PHP ile İnternet Programlama

Prof.Dr. Tolga GÜYER

Gazi Üniversitesi
Gazi Eğitim Fakültesi
Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü

5. BÖLÜM: Oturum Yönetimi ve Güvenlik

TOLGA GÜYER

Sayfaya Yönlendirme

PHP sayfamızdan belirli koşullar altında başka bir sayfaya yönlendirme yapmamız gereken durumlarda kullanabileceğimiz bir çok yöntem vardır. Aşağıdaki örnekte bu işlem header() fonksiyonu kullanılarak gerçekleştirilmiştir.

```
<?php ob_start();?>
<form action="" method="post">
<p>Şifre: <input type="password" name="sifre" ></p>
<p><input name="dugme" type="submit" ></p>
</form>
<?php
if(isset($_POST["dugme"])){
$sifre=$_POST['sifre'];
if ($sifre=="m") {
header("Location:
http://localhost/yonlendirme_1/sifre_tamam.html"); }
else{header("Location:
http://localhost/yonlendirme_1/sifre_olmadi.html");}}
ob_end_flush();
?>
```

Sayfaya Yönlendirme

Örnek kodda yer alan ob_start() ve ob_end_flush() fonksiyonları, Cannot modify header information - headers already sent by … hatasını engellemek için kullanılmaktadır.

Ancak belirli bir sayfaya şifre denetimli olarak girilmesini sağlayacak kodumuzda önemli güvenlik açıkları bulunmaktadır. Örneğin geçerli şifrenin kod içersinde yer alması bu tür uygulamalarda kabul edilebilir bir yöntem değildir. Kullanıcı adları ve şifreler veritabanı sisteminde bir tablo içersinde saklanırlar.

Bir sonraki örneğimiz bu doğrultuda geliştirilmiştir.

Sayfaya Yönlendirme

```
<form action="" method="post">
<table width="250" border="1">
<tr>
<td bgcolor="#FFFFCC">Kullanıcı Adı :</td>
<td bgcolor="#33FFFF"><input size="20" type="text" name="kln"></td>
</tr>
<tr>
<td bgcolor="#FFFFCC">Şifre         :</td>
<td bgcolor="#33FFFF"><input size="20" type="password" name="sfr"></td>
</tr>
<tr>
<td colspan="2" bgcolor="#FFCC99"><input name="gonder" type="submit" value="GÖNDER"></td>
</tr>
</table>
</form>
<?php
function sqlConnect()
{       $snc1 = mysqli_connect("localhost","root","");
        $snc2 = mysqli_select_db($snc1,"kullanici");
        mysqli_query($snc1,"SET NAMES UTF8");  // Türkçe harfleri içeren karakter setine geçiliyor.
        $sncDeger = $snc1 and $snc2;
        return $sncDeger;}

if(isset($_POST["gonder"]) )
{       if (sqlConnect()){
                $kullanici_adi=$_POST['kln'];
                $sifre=$_POST['sfr'];
                $sql="SELECT kln, sfr FROM kln WHERE kln='$kullanici_adi' AND sfr='$sifre'";
                $sorgu=mysqli_query($snc1,$sql);
                if(mysqli_num_rows($sorgu))  {
             echo "<meta http-equiv=\"refresh\" content=\"0; url=tamam.php\">";}
                else      {print "Şifre yanliş girilmiş";
                          echo "<meta http-equiv=\"refresh\" content=\"2; url=index.php\">";}
        }       }
?>
```

Sayfaya Yönlendirme

Bu uygulamamızda kullanıcı tarafından girilen kullanıcı adı ve şifre bilgileri veritabanında yer alan “kln” adlı bir tablodaki kayıtlarla karşılaştırılarak kontrol edilmekte, ancak eşleşme sağlandığı durumda “tamam.php” sayfasına yönlendirme yapılmaktadır.

Aksi durumda şifrenin yanlış girildiği bildirimi yapılarak “index.php” sayfası tekrar yüklenmektedir.

tamam.php sayfasının içeriği ise aşağıdaki gibidir.

```
<?php echo "TAMAM"; ?>
```

Sayfaya Yönlendirme

Bu örnekte ise yönlendirme işlemi “meta” etiketi kullanılarak gerçekleştirilmiştir.

Veritabanı denetimi, bir kullanıcının internet tarayıcısının adres çubuğuna doğrudan tamam.php dosyasının adresini yazarak ulaşmasını engelleyemez. Bunu kontrol edebilmek için, tamam.php dosyası üzerinde ikinci bir kullanıcı denetimi gerçekleştirilmelidir. Bunun için ise kullanıcı adı ve/veya şifre bilgilerinin tamam.php dosyasına aktarılması gerekir.

Bu aktarma işleminin en güvenilir yolu, oturum yönetimi ile sağlanmaktadır.

Oturum Yönetimi

Sonraki slaytta yer alan örnekte, ilk olarak bir kullanıcı oturumu (session) başlatılmıştır. Bu durum, oturum süresince kullanıcı tarafından girilen kullanıcı adı bilgisinin bir oturum değişkeninde saklanabilmesi ve dolayısıyla başka sayfalara aktarılabilmesi olanağını sağlamıştır.

Oturum Yönetimi

```
<? session_start(); ?>

<form action="" method="post">
<table width="250" border="1">
<tr>
<td bgcolor="#FFFFCC">Kullanıcı Adı :</td>
<td bgcolor="#33FFFF"><input size="20" type="text" name="kln"></td>
</tr>
<tr>
<td bgcolor="#FFFFCC">Şifre          :</td>
<td bgcolor="#33FFFF"><input size="20" type="password"
name="sfr"></td>
</tr>
<tr>
<td colspan="2" bgcolor="#FFCC99"><input name="gonder" type="submit"
value="GÖNDER"></td>
</tr>
</table>
</form>
```

Oturum Yönetimi

```
<?php
function sqlConnect()
{
     $snc1 = mysqli_connect("localhost","root","");
     $snc2 = mysqli_select_db($snc1,"kullanici");
     mysqli_query($snc1,"SET NAMES UTF8");  // Türkçe harfleri içeren
karakter setine geçiliyor.
     $sncDeger = $snc1 and $snc2;
     return $sncDeger;
}

if(isset($_POST["gonder"]) )
{
     if (sqlConnect())
     {
          $kullanici_adi=$_POST['kln'];
          $sifre=$_POST['sfr'];
          $sql="SELECT kln, sfr FROM kln WHERE kln='$kullanici_adi'
AND sfr='$sifre'";
          $sorgu=mysqli_query($snc1,$sql);
```

Oturum Yönetimi

```
            if(mysqli_num_rows($sorgu))
            {
            $_SESSION['username'] = $kullanici_adi; // kullanıcı adı
istemci tarafındaki session dosyasına aktarılıyor.
                  echo "<meta http-equiv=\"refresh\" content=\"0;
url=tamam.php\">";
            }
            else
            {
                  session_unset(); // session dosyasındaki değerler
siliniyor.
                  print "Şifre yanliş girilmiş";
                  echo "<meta http-equiv=\"refresh\" content=\"2;
url=index.php\">";
            }
      }
}

?>
```

Oturum Yönetimi

$_SESSION['username'] adlı değişkende saklanan kullanıcı adı, aşağıda içeriği verilen tamam.php dosyasında veritabanından tekrar denetlenmiştir. Dolayısıyla adres çubuğuna doğrudan tamam.php dosyasının adresinin yazılması suretiyle sisteme izinsiz giriş yapılması engellenmiştir.

```
<?php
session_start();

$snc1 = mysqli_connect("localhost","root","");
$snc2 = mysqli_select_db($snc1,"kullanici");
mysqli_query($snc1,"SET NAMES UTF8");
$sql="SELECT kln, sfr FROM kln WHERE
kln='".$_SESSION["username"]."'";
$sorgu=mysqli_query($snc1,$sql);
if(session_is_registered("username") and mysqli_num_rows($sorgu))
{    echo "TAMAM";
     // Kullanıcı adı doğruysa yapılacak işlemler burada olacak.
}else{echo "YETKİSİZ KULLANICI!";}
session_destroy(); ?>
```

Oturum Yönetimi

Son örneğimizde, “SQL-Injection” olarak adlandırılan, kötü amaçlı kullanıcıların sisteme giriş yapmak amacıyla kullandıkları tekniğe karşı alınacak basit önlemler üzerinde durulmuştur.

Oturum Yönetimi

SQL Injection Nedir?

PHP için meta karakter olarak adlandırılan bazı karakterler, kritik bir önem arz ederler. Örneğin “\” karakteri gibi.

Bu karakterlerden en önemlisi de programatik yapılarla sabit metinleri, yani text ve stringleri birbirlerinden ayırmaya yarayan “ ’ “ (tek tırnak) karakteridir.

Kullanıcı adı ve/veya şifre girişlerinin yapıldığı metin kutularına bu karakterin özelliğinin kullanıldığı SQL cümleleri girilerek, daha sonra programımız tarafından gerçekleştirilecek SQL sorgulamasının sonuçları her durumda geri döndürmesi sağlanabilir.

Oturum Yönetimi

Örneğin,

SELECT * FROM kullanici WHERE kln = '' OR ''='' AND sifre = '' OR ''=''

biçimindeki bir sorgulamanın sonucu her durumda doğru (true) olacaktır. Dolayısıyla “kullanıcı” tablosundaki bütün kullanıcıları getirecektir.

Bunu ise kullanıcı adı ve şifre alanlarına sırasıyla “' OR ''=” ve “' OR ''=” girerek sağlayabiliriz.

Oturum Yönetimi

Bu durumdan addslashes adlı basit bir PHP fonksiyonunu doğru bir biçimde kullanarak korunabiliriz.

Yapmamız gereken ilk olarak, kullanıcı tarafından girilen ve formdan gönderilen kullanıcı adı ve şifre verilerine, SQL sorgulamasına sokmadan önce addslashes fonksiyonu ile “\” karakterlerini eklemektir.

Bu fonksiyon kullanıcı adı ve şifre içersinde yer alan tek tırnak karakterlerinden önce “\” meta karakterini eklemek suretiyle bu karakterleri etkisiz hale getirmektedir.

Oturum Yönetimi

Aşağıda bu anlatılanların gösterildiği örnek bir kod parçası verilmiştir:

```
$kullanici_adi=addslashes(trim($_POST['kln']));
$sifre=addslashes(trim($_POST['sfr']));

$sql="SELECT kln_kodu, sifre FROM kullanici_profili WHERE kln_kodu='$kullanici_adi' AND sifre='$sifre'";
$sorgu=mysqli_query($snc1,$sql);
if(mysqli_num_rows($sorgu))     {
            $_SESSION['username'] = $kullanici_adi;
                                                }
```