Oturum Yönetimi

Oturum kurulumunda ki kimlik doğrulama aşamasında başarılı bir doğrulama gerçekleştiyse 302 FOUND cevabı istemciye dönderilir.

Oturum anahtarının (Session ID) tahmin edilebilirlğği BurpSuit ve WebScrab gibi Proxy araçları ile yapılabilir.

Güvnli Oturum Anahtarın da Olması Gerekenler

- Harf ,sayı,büyük,küçük duyarlı olmalıdır.
- En az 16 karakter olmalıdır Yada +24 karakter olmalıdır.
- Parola içerisinde kullanıcı adı,kullanıcı id bilgisi,e-posta,adı vs. kullanıcıya ait bilgilerden kesitler bulundurulmamalıdır.
- Oturum ID 'si oluşturulurken zamanlama fonksiyonlarından kaçınılmalıdır.
- Algoritma oluşturulurken rastgele değer üreten fonksiyon seçimi doğru yapılmalıdır.Standart algoritmalar ile tekkrarlanabilen değerler üreten algoritmalar seçilmemelidir.Yada zaman , saat vs. parametrelere bağımlı değer ataması yapan fonksiyonlardan kaçınılmalıdır.
  Örneğin; Java'da random( ) yerine
  Securerandom( )
  seçilmedilir.

COOKİE

- Oturum anahtarının taşınmasında ve istemcide de saklanmasında yaygın olarak bir yöntemdir.

Cookie'lerin Özellikleri

- Secure
- HTTPONLY
- Domain ve Path Özelliği
- Expires özelliği

Secure özelliği

Normal isteklerde paketler HTTP ile gönderilirken secure özelliği aktif olduğunda paketler HTTPS protokolü kullanılarak gönderilir.Yani paketler şfrelenerek ağda taşınırlar.

HTTPONLY Özelliği

- Bu özellik aktif istemcilerin barındırdıkları Cookie'lere SCRIPTING kodları kullanılarak erişilmesi engellenmiş olur.
- XSS'e karşı bir önlemdir aynı zamanda.

Domain ve Path Özelliği

- Tüm domain va subdomainlerin Cookie bilgilerine Scripting kodları ile erişilmesine engel olmaktadır.
- Path özelliğide domain özelliği gibidir.
  Aynı domain içerisinde farklı klasörlerde 2 uygulama varsa ve Cookie değerlerinin karışmamasını istiyorsanız Path=/App1 ve Path=/App2 şeklinde kullanmamız lazım.

- Daha çok yönetim panellerinde kullanılmaktadır.

Expires Özelliği

- Expires özelliği ile cookie içerisinde bulunan değerlerin yaşam süresi belirlenmektedir.
- Bu özellik ikiye ayrılmaktadır.
    - Session Cookie:
      Expires ve Max-Age değeri atanmamış cookielerdir. Bunlar oturum açılınca bellekte tutulur ve tarayıcı kapatılınca bellekten silinir.
    - Persistent Cookie:
      Expires ve Max-Age değerleri atanmıştır.Tarayıcı kapatıldığında bile oturum bilgileri tutulmaya devam edilir.Belirtilen zamandan önce bir istek yapılırsa bir önceki Cookie değeriyle birlikte sunucuya gönderilirler.

Güvenli Cookie

- ✓ http kullanan uygulamalarda Secure özelliği aktif edilmelidir.
- ✓ Scripting dilleri ile erişimin kapatılması için HttpOnly Özelliğinin aktif olması gerekmetedir.
- ✓ Gerekmedikçe Persistent Cookie kullanılmamalıdır.Halka açık olan bilgisayarlarda risk daha fazladır.
- ✓ Donain ve Path bilgileri uygulamaya özgü bilgiler ile doldurulmalıdır.

Hasan Baskın

Adli Bilişim Mühendisliği

www.hasanbaskin.com