Kimlik doğrulama ile yetkilendirme arasındaki fark nedir?



www.yzokul.com.tr

Kimlik doğrulama ile yetkilendirme arasındaki fark nedir?



Kimlik doğrulama ve yetkilendirme hakkında soru soruyorsun; bu iki kelime sık sık karıştırılır. Kısa cevap basittir: kimlik doğrulama kim olduğunu kontrol eder, yetkilendirme ise ne yapabileceğini kontrol eder. Ayrıntıları okurken bu tek satırlık cevabı aklında tut. Yakından bakmadan önce sana bütün fikri verir. Birçok yeni başlayan bunları karıştırır, ama bunlar ayrı kavramlardır.



Bu iki kelimenin arkasında iki farklı soru vardır. Kimlik doğrulama "sen kimsin" sorusunu yanıtlar, yetkilendirme ise "ne yapmana izin var" sorusunu yanıtlar. İlişkilidirler çünkü bir sistem genellikle ne yapabileceğine karar vermeden önce kim olduğunu bilmelidir. Ama aynı şey değildirler. Onları tek şey olarak ele almak karışıklığa yol açar, bu yüzden iki soruyu ayrı tut.



Kimlik doğrulama, kimliğini bir sisteme kanıtlamak anlamına gelir. Gerçekten iddia ettiğin kişi olduğunu gösterme eylemidir. Bir sistem, karşı tarafta kimin olduğundan emin olmak için kimlik doğrulamayı kullanır. O olmadan sistem seni başkalarından ayırt edemez. Yani kimlik doğrulama kimlikle ilgilidir, izinlerle veya erişim haklarıyla değil.



Bir giriş ekranı, kimlik doğrulamanın genellikle gerçekleştiği yerdir. Forma bir kullanıcı adı ve parola yazarsın, sistem bunları zaten elinde bulunan saklı değerlerle karşılaştırır. İkisi eşleşirse sistem, iddia ettiğin kişi olduğunu kabul eder. Eşleşmezlerse erişim reddedilir. Bu kontrol, kimlik doğrulamanın özüdür.



Yetkilendirme, belirli bir kullanıcı için hangi eylemlerin ve verilerin izinli olduğuna dair karardır. Sistem kim olduğunu bildikten sonra gerçekleşir. Sistem kimliğine ve rolüne bakar, sonra ne yapabileceğine karar verir. Yetkilendirme izinler ve erişim haklarıyla ilgilidir, kimlikle değil. Kim olduğun göz önünde bulundurularak ne yapabileceğini yanıtlar.



Öğrencilerin ve öğretmenlerin ikisinin de oturum açtığı bir okul sistemi düşün. Herkes aynı giriş ekranını ve aynı tür kullanıcı adı ile parolayı kullanır. Kimlik doğrulama onlara aynı şekilde davranır ve her birinin kimliğini doğrular. Ama sistemin içinde öğrencilerin ve öğretmenlerin yapmasına izin verilen şeyler farklıdır. Bu farkın devreye girdiği yer yetkilendirmedir.



Okul sistemine oturum açan bir öğrenciyi izle. Kullanıcı adı ve parola saklı değerlerle eşleştiği için kimlik doğrulama başarılı olur. Öğrenci ardından bir sayfada kendi notlarını görüntüleyebilir. Bu, kimlik doğrulamanın çalıştığını ve sınırlı bir iznin verildiğini gösterir. Öğrenci yalnızca kendi notlarını görür, başkalarınınkini değil.



Şimdi aynı öğrenci bir notu değiştirmeye çalışsın. Sistem öğrencinin tam olarak kim olduğunu bilir, yani kimlik doğrulama zaten geçmiştir. Ama notları düzenlemek öğrenciler için izinli değildir, bu yüzden sistem eylemi reddeder. Bu ret bir yetkilendirme kararıdır. Tanınmak, her şeyi yapmaya izinli olmakla aynı şey değildir.



Bunu aynı okul sistemine oturum açan bir öğretmenle karşılaştır. Öğretmen bir kullanıcı adı ve parola yazar ve kimlik doğrulama aynı şekilde başarılı olur. Ama rol farklı olduğu için öğretmenin notları düzenlemesine izin vardır. Aynı giriş adımı, farklı izinler. Yetkilendirme öğretmene öğrencide olmayan haklar verir.



Başarılı bir oturum açma tüm verileri açmaz. Sistem tarafından tanınmak, içindeki her şeyle güvenilmekle aynı şey değildir. Oturum açan öğrenci diğer öğrencilerin notlarını göremez veya hiçbir notu değiştiremez. Yani tek başına kimlik doğrulama yeterli değildir. Sistem yine de tanınan her kullanıcının ne yapabileceğine karar vermelidir.



Uygulama, yalnızca girişte bir kez değil, her önemli işlemde izinleri kontrol etmelidir. Her hassas eylemin çalışmadan önce kendi yetkilendirme kontrolüne ihtiyacı vardır. Örneğin, bir notu düzenleme her denendiğinde kontrol edilmelidir. Kontrol atlanırsa yanlış kullanıcı yanlış şeyi yapabilir. Girişte bir kez kontrol etmek, sonraki eylemleri korumasız bırakır.



İki adımın sırasına dikkat et. Önce sistem kimlik doğrulama yoluyla kim olduğunu doğrular. Sonra yetkilendirme yoluyla ne yapabileceğine karar verir. Yetkilendirmenin anlamlı olması için bilinen bir kullanıcıya ihtiyacı vardır, çünkü izinler belirli bir kimliğe bağlıdır. Doğrulanmış bir kimlik olmadan sistem hangi hakların geçerli olduğuna karar veremez.



Yaygın bir hata, kimlik doğrulama ile yetkilendirmeyi aynı kelimeymiş gibi kullanmaktır. İnsanlar aslında kullanıcının bir şey yapmaya izinli olduğunu kastederken kullanıcının kimliğinin doğrulandığını söyler. İki kelimeyi ayrı tutmak, erişim konusunda kafanın karışmasını önler. Kimliği izinlerden ayırdığında tasarımın daha net ve daha güvenli olur.



Bir başka yaygın hata, girişe fazla güvenmektir. Bazıları oturum açmış bir kullanıcının sistemdeki her şeye ulaşması gerektiğini varsayar. Okul örneği bu varsayımın neden yanlış ve güvensiz olduğunu gösterir. Oturum açmış bir öğrenci yine de notları düzenlememelidir. Giriş kimliği kanıtlar, ama asla tüm verilere tam erişim anlamına gelmez.



Önemli bir işlemde izin kontrolünü unutmak ciddi bir hatadır. Sistem yalnızca kim olduğunu kontrol edip ne yapabileceğini hiç kontrol etmezse yanlış kullanıcı yanlış eylemi gerçekleştirebilir. Her önemli eylemin kendi yetkilendirme kontrolüne ihtiyacı vardır. Bunu atlamak, oturum açan herkesin içinden geçebileceği bir boşluk bırakır.



Temel farkı hatırla: kimlik doğrulama kim olduğundur, yetkilendirme ise ne yapabileceğindir. Bir giriş asla tüm verilere tam erişim anlamına gelmez. Sistem, yalnızca bir kez değil, her önemli işlemde izinleri kontrol etmelidir. Bu noktaları aklında tutarsan en yaygın erişim hatalarından kaçınırsın.