iranphp articles

عنوان مقاله : ساخت تصاویر امنیتی با php قسمت اول
نگارنده : رامین فرمانی
آدرس پست الکترونیک : ramin.farmani@gmail.com
تاریخ نگارش : زمستان ۸۳

ساخت تصاویر امنیتی باphp :

چندی پیش در یکی از انجمنها بحث داغی در مورد برتری php بر asp.net و یا برعکس asp.net بر php شکل گرفته بود طرفداران asp.netدر موضوعاتی در همان انجمن سوالی در مورد ساخت و تولید تصاویر امنیتی که روبوتها قابل به خواندن آنها نیستند مطرح کرده بودند و پاسخ آن موضوع را یکی از دوستان ارجمند با تابعی مخصوص در asp.net داده بودند من به فکر ساخت چیز مشابهی با php افتادم و سری هم به سایت محبوبمان php.net زدم تا ببینم چیز بدرد بخوری گیر میاد یا نه باورتون نمیشه تو کمتر از چند ثانیه زدم تو خال همونی که می خواستم رو گیر آوردم یکمی هم انگولکش کردم تا جالب تر بشه و توضیح کاملش رو براتون میارم مثل ینکه همینطوری الکی الکی من دارم فقط از مسائل امنیتی براتون مقاله مینویسم .بگذریم ابتدا کد ین برنامه که در سه صفحه مجزا بید نوشته بشه .

صفحه اول که من اون رو تو فایلی به نام encod.php ذخیره می کنم :

encod.php

```
<?php
function get_rnd_iv($iv_len){
$iv = '';
while ($iv_len-- > 0) {
$iv .= chr(mt_rand() & 0xff);
}
return $iv;
}
function md5_encrypt($plain_text, $password, $iv_len = 16){
$plain_text .= "x13";
$n = strlen($plain_text);
if ($n % 16) $plain_text .= str_repeat("0", 16 - ($n % 16));
$i = 0;
$enc_text = get_rnd_iv($iv_len);
$iv = substr($password ^ $enc_text, 0, 512);
while ($i < $n) {
$block = substr($plain_text, $i, 16) ^ pack('H*', md5($iv));
$enc_text .= $block;
$iv = substr($block . $iv, 0, 512) ^ $password;
$i += 16;
}
return base64_encode($enc_text);
}
function md5_decrypt($enc_text, $password, $iv_len = 16){
$enc_text = base64_decode($enc_text);
$n = strlen($enc_text);
$i = $iv_len;
$plain_text = '';
$iv = substr($password ^ substr($enc_text, 0, $iv_len), 0, 512);
while ($i < $n) {
$block = substr($enc_text, $i, 16);
$plain_text .= $block ^ pack('H*', md5($iv));
$iv = substr($block . $iv, 0, 512) ^ $password;
$i += 16;
}
return preg_replace('/\\x13\\x00*$/', '', $plain_text);
}
?>
```

صفحه دوم که مربوط به تولید تصویر و من اونو تو فایلی به نام image.php ذخیره می کنم :

image.php

```
<?php
```

```php
require_once "encode.php";
$decid = urldecode(md5_decrypt($_REQUEST['id'], $_REQUEST['key']));


header("Content-type: image/png");
$img = imagecreatetruecolor(75, 25);
$black = imagecolorallocate($img, 0, 0, 0);
$red = imagecolorallocate($img, 236, 134, 72);
$bgline = imagecolorallocate($img, 81, 102, 125);
$bg = imagecolorallocate($img, 131, 152, 175);
imagefill($img, 0, 0, $bg);


imageline($img,0,6,75,6,$bgline);
imageline($img,0,12,75,12,$bgline);
imageline($img,0,18,75,18,$bgline);

imageline($img,7,0,7,25,$bgline);
imageline($img,14,0,14,25,$bgline);
imageline($img,21,0,21,25,$bgline);
imageline($img,28,0,28,25,$bgline);
imageline($img,35,0,35,25,$bgline);
imageline($img,42,0,42,25,$bgline);
imageline($img,49,0,49,25,$bgline);
imageline($img,56,0,56,25,$bgline);
imageline($img,63,0,63,25,$bgline);
imageline($img,70,0,70,25,$bgline);


imageline($img,3,6,70,18,$red);
imagestring($img, 5, 5, 5, $decid, $black);
//imagettftext($img,20,0,10,20,$brown,\"/path/arial.ttf\",$decid);
imagepng($img, '', 75);
imagedestroy($img);
?>
```

خوب میمونه صفحه آخر که متعلق به شماست هر کجا که خواستین اون عکس تولید بشه قطعه کد زیر رو قرار بدین:

```php
<?php
require_once "encode.php";
$string = md5(rand(0, microtime()*1000000));
$verify_string = substr($string, 3, 7);
$key = md5(rand(0,999));
$encid = urlencode(md5_encrypt($verify_string, $key));
echo "<img src='image.php?id=$encid&key=$key'><br>";
echo "to verify the user would hve to type in $verify_string";
?>
```

خوب بریم سراغ توضیحات این کدها :

نمی دونم از md5 چیزی میدونین یا نه به هر حال امیدوارم که بدونین چون این مقاله هدفش توضیح چیز دیگری‌ست ولی اگر مشکلی در فهم کلی قسمت encode.php داشتید برایم پیغام بگذارید تا اگر فرصت شد برایتان md5 را توضیح بدم .

ساختار برنامه به این صورت است که ابتدا قطعه کد سومی که برایتان نوشتم میاد و یک رشته رندم و همچنین یک کلید رندم تولید می کنه نام ایندو به ترتیب string$ و key$ هست که روی همرفته چیز خفنی از کار دراومد و چون میخواستم مثلا امنیت بالایی داشته باشه به این شکل عمل کردم که ایندو مقدار رو با اندکی سیخونک به فایل image.php ارسال کردم حالا همین یه تیکه رو براتون توضیح می دم :

ببینید خیلی سادست تو خط سوم مقدار $string رو برابر با ام دی فای و مقداری رندم بین صفر تا ثانیه قرار میدهم بعد $verify_string رو برابر با کاراکترهای سوم تا دهم مقدار $string قرار میدم و همچنین یک مقدار رندم بین صفر تا ۹۹۹ تولید می کنم و در $key قرارش می دیم همونطوری که می بینید در خط ششم مقدار urlencode شده md5_encrypt ایندو مقدار بالا رو در $encid قرار میده به دلیل پیچیدگی الگوریتم استفاده شده در فایل encode.php از توضیح آن قسمت ها صرفه نظر کردم تا برای مبتدیان زیاد پیچیده نشود نهایتا ما این مقادیر رو همونطوری که میبینید در خط هفتم به فایل image.php می فرستیم تا عکس ما را با مقدار $verify_string در داخل تصویری تولید کند .

خوب حالا ماهم با این مقادیر میریم به فایل image.php
خوب هرچی کد خفن تولید کرده بودیم به حالت پیش از کد شدن تبدیل می کنیم تا مقدار ما تحت امنیت کامل به درون تصویر منتقل شود در واقع این همه کد گذاری برای انتقال امن داده ها به درون فایل image.php بوده است
همونطوری که به راحتی از قطعه کد دوم مشخص است با توابعی تصویری را تولید می کنم و برای اینکه تصویر زیاد ساده نباشد یک پس زمینه مربعی و یک خط نارنجی رو کاراکترهای امنیتی می کشم در یک خط اضافی هم کدی رو نوشتم که شما با استفاده از اون می تونید حتی فونت نوشته ها رو در تصویرتون تغییر بدید فقط قسمت /path/ رو باید با مسیر فونت عوض کنید ولی من برای راحتی بیشتر از تابع imagestring استفاده کردم
پیشنهاد اکید این کمترین بر همه شما دوستان بزرگوار این است که به دنبال حفظ کردن این کدها و استفاده طوطی وار از آنها نباشید این مقالات باید بهانه برایتان باشند تا شما را به دنبال یادگیر مابقی توابع مرتبط و استفاده از آنها مجاب کنند مثلا خیلی خوب است که manual پی اچ پی رو باز کنید و لغت image رو سرچ کنید وتوابع کامل تصاویر رو ببینید و از آنها استفاده کنید. به همین دلیل است که من هیچ وقت در مقالاتم کد آماده و یک تکه از برنامه قرار نمی دم مگر آنکه توضیح الگوریتم هایی که استفاده کردم وقت گیر و دشوار باشد .