iranphp articles

عنوان مقاله : تصدیق هویت کاربر
نگارنده : .....
آدرس پست الکترونیک : .....
تاریخ نگارش : .....

تصدیق هویت کاربر:

متدهای تصدیق هویت کاربر یا همان Authentication Schemes یکی از مباحث جذاب در برنامه نویسی php است که باید نکات ایمنی را دقیقا در آن لحاظ کرد. روش های گوناگونی بدین منظور موجود است که با توجه به سطح امنیت مورد نیاز می توانید از آن ها استفاده کنید. مرسوم ترین روش برای این کار استفاده از یک بانک اطلاعاتی برای نگهداری اطلاعات کاربران است. مسلما در تصدیق هویت مبنی بر پایگاه داده ما قابلیت انعطاف و کارایی بیشتری در مقایسه با کار با فایل ها به عنوان نگهدارنده اطلاعات خواهیم داشت. برای مثال کار با توابعی همچون md5 و crypt را به عنوان پنهان سازی اطلاعات در نظر بگیرید !

در این پست قصد داریم اسکریپتی بنویسم که با توجه به اطلاعات موجود در پایگاه داده Mysql هویت کاربر را تشخیص دهد. بعلت آنکه از سطح مقدماتی مقاله خارج نشویم اطلاعات را به صورت متنی در فیلد های جدول ذخیره می کنیم، اما برای رعایت نکات امنیتی حتما باید کلمه عبور را رمزنگاری کرد
query مورد نیاز برای ساخت جدول به شکل زیر است :

```
CREATE TABLE users (
   id INT NOT NULL,
   username VARCHAR(16),
   password VARCHAR(8),
   PRIMARY KEY(id));
INSERT INTO `users` VALUES (0, '2005', '2005');
```

همان گونه که مشاهده می کنید این query یک جدول بنام users ایجاد می کند که دارای سه فیلد id ، password وusername است. برای هر فیلد مقداری را وارد می کنیم. دقت کنید که شناسه کاربری و اسم رمز در این مقادیر برابر ۲۰۰۵ است.در مرحله بعدی برای اتصال به پایگاه داده یک تابع جدید بنام connect مطابق زیر ایجاد می کنیم :

```
<?php
  function connect() {
    if(!$db = @mysql_pconnect("localhost","mysqluser","password")){
      print("<h1>Cannot Connect to the DB!\n");
      return 0;
    } else {
      mysql_select_db("php", $db);
      return 1;
    }
}
```

بجای localhost سرور پایگاه داده، mysqluser نام کاربری و password کلمه عبور دسترسی به پایگاه داده را قرار دهید. ضمنا آرگومان اولی تابع mysql_select_db نشانگر نام پایگاه در دتابیس سرور است که بصورت پیشفرض php انتخاب شده است. دقت کنید آن را مطابق با نام پایگاه داده خودتان تنظیم کنید. در کل، کار تابع mysql_select_db انتخاب پایگاه داده در دتابیس است و دو آرگومان دریافت می کند همان گونه که ذکر شد، اولی نام پایگاه داده و دومی پارامتر برقراری پیوند است. در مرحله بعدی برای چک کردن اطلاعات کاربر با اطلاعات موجود در پایگاه داده، تابع check_user رو به شکل زیر ایجاد می کنیم :

```
function check_user($user, $password) {
    if(connect()) {
      $password = substr($password, 0, 8);
      $sql = "select * from users where username = '$user' and password = '$password'";
      $result = mysql_query($sql);
      if (mysql_num_rows($result) == 1) {
        setcookie("user",$user);
        setcookie("password",$password);
```

```
        return 1;
      } else {
              echo "<h3>Sorry, you are not authorized!</h3>";
        return 0;
      }
    }
}
```

همان طور که مشاهده می شود در این تابع دو آرگومان کلمه کاربری و رمز عبور دریافت می شود. در ابتدای کار ما در این تابع، تابع connect مرحله قبل را فراخوانی می کنیم. یک عبارت شرطی ایجاد می کنیم، اگر اتصال برقرار شد کلمه عبور و نام کاربری را که به عنوان ورودی به تابع ارسال شد با مقادیر ذخیره شده در بانک اطلاعاتی مقایسه می کنیم. اگر یکسان بود هویت کاربر تصدیق می شود در غیر اینصورت پیامی را مبنی بر عدم اختیار نمایش می دهیم. فکر نکنم نیاز به تحلیل یک یک توابع باشد .

فقط در همین حد بدانید که تابع setcookie تابعی است که کوکی توسط آن به سیستم کاربر ارسال می شود. در اکثر موارد از دو آرگومان اول تابع استفاده می شود که اولی نام و دومی مقدار است. اما این تابع چهار آرگومان دیگر نیز دارد که توضیح آن در این حوصله نمی گنجد. ما در این مثال بعد از تصدیق هویت دو نام user و password را به همراه مقادیرشان به مرورگر کاربر ارسال کردیم. تقریبا عمده کار تمام شده است تنها یک عبارت شرطی به شکل زیر ایجاد می کنیم :

```
  if(!isset($user) or !check_user($user, $password)) {
    ?>
    <h1>You must log in to view this page</h1>
    <form action = "authenticate.php" method="post">
    <p>Username: <input type="text" name="user"/><br />
    Password: <input type="password" name="password" maxlength="8" size="8"/><br />
    <input type="submit" name="submit" value="Submit"/>
    </p></form>
    <?php
  } else {
    ?>
    <h1>Authorized!</h1>
    <?php
  }
  ?>
```

همان طور که مشاهده می شود در عبارت شرطی فوق از عملگر or استفاده کردیم. یعنی حداقل باید یکی از دو بخش دارای ارزش TRUE باشد، تا نتیجه TRUEشود. حال دو بخش ما چیست؟ یکی اینکه توسط تابع isset تعیین می کنیم که آیا برای متغیر user مقداری در نظر گرفته شده است یا خیر؟ اگر مقدار داده شده درست بود شرط کافی است و دومی اینکه توسط تابع check_user که ایجاد کرده ایم، کلمه کاربری و رمز عبور را با اطلاعات ذخیره شده در دتابیس مقایسه می کنیم .
حال اگر حداقل یکی از دو شرط فوق برقرار بود پیام Authorized را نمایش می دهیم در غیر اینصورت یک فرم را برای ورود اطلاعات به همراه پیغام مناسب نمایش می دهیم. تنها دقت کنید چون اکشن فرم برابر با authenticate.php قرار گرفته است، نام صفحه مان را هنگام ذخیره کردن مشابه آن در نظر بگیریم. برای تمرین بیشتر می توانید این اسکریپت را از آدرس زیر دریافت کنید .

http://weblog.mybesthost.com/files/authenticate.zip