function ayarlar($baglanti) { $id=self::coz($\_COOKIE["kulbilgi"]); $sonuc=self::sorgum($baglanti,"SELECT \* FROM yonetim where id=$id",1 );

 **$baglanti**: Veritabanı bağlantısını temsil eder.

 **$id**: $\_COOKIE["kulbilgi"] çerezindeki bilgiyi çözerek kullanıcının id değerini alır. self::coz() fonksiyonu, çerezdeki şifrelenmiş bilgiyi çözmek için kullanılır.

 **$sonuc**: Kullanıcı bilgilerini veritabanından çeker. self::sorgum() fonksiyonu, yonetim tablosundan, kullanıcı id'sine göre veri döndürür.

if ($\_POST): @$kulad=htmlspecialchars($\_POST["kulad"]); @$eskisif=htmlspecialchars($\_POST["sifre"]); @$yenisif=htmlspecialchars($\_POST["yenisifre"]); @$yenisif2=htmlspecialchars($\_POST["yenisifre2"]);

 **$\_POST**: Kullanıcıdan gelen form verilerini alır.

 **htmlspecialchars()**: Formdan gelen verileri filtreleyerek XSS gibi saldırılara karşı güvenliği artırır.

 **Değişkenler:**

* $kulad: Yeni kullanıcı adı.
* $eskisif: Kullanıcının girdiği eski şifre.
* $yenisif: Yeni şifre.
* $yenisif2: Yeni şifrenin doğrulama kısmı (tekrar girilen şifre).

if ($kulad == "" || $eskisif == "" || $yenisif == "" || $yenisif2 == ""): echo '<div class="alert alert-danger mt-5">Hiçbir alan boş geçilemez.</div>'; header("refresh:2,url=control.php?sayfa=ayarlar");

Eğer herhangi bir alan boş bırakılmışsa:

* Bir hata mesajı gösterilir: *"Hiçbir alan boş geçilemez."*
* Kullanıcı 2 saniye sonra ayarlar sayfasına yönlendirilir.

$sifrelihal = md5(sha1(md5($eskisif))); if ($sonuc['sifre'] != $sifrelihal): echo '<div class="alert alert-danger mt-5">Eski şifre hatalı girildi.</div>'; header("refresh:2,url=control.php?sayfa=ayarlar");

 **$sifrelihal**: Kullanıcının girdiği eski şifre, önce md5, sonra sha1, en son tekrar md5 ile şifreleniyor.

 Veritabanındaki şifre ile karşılaştırılıyor:

* Eğer eşleşmiyorsa, bir hata mesajı gösteriliyor: *"Eski şifre hatalı girildi."*
* Kullanıcı 2 saniye sonra tekrar ayarlar sayfasına yönlendiriliyor.

if ($yenisif != $yenisif2): echo '<div class="alert alert-danger mt-5">Yeni şifreler eşleşmiyor.</div>'; header("refresh:2,url=control.php?sayfa=ayarlar");

**Kontrol:** Kullanıcının girdiği iki yeni şifre eşleşiyor mu?

* Eğer eşleşmiyorsa, bir hata mesajı gösterilir: *"Yeni şifreler eşleşmiyor."*
* Kullanıcı tekrar ayarlar sayfasına yönlendirilir.

**6. Yeni Şifre Güncellemesi**

$yenisifson = md5(sha1(md5($yenisif)));

$guncelleme = $baglanti->prepare("update yonetim set kulad=?, sifre=? where id=$id");

$guncelleme->bindParam(1, $kulad, PDO::PARAM\_STR);

$guncelleme->bindParam(2, $yenisifson, PDO::PARAM\_STR);

$guncelleme->execute();

 **$yenisifson**: Yeni şifre, önce md5, sonra sha1, en son tekrar md5 ile şifreleniyor.

 **SQL Güncelleme:** Kullanıcı adı ve şifre yonetim tablosunda güncellenir.

 **bindParam**: SQL enjeksiyonunu önlemek için kullanılır:

* $kulad: Yeni kullanıcı adı.
* $yenisifson: Yeni şifre (şifrelenmiş hali).