Toc531809071)

[14.4 Kiểm tra Cid, Pid để in đậm tab đang chọn 13](#_Toc531809072)

[14.5 Hàm kiểm tra các giá trị nhập và truy vấn csdl 13](#_Toc531809073)

[15. ỨNG DỤNG CODE 14](#_Toc531809074)

[15.1 Tạo readmore cho đoạn văn 14](#_Toc531809075)

[15.2 Sử dụng dữ liệu ngoài cậu lệnh if && hiện titel để SEO 14](#_Toc531809076)

[15.3 Biến bài văn được chia ra từng đoạn 15](#_Toc531809077)

[15.4 Cắt đoạn nội dung dài thành đoạn ngắn để hiển thị 15](#_Toc531809078)

[15.5 Các cách chống spam 16](#_Toc531809079)

[**a)** Random question 16](#_Toc531809080)

[**b)** Honey pot 17](#_Toc531809081)

[**c)** Salt pot 17](#_Toc531809082)

[**d)** Dùng Recaptra 17](#_Toc531809083)

[15.6 Làm Contact Form 19](#_Toc531809084)

[15.7 Đăng ký thành viên bằng cách gửi mail để xác nhận 19](#_Toc531809085)

[15.8 Cách truy vấn cơ sở dữ liệu bằng Statement 21](#_Toc531809086)

[15.9 Sử dụng array kết hợp foreach để hiển thị 23](#_Toc531809087)

[15.10 Tránh ăn cắp SESSION Admin 23](#_Toc531809088)

[16. Các cách chống phá hủy Database và bảo mật web 23](#_Toc531809089)

[16.1 Quy tắc vàng: VALIDATE INPUT và ESCAPE OUTPUT 23](#_Toc531809090)

[**a)** Validate input 23](#_Toc531809091)

[17. Upload file ảnh 24](#_Toc531809092)

[17.1 Upload 1 file ảnh 24](#_Toc531809093)

[17.2 Upload nhiều file ảnh 24](#_Toc531809094)

# Cài đặt XAMPP

## Lưu ý trong file Php.ini

### Cách 1: tác động trực tiếp vào file Php.ini

Lưu ý cách cấu hình XAMPP bằng cách config file php.ini

- Display error=ON : hiển thị debug lỗi, hiện hay ko hiện, default là ON

- Short\_open\_tag=off : enable short tag PHP <?=$abc?>

- memory\_limit=128: dung lượng chiếm bao nhiêu mb khi chạy script dữ liệu

- max\_execution\_time=30 : thời gian tối đa chạy 1 script

- max\_input\_time=60 : thiết lập thời gian input của bạn

- Upload\_max\_filesize=2M: dung lượng upload dung lượng hình ảnh.

- max-file\_upload=20: số lượng file upload lên sever 1 lần

- error\_reporting=E\_ALL & ~E\_DEPRECATED & ~E\_STRICT : cách hiện hay không hiện từng trạng thái lỗi.

*Lưu ý khi thay đổi cần restart Apache.*

### Cách 2: dùng lệnh trong php để cấu hình

ini\_set('display\_errors', false);

# Echo – Print

+ Giống:

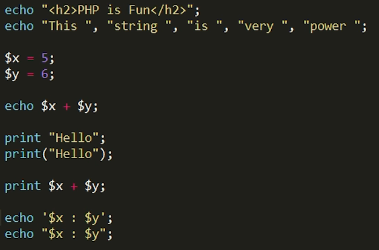
Đều là hiển thị nội dung ra trình duyệt

+ Khác:

- Print thường trả kết quả về là 1 (return 1) thường dùng trong các câu điều kiện.

- Echo có thể dùng nhiều biến số cách nhau bởi dấu phẩy để in ra trình duyệt, còn Print chỉ dùng duy nhất 1 biến số.

- Echo nhanh hơn Printf



*Lưu ý: Câu lệnh Echo dấu nháy đơn ‘’ và dấu nháy kép “ “: nháy đơn thì ko in ra được giá trị của biến, còn nháy kép thì đc.*

# Comment trong PHP

## Comment dòng đơn // hoặc #

// đây là comment dòng đơn

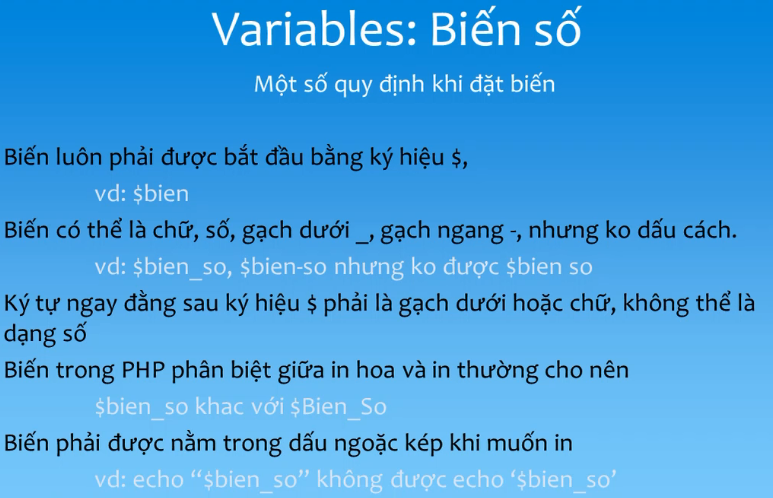
# đây là comment dòng đơn

## Comment đoạn văn

/\* Đây là comment một đoạn văn

Đây là comment một đoạn văn \*/

# Biến số trong PHP



# Các kiểu string

## Chiều dài string: strlen($string1)

Kết quả trả về số.

## In hoa tất cả string: strtoupper($string2)

Kết quả trả về chuỗi.

## In thường tất cả string: strtolower($string2)

Kết quả trả về chuỗi.

## In hoa chữ đầu: ucfirst($string1)

Kết quả trả về chuỗi.

## In hoa tất cả chữ đầu: ucwords($string1)

Kết quả trả về chuỗi.

## String thay thế: str\_replace('biên', 'song', $string3)

Kết quả trả về chuỗi.

## Cắt kí tự trong chuỗi: Substr($chuỗi, từ đâu, SoKitu)

Ex: Substr($string, 0, 4); //cắt chuỗi từ giá trị 0 và lấy 4 kí tự, trả về string, dùng để phần readmore

## Đếm số kí tự trước giá trị cuối cùng cần tìm: strrpos($text, ‘ ’)

Trả về giá trị số, Dùng để phần readmore

.

Ex: $t = “toi la nguoi den sau ” ;

$r = strrpos($t, ‘ ’)// 20

# Biến Constance

**Define(‘TÊN BIẾN’, ‘giá trị biến’);**

Define (‘TODAY’, ‘14/2’);

echo "<p>Hom nay la ngay: " . TODAY . "ban dang su dung phien ban PHP ". PHP\_VERSION . "Tren he dieu hanh " . PHP\_OS."</p>";

***Hằng số phải đặt ra ngoài echo và liên kết với chuỗi.***

# Mảng Array

## Khai báo mảng, truy xuất phần tử

$myArray =

array(34, 39, 56, 67, 76, array('a'=>'apple', 'b'=>'banana', 'c'=>'coconut'));

**echo $myArray[5]['c'];**

echo "<p>there are **{$myArray[1]} {$myArray[5]['b']}** in the box.</p>";

**echo "<pre>";**

**print\_r($myArray);**

**echo "</pre>";**

KẾT QUẢ:

Coconut

there are 39 banana in the box.

Array

(

[0] => 34

[1] => 39

[2] => 56

[3] => 67

[4] => 76

[5] => Array

(

[a] => apple

[b] => banana

[c] => coconut

)

)

## Đếm số lượng phần tử trong mảng

<?php

$myArray = array(2,3,7,8,34, 39, 56, 67,76);

?>

**count**($myArray) // Đếm số phần tử trong mảng

## Giá trị lớn nhất, bé nhất, sắp xếp trong mảng

**max**($myArray) // giá trị lớn nhất trong mảng

**min**($myArray) // giá trị bé nhất trong mảng

**sort**($myArray) // sắp xếp các ptu từ bé đến lớn

//Hiển thị mảng

echo "<pre>";

print\_r($myArray);

echo "</pre>";

rsort($myArray); //Sắp xếp từ lớn đến bé

## Tách, gộp các phần tử trong mảng

implode('\*', $myArray); // chèn kí tự \* vào các phần tử

Ví dụ:

<?php

$myEmails = 'izwebz@yahoo.com, admin@yahoo.com, support@izwebz.com';

$split = explode(',', $myEmails); //tách các ptu trong mảng

echo "<pre>";

print\_r($split);

echo "</pre>";

$last = end($split);// hiển thị phần tử cuối cùng của mảng

echo $last;

?>

$myArray = array('html', 'css', 'wordpress', 'jquery', 'php');

$array = array('photoshop', 'illustrator', 'corelDraw', 'thinkpad');

## Lấy phần tử ngẫu nhiên, hiện thị phần tử

$rand = array\_rand($myArray);// lấy key ngẫu nhiên của phần tử

$viet\_hoa = array\_map('ucfirst', $array);// lấy lần lượt các giá trị trong mảng $array và viết hoa.

**foreach ($viet\_hoa as $hoa) {**

**echo "<li>{$hoa}</li>";**

**}**

**shuffle**($myArray); // hiện thị lẫn lộn các phần tử

**if(in\_array('csss', $myArray)) {**

**echo "yes, it is in array";**

**}**

$merged = **array\_merge**($myArray, $array);// cộng 2 mảng lại với nhau

$myArray[] = 'ajax';

**array\_splice**($myArray, 3, 1, 'oop');// thêm một phần tử vào mảng chèn vào vị trí thứ 3, 1: chèn 1 phần tử.

**unset**($myArray[5]); // xóa hết key và giá trị của phần tử

//array\_splice($myArray,3, 2);

//print\_r($myArray[$rand]);

# Numbers và các hàm tính

$num = 3.14;

echo round($num, 1); // cách hiện thị số sau dấu phẩy (1)

echo ceil($num); // làm tròn lên

echo floor($num); // làm tròn xuống

echo rand(); //hiện giá trị ngẫu nhiên

echo rand(1,100); // hiện ngẫu nhiên từ 1 đến 100

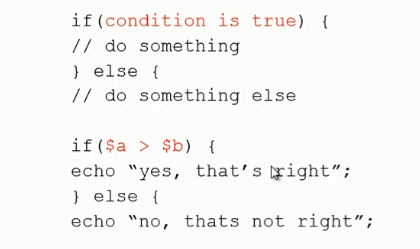
$float = 30456;

echo number\_format($float, 2); //định dạng số, 2 số xhien sau dấu phẩy

# Vòng lặp

## Vòng lặp if … else…

**Cách 1:**



**Cách 2:**

//If else PHP trong file HTML

<?php if (expr): ?>

<?php else: ?>

<?php endif ?>

**Cách 3:**

$retVal = (condition) ? a : b ;

## Vòng lặp switch

Switch (điều\_kiện){

Case 1:

// làm cái gì;

Break;

Case 2:

// làm cái gì;

Break;

default:

// làm những cái còn lại;

Break;

}

## Vòng lặp For

For (i=1; i<= 10; i++){

//làm cái gì;

//echo …

}

## Vòng lặp While

Đa phần dùng với array.

<ul class="pagination">

<?php

$count = 0;

while($count <= 10) {

if($count == 7) {

echo "...";

} else {

echo "<li><a href='{$count}'>{$count}</a></li>";

}

$count++;

}// End While loop

?>

</ul>

# Function

## Function trả lại 1 giá trị

**function** xin\_chao($name = 'ban hien') {

echo "Xin chao, $name!";

}

**xin\_chao();**

## Function trả lại nhiều giá trị

function **cong\_tru**($x, $y) {

$tong = $x + $y;

$hieu = $x - $y;

$dap\_so = array($tong, $hieu);

return $dap\_so;

}

**$total = cong\_tru(8, 5);**

echo "Tong so: **$total[0]** <br/>";

echo "Hieu so: **$total[1]** <br/>";

**list($tong, $hieu) = cong\_tru(8, 5);**

echo "Tong so: **$tong** <br/>";

echo "Hieu so: **$hieu** <br/>";

# Fuction biến toàn cục

$var = "Toi o ngoai funciton";

function scope($var) {

**global $var;**

$var = "Toi nam o trong function";

**return $var;**

}

echo scope($var) . '<br/>';

// In ra bien da dat

echo $var;

# Biến $\_POST

Khai báo biến:

<?php

if(**isset($\_POST['submit'])**) {

// *Da co gia tri de xu ly form, sau khi nut submit duoc nhan*

**$ngay = $\_POST['ngay'];**

$thang = $\_POST['thang'];

$nam = $\_POST['nam'];

$gender = $\_POST['gender'];

$hidden = $\_POST['hidden'];

echo "ngay hom nay la ngay {$ngay}, $thang $nam ban co gioi tinh la $gender Cai nay ban ko can biet la hidden $hidden;";

}

?>

# Biến $\_GET

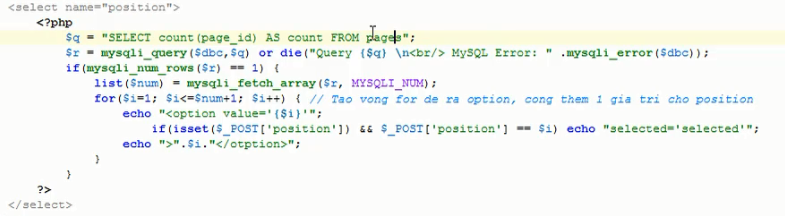
<a href='<?php echo **rawurlencode('encode-2.php');?>**?name**=<?php echo urlencode('cong vu'); ?>**'>

<?php

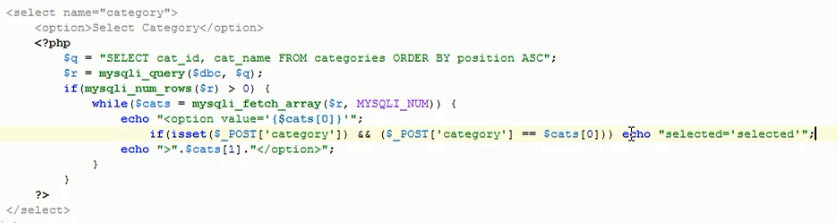
**echo htmlentities('<script>URLEncode</script>');** ?></a>

# IZWEBZ

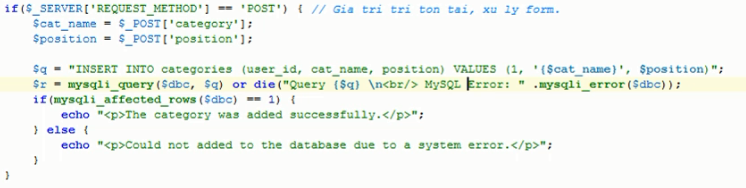
## Query đếm số page trong CSDL để hiện trong <option>

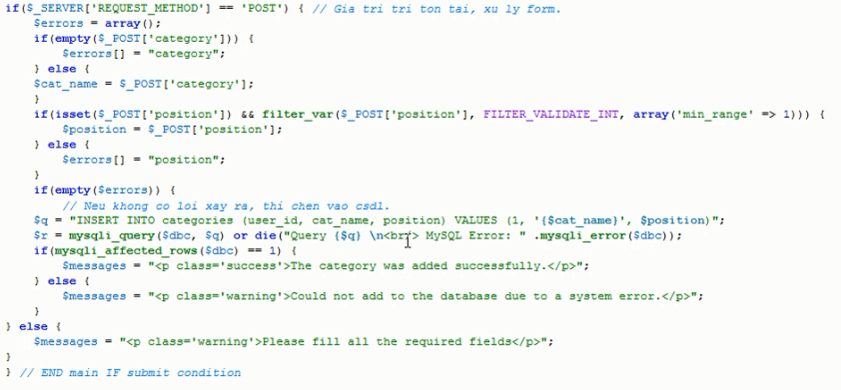


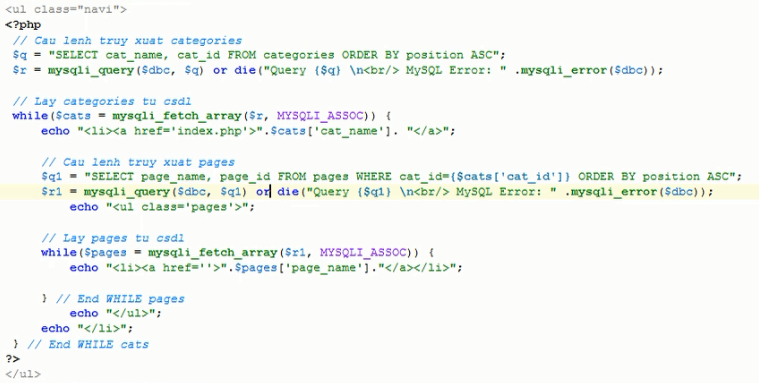
## Query truy xuất Category trong CSDL để hiện trong <option>



## Query thêm dữ liệu vào CSDL và báo kết quả







## Kiểm tra Cid, Pid để in đậm tab đang chọn



## Hàm kiểm tra các giá trị nhập và truy vấn csdl

preg\_match(**'/^**[\w\'.-]{2,20}**$/**i**'**, trim($\_POST['account'])))

**‘/^ $/’:** định dạng cho các kí tự hợp lệ

**\w:** gồm các kí tự a-z, A-Z, 0-9, \_

**{2,20}:** từ 2 đến 20 kí tự

**i:** ko phân biệt in hoa, in thường

$tk = $ht = $gm = $cv = $sdt = $qh = $p = FALSE;

if(preg\_match('/^[\w\'.-]{2,20}$/i', trim($\_POST['account']))){

$tk = mysqli\_real\_escape\_string($dbc, trim($\_POST['account']));

} else {

$error[] = 'account';

}

if(filter\_var($\_POST['email'], FILTER\_VALIDATE\_EMAIL)){

$gm = mysqli\_real\_escape\_string($dbc, trim($\_POST['email']));

} else {

$error[] = 'email';

}

if(isset($\_POST['level'])){

$qh = mysqli\_real\_escape\_string($dbc, trim($\_POST['level']));

} else {

$error[] = 'quyen han';

}

if(preg\_match('/^[\w\'.-]{6,20}$/', trim($\_POST['matkhau1']))){

if($\_POST['matkhau1'] == $\_POST['matkhau2']){

//khop matkhau voi nhau thi luu vao csdl

$p = mysqli\_real\_escape\_string($dbc, trim($\_POST['matkhau1']));

} else {

$error[] = "Mat khau khong khop";

}

} else {

$error[] = 'matkhau';

}

if($tk && $ht && $gm && $cv && $sdt && $qh && $p){

$q = "SELECT taikhoan";

} else {

// thieu gia tri thong bao ra ngoai

}

# ỨNG DỤNG CODE

## Tạo readmore cho đoạn văn

- Trong câu truy xuất CSDL thì ta *LEFT($content, 400)* – cắt nội dung với chiều dài 400 kí tự.

- Sau đó lúc hiện thị ra ta dùng *SUBSTR($content, 0, STRRPOS($content, “ ”))* để cắt kí tự không thành chữ.

## Sử dụng dữ liệu ngoài cậu lệnh if && hiện titel để SEO

- Trước khi chạy câu lệnh IF thì ta nên tạo 1 array để lấy các giá trị trong câu lệnh IF.

- Sau đó dùng vòng lặp foeach để dẫn ra các số liệu lưu trong array.

$posts = array(); // Tao mot array trong de luu gia tri vao su dung sau nay cho phan noi dung

if(mysqli\_num\_rows($set) > 0) {

// Neu co post de hien thi ra trinh duyet.

$pages = mysqli\_fetch\_array($set, MYSQLI\_ASSOC);

$title = $pages['page\_name'];

$posts[] = array(

'page\_name' => $pages['page\_name'],

'content' => $pages['content'],

'author' => $pages['name'],

'post-on' => $pages['date'],

'aid' => $pages['user\_id']

);

} else {

echo "<p>There are currenlty no post in this category.</p>";

}

} else {

// Neu pid khong hop le, thi chuyen huong nguoi dung ve trang index.

redirect\_to();

}

include('includes/header.php');

include('includes/sidebar-a.php');

?>

<div id="content">

<?php

foreach($posts as $post) {

echo "

<div class='post'>

<h2>{$post['page\_name']}</h2>

<p>".the\_content($post['content'])."</p>

<p class='meta'>

<strong>Posted by:</strong><a href='author.php?aid={$post['aid']}'> {$post['author']}</a> |

<strong>On: </strong> {$post['post-on']}

<strong>Page views: </strong> {$page\_views}

</p>

</div>

";

} // End foreach.

## Biến bài văn được chia ra từng đoạn

- Có thẻ dùng : ***nl2br()*** để biến các thẻ \n thành thẻ <br/> nhưng <br> không tốt vì có thể dùng css để design sẽ ko hợp chuẩn.

- Khi soạn đoạn văn sẽ có ngắt câu, xuống hàng thì tương tự với các thẻ \r \n hoặc \n. Và phải validate dữ liệu trong nội dung.

// Tao paragraph tu CSDL

function the\_content($text) {

$sanitized = htmlentities($text, ENT\_COMPAT, 'UTF-8');

return str\_replace(array("\r\n", "\n"),array("<p>", "</p>"),$sanitized);

}

## Cắt đoạn nội dung dài thành đoạn ngắn để hiển thị

// Cat chu~ de hien thi thanh doan van ngan.

function the\_excerpt($text, $string = 400) {

$sanitized = htmlentities($text, ENT\_COMPAT, 'UTF-8');

if(strlen($sanitized) > $string) {

$cutString = substr($sanitized,0,$string);

$words = substr($sanitized, 0, strrpos($cutString, ' '));

return $words;

} else {

return $sanitized;

}

} // End the\_excerpt

## Các cách chống spam

### Random question

Thêm câu hỏi random như captra để tránh spam.

- Trước tiên do dùng đến SESSION nên phải khởi tạo SESSION bằng cách thêm lệnh vào trước header.

<?php

ini\_set('session.use\_only\_cookies', true);

session\_start(); ?>

- Sau đó xử lý form:

/\* Validate captcha question\*/

if(isset($\_POST['captcha']) && trim($\_POST['captcha']) != $\_SESSION['q']['answer']) {

$errors[] = "wrong";

}

/\* Xử lý form \*/

<div>

<label for="captcha">Phiền bạn điền vào giá trị số cho câu hỏi sau: <?php echo captcha(); ?><span class="required">\*</span>

<?php if(isset($errors) && in\_array('wrong',$errors)) {echo "<span class='warning'>Please give a correct answer.</span>";}?></label>

<input type="text" name="captcha" id="captcha" value="" size="20" maxlength="5" tabindex="4" />

</div>

- Thêm function captra:

// Ham dung chong spam trong form

function captcha() {

$qna = array(

1 => array('question' => 'Mot cong mot', 'answer' => 2),

2 => array('question' => 'ba tru hai', 'answer' => 1),

3 => array('question' => 'ba nhan nam', 'answer' => 15),

4 => array('question' => 'sau chia hai', 'answer' => 3),

5 => array('question' => 'nang bach tuyet va .... chu lun', 'answer' => 7),

6 => array('question' => 'Alibaba va ... ten cuop', 'answer' => 40),

7 => array('question' => 'an mot qua khe, tra .... cuc vang', 'answer' => 1),

8 => array('question' => 'may tui .... gang, mang di ma dung', 'answer' => 3)

);

$rand\_key = array\_rand($qna); // Lay ngau nhien mot trong cac array 1, 2, 4

$\_SESSION['q'] = $qna[$rand\_key];

return $question = $qna[$rand\_key]['question'];

} // END function captcha

### Honey pot

Bẫy input không được nhập vào thì mới submit được giá trị, người dùng ko thấy còn con spam pot sẽ thấy và điền giá trị thì ko submit được form.

if(!empty($\_POST['url'])) {

redirect\_to('thankyou.html');

}

………

<div class='website'>

<label for="website"> Nếu nhìn thấy, thì ĐỪNG điền gì vào hết</label>

<input type="text" name="url" id="url" value="" size="20" maxlength="20" />

</div>

### Salt pot

Nếu muốn submit form thì bắt người dùng phải xóa trường này để tránh spam.

if(!empty($\_POST['question'])) {

$errors[] = 'delete';

}

…………

<div>

<label for="question"> Phiền bạn xóa giá trị ở trường dưới, trước khi submit form.

<?php if(isset($errors) && in\_array('delete',$errors)) { echo "<span class='warning'>Bạn quên chưa xóa giá trị.</span>"; } ?>

</label>

<input type="text" name="question" id="question" value="Xóa đi giá trị này" size="20" maxlength="40" />

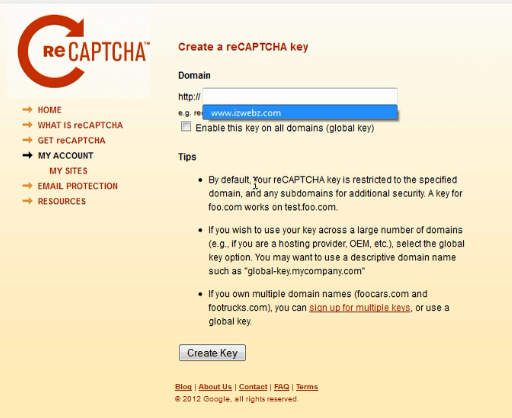
</div>

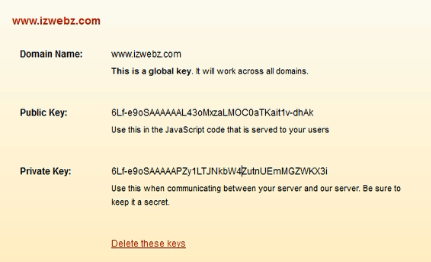
### Dùng Recaptra

Dùng mã gõ captra của google để tránh spam với website lớn.

- Vào trang [*http://google.com/recaptcha*](http://google.com/recaptcha)







## Làm Contact Form

Validate bằng biểu thức chính quy

if(!preg\_match('/^[\w.-]+@[\w.-]+\.[a-zA-Z]{2,6}$/', $clean['email'])) {

$errors[] = 'email';

}

/^ $/: cú pháp để kiểm tra các kí tự bên trong

[\w.-]**+**@[\w.-]**+**\.[a-zA-Z]{2,6}: Thành phần của 3 phần ngăn cách bởi dấu +.

// KIem tra xem co loi o form hay khong, neu khong co, gui email

if(empty($errors)) {

$body = "Name: {$clean['name']} \n\n Comment:\n ". strip\_tags($clean['comment']);

$body = wordwrap($body, 70);

if(mail('izwebz@yahoo.com', 'Contact form submission', $body, 'FROM: localhost@localhost')) {

echo "<p class='success'>Thank you for contacting me. I will get back to you ASAP</p>";

$\_POST = array();

} else {

echo "<p class='warning'>Sorry, your email could not be sent.</p>";

}

} else {

// Neu co loi trong bien errors, do nguoi dung quen nhap vao truong

echo "<p class='warning'>Please fill out all the required fields.</p>";

}

## Đăng ký thành viên bằng cách gửi mail để xác nhận

if(preg\_match('/^[\w\'.-]{4,20}$/', trim($\_POST['password1']))) {

if($\_POST['password1'] == $\_POST['password2']) {

// Neu mat khau mot phu hop voi mat khau hai, thi luu vao csdl

$p = mysqli\_real\_escape\_string($dbc, trim($\_POST['password1']));

} else {

// Neu mat khau khong phu hop voi nhau

$errors[] = "password not match";

}

} else {

$errors[] = 'password';

}

if($fn && $ln && $e && $p) {

// Neu moi thu deu day du, truy van csdl

$q = "SELECT user\_id FROM users WHERE email = '{$e}'";

$r = mysqli\_query($dbc, $q);

confirm\_query($r, $q);

if(mysqli\_num\_rows($r) == 0) {

// Luc nay email van con trong, cho phep nguoi dung dang ky

// Tao ra mot chuoi Activation Key

$a = md5(uniqid(rand(), true));

// Chen gia tri vao CSDL

$q = "INSERT INTO users (first\_name, last\_name, email, pass, active, registration\_date)

VALUES ('{$fn}', '{$ln}', '{$e}', SHA1('$p'), '{$a}', NOW())";

$r = mysqli\_query($dbc, $q);

confirm\_query($r, $q);

if(mysqli\_affected\_rows($dbc) == 1) {

// Neu dien thong tin thanh cong, thi gui email kich hoat cho nguoi dung

$body = "Cảm ơn bạn đã đăng ký ở trang izCMS. Một email kích hoạt đã được gửi tới địa chỉ email mà bạn cung cấp.

Phiên bạn click vào đường link để kích hoạt tài khoản \n\n ";

$body .= BASE\_URL . "processor/activate.php?x=".urlencode($e)."&y={$a}";

if(mail($\_POST['email'], 'Kích hoạt tài khoản tại izCMS', $body, 'FROM: localhost')) {

$message = "<p class='success'>Tài khoản của bạn đã được đăng ký thành công. Email đã được gửi tới địa chỉ của bạn. Bạn phải

nhấn vào link để kích hoạt tài khoản trước khi sử dụng nó.</p>";

} else {

$message = "<p class='warning'>Không thể gửi được email cho bạn. Rất xin lỗi về sự bất tiện này.</p>";

}

} else {

$message = "<p class='warning'>Sorry, your order could not be processed due to a system error.</p>";

}

} else {

// Email da ton tai, phai dang ky bang email khac.

$message = "<p class='warning'>The email was already used previously. Please use another email address.</p>";

}

} else {

// Neu mot trong cac truong bi thieu gia tri

$message = "<p class='warning'>Please fill in all the required fields.</p>";

}

File để active dữ liệu để NULL trong trường active trong CSDL

<?php

if(isset($\_GET['x'], $\_GET['y']) && filter\_var($\_GET['x'], FILTER\_VALIDATE\_EMAIL) && strlen($\_GET['y']) == 32) {

// Neu day du thong tin va hop le, xu ly form va truy van csdl

$e = mysqli\_real\_escape\_string($dbc, $\_GET['x']);

$a = mysqli\_real\_escape\_string($dbc, $\_GET['y']);

$q = "UPDATE users SET active = NULL WHERE email = '{$e}' AND active = '{$a}' LIMIT 1";

$r = mysqli\_query($dbc, $q); confirm\_query($r, $q);

if(mysqli\_affected\_rows($dbc) == 1) {

echo "<p class='success'>Your acccount has been activated successfully. You may <a href='".BASE\_URL."/login.php'>login </a> now.</p>";

} else {

echo "<p class='warning'>Your account could not be activated. Please try again later.</p>";

}

} else {

// Thong tin khong dung, hoac khong hop le, chuyen huong nguoi dung ve trang index

redirect\_to();

}

?>

## Cách truy vấn cơ sở dữ liệu bằng Statement

<?php

if($\_SERVER['REQUEST\_METHOD'] == 'POST') {

$errors = array();

// Trim all incoming data

$trimmed = array\_map('trim', $\_POST);

if(preg\_match('/^[\w]{2,10}$/i', $trimmed['first\_name'])) {

$fn = $trimmed['first\_name'];

} else {

$errors[] = "first\_name";

}

if(preg\_match('/^[\w]{2,10}$/i', $trimmed['last\_name'])) {

$ln = $trimmed['last\_name'];

} else {

$errors[] = "last name";

}

if(filter\_var($trimmed['email'],FILTER\_VALIDATE\_EMAIL)) {

$e = $trimmed['email'];

} else {

$errors[] = "email";

}

// Check for website (not required)

$web = (!empty($trimmed['website'])) ? $trimmed['website'] : NULL;

// Check for yahoo (not required)

$yahoo = (!empty($trimmed['yahoo'])) ? $trimmed['yahoo'] : NULL;

// Check for website (not required)

$bio = (!empty($trimmed['bio'])) ? $trimmed['bio'] : NULL;

if(empty($errors)) {

$q = "UPDATE users SET

first\_name = ?, last\_name = ?, email = ?, website = ?, yahoo = ?, bio = ?

WHERE user\_id = ?

LIMIT 1";

$stmt = mysqli\_prepare($dbc, $q);

mysqli\_stmt\_bind\_param($stmt, 'ssssssi', $fn, $ln, $e, $web, $yahoo, $bio, $\_SESSION['uid']);

mysqli\_stmt\_execute($stmt) or die("MySQL Error: $q" . mysqli\_stmt\_error($stmt));

if(mysqli\_stmt\_affected\_rows($stmt) > 0) {

// Update thanh cong

$message = "<p class='success'>Your profile has been updated successfully.</p>";

} else {

// Co loi he thong xay ra

$errrors[] = "<p class='error'>Your profile could not be updated due to a system error.</p>";

}

}

}// END $\_SERVER IF

?>

## Sử dụng array kết hợp foreach để hiển thị

<select name="user\_level">

<?php

// Set up array for roles

$roles = array(1 => 'Registered Member', 2 => 'Moderator', 3 => 'Super Mod', 4 => 'Admin');

foreach ($roles as $key => $role) {

echo "<option value='{$key}'";

if($key == $user['user\_level']) {echo "selected='selected'";}

echo ">".$role."</option>";

}

?>

</select>

## Tránh ăn cắp SESSION Admin

Hack có thể ăn cắp tài khoản admin bằng cách gửi ID session của người dùng sang Admin và admin đăng nhập thì như ID đó như của Admin và sẽ bị chiếm quyền admin.

Để tránh cần phải dùng ID session theo COOKIE của web chứ ko dùng ID ở thanh URL người ta gửi.

**Cú pháp làm:**

<?php

ini\_set('session.use\_only\_cookies', true);

session\_start();

if(!isset($\_SESSION[‘time’]) || $\_SESSION[‘time’] < (time()-30)){

sesion\_regenerate\_id();

$\_SESSION[‘time’] = time();

}

?>

Hoặc có thể sau khi trả về tài khoản để người dùng đăng nhập thì dùng hàm ***sesion\_regenerate\_id();*** tạo ra 1 session mới và đăng nhập vào:

sesion\_regenerate\_id();

# Các cách chống phá hủy Database và bảo mật web

## Quy tắc vàng: VALIDATE INPUT và ESCAPE OUTPUT

### Validate input

- Biểu thức chính quy

preg\_match('/^[\w]{2,10}$/i', $trimmed['first\_name']));

- Dùng isset()

- Dùng Filter\_var()

filter\_var($bien, FILTER\_VALIDATE\_EMAIL)

*Filter\_validate\_email, Filter\_validate\_int,*

*Filter\_sannitize\_string, sannitize\_special\_char*

- Dùng Strip\_tags()

# Upload file ảnh

## Upload 1 file ảnh

Phải có thuộc tính **enctype="multipart/form-data">** để có thể upload file ảnh và **method="POST".**

**FORM:**

<form action="upload.php" method="POST" enctype="multipart/form-data">

<input type="file" name="avatar">

<button>Upload</button>

</form>

**XỬ LÝ:**

if($file['size'] <= 1024\*1024){

//trả về đuôi ảnh

$ext = strtolower(pathinfo($name,PATHINFO\_EXTENSION));

$arrExt = ['png', 'jpg', 'gif'];

//kiểm tra đuôi có hợp lệ ko

if(in\_array($ext,$arrExt)){

// 2018-10-20-19-58-24-a.png

date\_default\_timezone\_set('Asia/Ho\_Chi\_Minh');

$newName = date('Y-m-d-H-i-s',time()).'-'.$name;

//chuyển ảnh vào file

move\_uploaded\_file($tmpName,"avatars/$newName");

//kiểm tra ảnh tồn tại hay ko

if(file\_exists("avatars/$newName")){

echo 'thanh cong';

} else {

echo 'Upload fail';

}

} else {

echo 'File not allow!';

}

} else {

echo "File too large!";

}

## Upload nhiều file ảnh

Phải có thuộc tính **multiple** vào thẻ input:file và name kiểu mảng để có thể upload nhiều file ảnh.

<input type="file" name="avatar[]" multiple>

**FORM**

<form action="xuly-upload.php" method="post" enctype="multipart/form-data">

<input type="file" name="avatar[]" multiple>

<button>Upload</button>

</form>