Web Fundamentals

Muhammed Fatih YILMAZ

mfth78@hotmail.com

İÇERİK

- HTTP1.0 vs HTTP1.1vs HTTP2.0 vs HTTP3.0
- Cookiler Nedir? Niçin Kullanılır?
- httpOnly ve secure flag ne işe yarar?
- Session Fixation Nedir?

HTTP 1.0

HTTP nin yayınlanan ilk versiyonunda sadece serverdan get talepleri ile istek atılabiliyordu. İnternetin gelişmesiyle birlikte bu verimsiz bir hal almaya başladı kullanıcılar çoğaldı. 1996 yılında bu bağlamda HTTP1.0 yayınlandı.

Yenilikleri

- Header: Sadece kaynak ve methoddan oluşan önceki http istekleri HTTP1.0 ile Header'a alındı. Bu sayede metadatalarla protokol daha esnek ve genişletilebilir hale getirildi.
- Versioning: Kullanıcıların kullandıpı tarayıcıların versiyon bilgileri istek satırına eklendi.
- Status Code -> Status codeları sayesinde kullanıcılar istekğin başarılı olup olmadığını öğrenebilir hale geldi.
- Content Type -> HTTP başlığı sayesinde Content Type alanına özel olarak HTTP, HTML dosyasından başka belge türlerinide ekleyebilir hale geldi.
- New Methods -> POST ve HEAD metodları eklendi. Bu sayede sadece serverdan veri almanın yanı sıra gönderme de sağlandı

HTTP1.1

HTTP1.0 ardından bir sene sonra HTTP1.1 yeni güncellemelere ortaya çıktı.

Yenilikler

- Host-Header: Bu başlık, bir iletiyi proxy sunucular üzerinden yönlendirmenize olanak sağladığından ve web sunucunuz aynı sunucudaki farklı siteler arasında ayrım yapababildiğinden dolayı aynı ıp yi işaret eden 2 farklı adres varsa sunucu istemcinin hangisini istediğini bu sayede öğrenmiş olur.
- Persistent connections: HTTP1.0 da her rq rsp isteğinde yeni connection oluşturulurken bunun gelmesiyle birlikte tek connetionla daha fazla rq rsp işlemi gerçekleştirilebilir hale geldi.
- Continue Status: İstemci bu sayede sunucunun isteği çalıştırabildiğinden veya sunucu çalıştıramazken büyük bir istek göndermeyi engellemek için ortaya çıkmıştır. İstemci sadece HEADER gönderir ve sunucu 100 kodunu dönerse body kısmıyla devam eder.
- New Methods -> 6 tane extra method ekleniştir bunlar PUT, PATCH, DELETE, CONNECT, TRACE, ve OPTIONS. Put sayesinde kaynaklar değiştirileblir. PATCH sayesinde istediğimiz verileri güncelleyebiliriz. DELETE ile kayanağı direkt silebiliriz.
  Bunların yanı sıra bir sürü küçük geliştirmeler de yapılmıştır örneğin compression decompression yapma, çoklu dil desteği gibi

HTTP2.0

18 yıl aradan sonra HTTP1.1 ‘in ardından çıkarılan HTTP2.0 daha çok protokollerin performansını geliştirmek için ortaya çıktı.

YENİLİKLER

- Request Multiplexing: 1.1 versiyonu ardışık protokoldü yani her bir soya için tek istek yoluyordu. Fakat bu 2.0 sürümü ile gelen istekler toplu olarak alınıp tek TCP connection ile yollanmaya başladı. Bu sayede açılış hızında ki gecikmelerin önüne geçildi.
- Request prioritization -> Bu özellik sayesinde dosyaların yüklenme önceliğini belirten numaralandırmayı biz ayarlayabiliyoruz. Bu sayede yanıtları hangi sırayla beklediğimizi belirtebiliriz. Örneğin CSS dosyalarını JS dosyasındandan önce yüklenmesini istemek gibi
- Automatic compressing : Bir önceki sürümde isteklerin açıkça sıkıştırılımasını zorunlu kılmayız. Yani sıkıştırma olmadan da bize gelebilir fakat bu özellik sayesinde rqst ve rsp otomatik olarak sıkıştırılır.
- Connection Reset : server-client arasındaki bağlantıyı sebepler sonucu kapatıp hemen yenisini açmayı sağlıyor.
- Server Push : Server çok fazla istek birikimi olmasın diye clientin isteyeceği şeyleri önceden tahmin ederek clientin cachesine gönderir

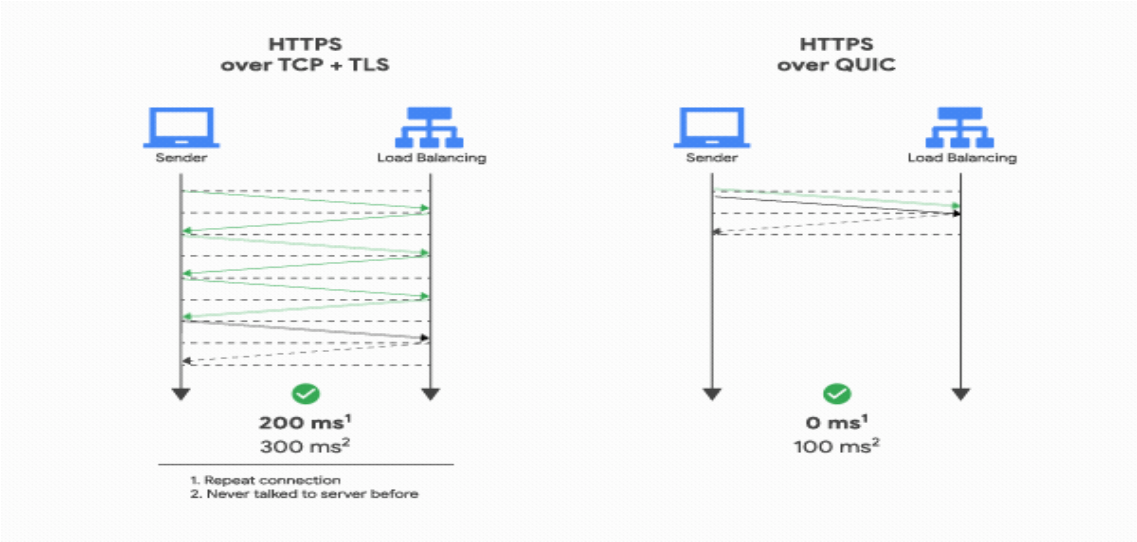
HTTP3.0

Bu versiyonda daha çok hızın ve güvenliğin artırılması göz önüne alınmıştır.

YENİLİKLER

- QUIC protokol : Bu protokol TCP yerine UDP protokolü üzerinden verilerin gönderilmesi amaçlanmıştır. QUIC hem trafiği hızlandırmak hemde güvenli hale getimek için tasarlanmıştır. TCP de aktarım sırasında bi hata meydana gelse bütün paketler aksıyodu fakat bu protokol sayesinde kaybolan paket sadece o paketteki verileri etkiler diğer veriler bundan etkilenmez . Sanki birisi trafik kazasına karışan arabaları sihirli bir şekilde yolun kenarına götürür, böylece araçlar yoldan geçmeye devam edebilir gibi örnekleyebiliriz.

Bu versiyon yerleşik şifrelemeye sahiptir. HTTPS portuna atanmasına gerek yoktur. Kendi içinde TLS 1.3 şifrelemesini çalıştırır.



QUIC PROTOCOL GİF

Cookiler Nedir ?

Cookiler web sitelerinin sizi tanıması için sizin cihazlarınıza kaydettiği geçici kimliktir.İnternette gezinirken ziyaret ettiğiniz web siteler cihazlarınıza bilgi dosyaları kaydeder. Bu dosyalar cihazlarınızın hafızasında saklanır. Daha sonra aynı siteleri ziyaret ettiğinizde bu kayıtlı bilgi dosyaları sayesinde siteler sizi tanıyabilir.Bilgileriniz bu dosyalara yazıldığından dolayı tekrar aynı web sayfalarını ziyaret ettiğinizde bilgilerinizi yeniden girmeye gerek duymazsınız. Bu kayıtlı bilgi dosyalarına cookie denir

Cookiler Niçin Kullanılır?

Cookiler birçok nedenle kullanılabilir. Kullanıcıların login bilgilerini ve tercihlerini hatırlamak için kullanılabilir. Aynı zamanda kendi araştırmalarına yönelik ürün tanıtım reklamları için kullanılabilir mesela ayakkabı yazdınız birkaç site ziyaret ettiniz bunu kaydedilen cookilere göre size ayakkabı reklamları karşınıza çıkabilir. Tracking konusunda da alışveriş siteleri daha önce bakmış olduğunuz ürünleri yeniden herhangi bir indirim veya stok durumuna göre sizin cookiniz üzerinden verileri öğrenip buna göre size bildirim yollayabilirler.

HTTP de Neden Cookilere İhtiyacımız Var ?

Kullanım kolaylığı sağladığı için örneğin bir siteye girdiğinizi düşünün burada kart bilgileriniz var aniden browseriniz kapansa bu hesap bilgilerini her defasında çıkış yaptıktan sonra bir daha girmeniz gerekecekti cookiler sayesinde sizin olduğunuzu anlayıp kaldığınnız yerden devam etmeinizi sağlar Ayrıca e ticaret siteleri veya ticaret ürünleri üzerine cookiler kullanılarak kişininin ilgi alanları belirlenip ona uygun daha isabetli satış pazarlama kararları verilir. Bu sayede hem kullancı hem de satıcı kendine gereken veriyi almış olur. Kullanıcı web sitesinde gezinirken, ziyaret ettiği her yeni sayfa tarayıcıyı sorgulayarak çerezi arar. Çerezin URLsi web sitesinin URLsi ile eşleşirse web sitesi oluşturulan unique idyi kullanarak kullanıcı bilgilerini sunucusundan alır. Bu şekilde web sitesi kullanıcının deneyimini göz atma geçmişini yansıtacak şekilde ayarlar.

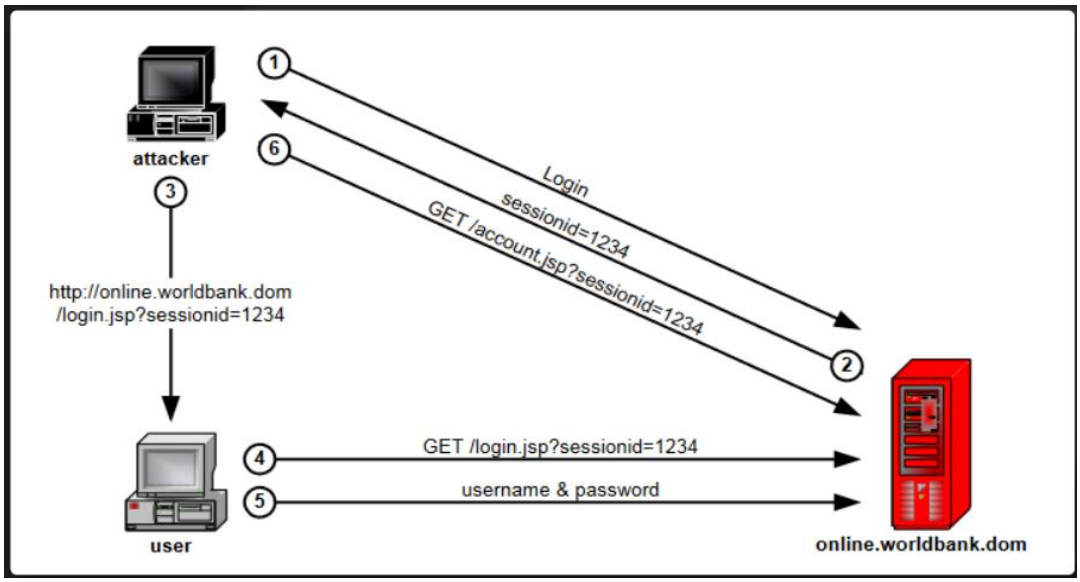
Cookideki HttpOnly ve secure flag nedir?

Server ilk requestten sonra response dönerken Set-Cookiyle cookie gönderilir. Bunun içinde bazen httpOnly ibaresiyle karşılaşırız. Bunun sebebi Cookie güvenliğiyle alakalıdır. Cookiler bir nevi kimliklerimiz olduğu için güvenli saklanması gereken unsurlardır. httpOnly sayesinde sadece http dosyaları cookiye erişir. Javascript dosyaları veya herhangş bir dosya erişemez. XSS saldırılarıyla session hackinge önlem olarak ortaya konmuştur.

Eğer secure flag kullanılırsa cookiler sade HTTPS üzerinden gönderilir. Saldırgan arada giden cookileri okuyamaz. HTTPS, kimlik doğrulama, veri bütünlüğü ve gizlilik sağlar.

Session Fixation Nedir ?

Kullanıcının oturum kimliği, oturum açma sırasında rastgele oluşturulmak yerine önceden sabitlendiğinden, bu saldırının adı Session Fixation "oturum sabitleme" saldırısı olarak adlandırılır.Bir Session Fixation saldırısında kurban saldırgan tarafından bilinen belirli bir session ID kullanması için kandırılır. Bu zaafiyetin ortaya çıkması loginden sonra yeni bir session ID verilmemesinden kaynaklanmaktadır. Kurbanını pcsisine login sessiın ID si hacker tarafından bilinen URL verilir kurban kendi hesabıyla login olunca o session ID üzerinden hacker kurban gibi kendini gösterip accounta erişim sağlayabilir.



Session Fixation Example