# Testing for Cookies Attributes (Çerezler için test özellikleri)

## Summary (Özet)

Web Çerezleri (burada çerez olarak adlandırılır) genellikle kötü amaçlı kullanıcılar için anahtar bir saldırı vektörüdür (genellikle diğer kullanıcıları hedeflemek) ve uygulama çerezleri korumak için her
zaman gerekli özeni göstermelidir.

HTTP, vatansız bir protokoldür, yani aynı kullanıcı tarafından gönderilen isteklere herhangi bir referans tutmaz. Bu sorunun giderilmesi için oturumlar oluşturuldu ve HTTP isteklerine eklendi. Tarayıcılar, test tarayıcısı depolamada tartışıldığı gibi, çok sayıda depolama mekanizması içerir. Rehberin bu bölümünde, her biri iyice tartışılır.

Tarayıcılarda en çok kullanılan oturum depolama mekanizması çerez depolamasıdır. Çerezler, sunucu tarafından bir dahil edilerek ayarlanabilir `Set-Cookie` HTTP yanıtında veya JavaScript üzerinden başlık. Kurabiyeler, aşağıdaki gibi çok sayıda nedenden dolayı kullanılabilir:

- Oturum yönetimi
- Kişiselleştirme
- İzleme

Çerez verilerini güvence altına almak için, endüstri bu çerezleri kilitlemeye ve saldırı yüzeylerini sınırlamaya yardımcı olmak için araçlar geliştirdi. Zamanla çerezler, kullanım ve korumada büyük
esneklik sağladığı için web uygulamaları için tercih edilen bir depolama mekanizması haline gelmiştir.

Çerezleri korumanın yolları şunlardır:

- Kurabiye Özellikleri
- Kurabiye Ön Sıfatları

## Test Objectives (Test Hedefleri)

- Uygun güvenlik yapılandırmasının çerezler için ayarlandığından emin olun.

## How to Test (Nasıl Test Edilir)

Aşağıda, her özniteliğin ve ön ekinin bir açıklaması tartışılacaktır. Test cihazı, uygulama tarafından düzgün bir şekilde kullanıldığını doğrulamalıdır. Çerezler, bir önleyici bir proxy kullanarak veya tarayıcının çerez kavanozunu inceleyerek incelenebilir.

## Cookie Attributes (Kurabiye Özellikleri)

## Secure Attribute (Güvenli Nitelik)

The (İngilizce) `Secure` sıfat, tarayıcıya yalnızca isteğin güvenli bir kanal üzerinden gönderilmesi durumunda çerezi göndermesini söyler. `HTTPS` . . Bu, çerezin şifrelenmemiş isteklerde geçmesini önlemeye yardımcı olacaktır. Uygulamaya her ikisine de ulaşılabiliyorsa `HTTP` ve `HTTPS` Bir saldırgan, kullanıcıyı çerezlerini korunmayan isteklerin bir parçası olarak göndermeye yönlendirebilir.

## HttpOnly Attribute (HttpT Sadece Atıfta)

The (İngilizce) `HttpOnly` Hindeti, oturum sızıntısı gibi saldırıları önlemeye yardımcı olmak için
kullanılır, çünkü çerezin JavaScript gibi bir istemci tarafı komut dosyası aracılığıyla erişilmesine izin vermez.

> Bu, XSS saldırılarının tüm saldırı yüzeyini sınırlamaz, çünkü bir saldırgan hala kullanıcının yerine istek gönderebilir, ancak XSS saldırı vektörlerinin erişimini son derece sınırlar.

## Domain Attribute (Alan Adı Atar)

The (İngilizce) `Domain` Öznitelik, çerezin etki alanını HTTP isteğinin yapıldığı sunucunun alanına
kıyaslamak için kullanılır. Domain eşleşiyorsa veya bir subdomain ise, o zaman `path` Bir sonraki ipucu kontrol edilecek.

Sadece belirtilen alana ait olan ana bilgisayarların bu alan adı için bir çerez ayarlayabilir. Ek olarak, bu `domain` nitelik üst düzey bir alan olamaz (örneğin `.gov` ya

da `.com`) sunucuların başka bir alan adı için keyfi çerezler ayarlamasını önlemek için (bir çerez ayarlamak gibi `owasp.org`). Alan adı özelliği belirlenmezse, çerezi oluşturan sunucunun ana adı, varsayılan değeri olarak kullanılır. `domain`. .

Örneğin, bir çerez bir uygulama tarafından ayarlanırsa `app.mydomain.com` Alan adı özelliği olmadan, çerez sonraki tüm talepler için yeniden gönderilecektir. `app.mydomain.com` ve onun alt doyanı (böylece `hacker.app.mydomain.com`, ama değil `otherapp.mydomain.com`. . Bir geliştirici bu kısıtlamayı gevşetmek istiyorsa, o zaman ayarlayabilirdi. `domain` atfedilmesi için atfedilmesi `mydomain.com`. . Bu durumda çerez tüm taleplere gönderilecektir. `app.mydomain.com` ve `mydomain.com` Subdominalar, örneğin `hacker.app.mydomain.com`, ve hatta `bank.mydomain.com`. . Bir subdomain'de savunmasız bir sunucu varsa (örneğin, `otherapp.mydomain.com`) ve bu `domain` Hindifikasyon çok gevşek bir şekilde belirlenmiştir (örneğin, `mydomain.com`), o zaman savunmasız sunucu, tam kapsamı boyunca çerezleri (sezon belirteçleri gibi) hasat etmek için kullanılabilir. `mydomain.com`. .

## Path Attribute (Yol Atıfta)

The (İngilizce) `Path` özellik, çerezlerin kapsamını ile birlikte belirlemede önemli bir rol oynar `domain`.
. Etki alanına ek olarak, çerezin geçerli olduğu URL yolu da belirtilebilir. Alan adı ve yol eşleşirse, çerez talepte gönderilecektir. Tıpkı etki alanı özniteliğinde olduğu gibi, yol özelliği çok gevşek bir şekilde ayarlanırsa, uygulamayı aynı sunucudaki diğer uygulamaların saldırılarına karşı savunmasız bırakabilir. Örneğin, yol özelliği web sunucusu köküne ayarlanmışsa
`/` Daha sonra uygulama çerezleri aynı etki alanı içindeki her uygulamaya gönderilecektir (birden fazla uygulama aynı sunucunun altında bulunursa). Aynı sunucunun altındaki birden fazla uygulama için birkaç
örnek:

- `path=/bank`
- `path=/private`
- `path=/docs`
- `path=/docs/admin`

## Expires Attribute (Nitelik Süresi Doldurur)

The (İngilizce) `Expires` Bağlılık şöyle kullanılır:

- Kalıcı kurabiye seti
- Bir seans çok uzun yaşarsa ömürleri sınırlayın
- Bir kurabiyeyi geçmiş bir tarihe ayarlayarak zorla çıkarın

Oturum çerezlerinin aksine, çerez süresi dolana kadar tarayıcı tarafından kalıcı çerezler  kullanılacaktır. Son kullanma tarihi belirlenen süreyi aştıktan sonra, tarayıcı çerezi siler.

## SameSite Attribute (SameSite Atıf)

The (İngilizce) `SameSite` Bir çerezin çapraz site istekleriyle birlikte gönderilmemesi gerektiğini
iddia etmek için öznitelik kullanılır. Bu özellik, sunucunun çapraz sorgu bilgi sızıntısı riskini azaltmasını sağlar. Bazı durumlarda, siteler arası sahtecilik saldırılarını önlemek için risk azaltma (veya derinlik mekanizmasında savunma) stratejisi olarak da kullanılır. Bu özellik üç farklı modda
yapılandırılabilir:

- `Strict`
- `Lax`
- `None`

## Strict Value (Katı Değer)

The (İngilizce) `Strict` değer en kısıtlayıcı kullanımıdır `SameSite` Tarayıcının çerezi üst düzey gezinme olmadan yalnızca birinci taraf bağlamına göndermesine izin verir. Başka bir deyişle, çerezle ilişkili veriler yalnızca tarayıcı URL çubuğunda gösterilen mevcut siteyi eşleştiren
isteklere gönderilecektir. Kurabiye, üçüncü taraf web siteleri tarafından oluşturulan taleplere gönderilmeyecektir. Bu değer özellikle aynı alanda gerçekleştirilen eylemler için önerilir. Bununla birlikte, kullanıcı navigasyon deneyimini olumsuz yönde etkileyen bazı oturum yönetim sistemleri ile bazı sınırlamalara sahip olabilir. Tarayıcı, çerezi üçüncü taraf bir etki alanından veya e-postadan oluşturulan herhangi bir istekle göndermeyeceği için, kullanıcının zaten doğrulanmış bir oturumu olsa bile tekrar oturum açması gerekecektir.

## Lax Value (Gevşek Değer)

The (İngilizce) `Lax` değerden daha az kısıtlayıcıdır `Strict` . . URL, bağlantı üçüncü taraf bir alandan gelse bile, URL'nin etki alanına (birinci taraf) eşitse gönderilecektir. Bu değer çoğu tarayıcı
tarafından varsayılan davranış olarak kabul edilir, çünkü daha iyi bir kullanıcı deneyimi sağlar.
`Strict` Değer. Çerezlerin onlara erişmek için gerekli olmayabileceği görüntüler gibi varlıkları tetiklemez.

## None Value (Hiçbir değer yok)

The (İngilizce) `None` değer, tarayıcının çerezi çapraz site taleplerine göndereceğini belirtir (uygulamadan önceki normal davranış `SamseSite` Sadece eğer öyleyse `Secure` Nitelik de kullanılır, *örneğin.* `SameSite=None; Secure` . . Herhangi bir belirtmemek yerine tavsiye edilen bir değerdir. `SameSite` değer, kullanımı zorladığı için `secure` Bir özellik.

## Cookie Prefixes (Kurabiye Ön Sıfatları)

Tasarım çerezleri, içinde saklanan bilgilerin bütünlüğünü ve gizliliğini garanti etme yeteneklerine sahip değildir. Bu sınırlamalar, bir sunucunun belirli bir çerezin niteliklerinin nasıl yaratımda
belirlendiği konusunda güven duymasını imkansız kılar. Sunuculara bu tür özellikleri geriye doğru uyumlu bir şekilde vermek için, endüstri kavramını tanıttı. `Cookie Name Prefixes` Bu tür ayrıntıları çerez adının bir parçası olarak gömülü geçmeyi kolaylaştırmak.

## Host Prefix (Ev sahibi Prefix)

The (İngilizce) `__Host-` Prefix, çerezlerin aşağıdaki koşulları yerine getirmesini bekler:

1. Kurabiye ile ayarlanmalıdır `Secure` Bir özellik.
2. Çerez, kullanıcı temsilcisi tarafından güvenli kabul edilen bir URI'den ayarlanmalıdır.
3. Sadece kurabiyeyi ayarlayan ve herhangi bir şey içermemeli `Domain` Bir özellik.

4. Kurabiye ile ayarlanmalıdır `Path` Bir değere sahip bir özellik `/` Böylece ev sahibine her türlü talebe gönderilir.

Bu nedenle, kurabiye `Set-Cookie: __Host-SID=12345; Secure; Path=/` Aşağıdakilerden herhangi biri her zaman reddedilirken kabul edilir:

`Set-Cookie: __Host-SID=12345Set-Cookie: __Host-SID=12345; SecureSet-Cookie: __Host-SID=12345; Domain=site.exampleSet-Cookie: __Host-SID=12345; Domain=site.example; Path=/Set-Cookie: __Host-SID=12345; Secure; Domain=site.example; Path=/`

## Secure Prefix (Güvenli Ön Söndürme)

The (İngilizce) `__Secure-` önek daha az kısıtlayıcıdır ve vakaya duyarlı ipin eklenmesiyle getirilebilir `__Secure-` - Kurabiye adına. Öne fikre uyan herhangi bir kurabiye `__Secure-` Aşağıdaki koşulları yerine getirmesi beklenir:

1. Kurabiye ile ayarlanmalıdır `Secure` Bir özellik.
2. Çerez, kullanıcı temsilcisi tarafından güvenli kabul edilen bir URI'den ayarlanmalıdır.

## Strong Practices (Güçlü Uygulamalar)

Uygulama ihtiyaçlarına ve çerezin nasıl işlemesi gerektiğine bağlı olarak, öznitelikler ve ön ekler uygulanmalıdır. Kurabiye ne kadar çok kilitlenirse o kadar iyi.

Tüm bunları bir araya getirerek, en güvenli çerez özellik yapılandırmasını şu şekilde tanımlayabiliriz: `Set-Cookie: __Host-SID=<session token>; path=/; Secure; HttpOnly; SameSite=Strict` . .

## Tools (Araçlar)

## Proxy'yi Yakalamak

- OWASP Zed Saldırı Proxy Projesi
- Web Proxy Burp Suite yakınındaki oteller

## Tarayıcı Ekleme

- FF Quantum için Taper Verileri

- FireFox için "FireSheep"
- Chrome için “EditThisCookie”
- FireFox için "Cookiebro - Cookie Manager"

## Referance (Referanslar)

- RFC 2965 - HTTP Devlet Yönetimi Mekanizması
- RFC 2616 – Hipertext Transfer Protokolü – HTTP 1.1
- Same-Site Çerezler - taslak-ihat-htpbis-sahte-sahte-sahne-site-00
- Set-Cookie'nin önemli "sonuçları" özelliği
- URL ve Sayfa Bedeninde Sadece Oturum Kimliği