

Web Çerezleri (Cookies): Tanımı, İşlevi ve Güvenlik Boyutu

Web çerezleri, internet kullanıcılarının tarayıcıları aracılığıyla web siteleriyle etkileşim kurarken oluşturulan ve saklanan küçük veri dosyalarıdır. Bu dosyalar, kullanıcı deneyimini geliştirmek, oturum yönetimi sağlamak ve kişiselleştirilmiş içerik sunmak gibi çeşitli amaçlarla kullanılır.

1. Çerezin Tanımı

Çerez (cookie), bir web sitesinin tarayıcıya gönderdiği ve kullanıcının cihazında saklanan küçük metin dosyalarıdır. Bu dosyalar, kullanıcının site üzerindeki tercihlerini, oturum bilgilerini ve gezinme geçmişini kaydederek sonraki ziyaretlerde daha hızlı ve kişiselleştirilmiş bir deneyim sunar.

2. Çerez Türleri

Web çerezleri farklı amaçlara ve kullanım sürelerine göre sınıflandırılır:

a. Sürelerine Göre

Oturum Çerezleri (Session Cookies): Tarayıcı kapatıldığında silinir. Genellikle oturum yönetimi için kullanılır.

Kalıcı Çerezler (Persistent Cookies): Belirli bir süre boyunca cihazda saklanır. Kullanıcının tercihlerini hatırlamak için kullanılır.

b. Kaynağa Göre

Birinci Taraf Çerezleri (First-party Cookies): Ziyaret edilen web sitesi tarafından oluşturulur.

Üçüncü Taraf Çerezleri (Third-party Cookies): Reklam, analiz veya sosyal medya hizmetleri gibi harici servis sağlayıcılar tarafından oluşturulur.

3. Çerezlerin Kullanım Amaçları

Web çerezleri birçok farklı işlevi yerine getirir:

Oturum Yönetimi: Kullanıcının giriş yapmış olduğunu hatırlamak.

Kişiselleştirme: Dil tercihi, tema seçimi gibi kullanıcı ayarlarını saklamak.

Analitik: Kullanıcı davranışlarını analiz ederek site performansını değerlendirmek.

Reklamcılık: Kullanıcının ilgi alanlarına göre hedeflenmiş reklamlar sunmak.

4. Çerezlerin Teknik Yapısı

Bir çerez genellikle şu bilgileri içerir:

Ad (Name): Çerezin tanımlayıcı adı.

Değer (Value): Saklanan veri.

Alan Adı (Domain): Çerezin ait olduğu web sitesi.

Yol (Path): Çerezin geçerli olduğu URL yolu.

Süre (Expiration): Çerezin geçerlilik süresi.

Güvenlik Bayrağı (Secure/HttpOnly): Çerezin sadece HTTPS üzerinden iletilip ileilmeyeceğini ve JavaScript erişimine kapalı olup olmadığını belirler.

5. Çerezlerin Oluşturulması ve Yönetimi

Web geliştiricileri çerezleri genellikle HTTP yanıt başlıkları veya JavaScript aracılığıyla oluşturur:

HTTP Başlığı ile:

Code

```
Set-Cookie: username=ahmet; Expires=Wed, 21 Oct 2025 07:28:00 GMT; Path=/; Secure; HttpOnly
```

JavaScript ile:

javascript

```
document.cookie = "username=ahmet; path=/; expires=Wed, 21 Oct 2025 07:28:00 GMT";
```

6. Çerezlerin Güvenlik ve Gizlilik Boyutu

Çerezler kullanıcı deneyimini geliştirirken bazı güvenlik ve gizlilik riskleri de barındırır:

Çapraz Site Betikleme (XSS): Kötü niyetli kodlar çerezlere erişebilir.

Çapraz Site İstek Sahteciliği (CSRF): Oturum bilgileri kötüye kullanılabilir.

Takip ve Profilleme: Üçüncü taraf çerezleriyle kullanıcı davranışları izlenebilir.

Bu riskleri azaltmak için şu önlemler alınabilir:

HttpOnly ve Secure bayraklarının kullanılması.

Çerezlerin sadece gerekli olduğu durumlarda oluşturulması.

Kullanıcıdan açık rıza alınması (KVKK ve GDPR kapsamında).

7. Yasal Düzenlemeler

Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR) ve Türkiye'deki Kişisel Verilerin Korunması Kanunu (KVKK), çerezlerin kullanımı konusunda açık rıza ve bilgilendirme yükümlülüğü getirmiştir. Web siteleri, kullanıcıya çerez politikası sunmalı ve tercihlerine saygı göstermelidir.

8. Alternatif Teknolojiler

Çerezlerin yerine veya yanında kullanılabilecek bazı teknolojiler şunlardır:

Local Storage / Session Storage: Tarayıcıda veri saklamak için kullanılır, ancak sadece istemci tarafında çalışır.

IndexedDB: Daha büyük ve yapılandırılmış veri saklama imkanı sunar.

Server-side Session Management: Oturum bilgileri sunucu tarafında saklanır, çerez sadece oturum kimliği taşır.