Feature Policy Header

Feature Policy kullanıcıların tarayıcılarda görüntüledikleri web sitesinde hangi feature (mikrofon, kamera, …) ve API'ları (geo konumlama,...) kullanabileceğini / izinli olduklarını kontrol eden bir http **response** başlığıdır.

Http response paketleri feature policy başlığı ile gönderildiklerinde gelen paketler tarayıcıya belirtilen feature veya api deaktif halde yansıyacaktır. Tarayıcıda (arayüzde) kullanıcı deaktif bu feature ve api'ı aktif edemeyecektir. Çünkü response paket okunmuş / render edilmiş halde tarayıcısına yasıyacaktır. Bu sayede çeşitli ataklar altında kalabilecek kullanıcıya arayüzde yetki kısıtlaması yaparak bir koruma sağlanmış olacaktır. Kullanıcının deaktif feature veya API'ları eğer web uygulamada mevcut ama örneğin belirtilen sayfalarda kullanılamaz durumdalarsa kullanılabilmesi için gelen http response başlığını düzenleyerek tarayıcısına yansıtması gerekecektir. Bunu normal bir kullanıcı yapmayacağı için ve sadece tarayıcı arayüzünde kendisine sunulduğu kadarıyla gezinme işlemlerini yapacağı için normal kullanıcılar kendilerine gelen çeşitli ataklardan (mikrofon dinleme, konum bilgisini alma, …) korunacaktır.

> Not:
> Eğer yerel ağda bir saldırı hazırlığı içerisinde kimse varsa yerel ağ saldırısı mitm yapabileceği için feature policy başlığını manipule edebilir ve sonraki ataklarına zemin hazırlayabilir.

Feature Policy başlığı response paketlerde şu şekilde kullanılır:

```
Feature-Policy: <directive> <allowlist>
```

Direktif, feature veya api adını alır. Allowlist ise site içerisinde direktifin izinli olduğu kaynakları alır. Örneğin,

```
Feature-Policy: microphone 'none'; geolocation 'none'
```

dersek web uygulamasını tarayıcılarında görüntüleyen kullanıcıların mikrofon ve geo konumlama API'nı sitenin heryerinde kullanılamaz / kapalı tut demiş oluruz.

Direktiflere örnek olarak aşağıdakiler verilebilir:

```
Directives:

autoplay        // Uygulama görüntülenirken medya içeriklerinin otomatik
                // oynatılıp oynatılmayacağını kontrol eder. <video> ve <audio>
                // html etiketlerindeki autoplay attribute'una göre baskındır.
                // Bu direktif örneğin; rahatsız edici şakaların (sürekli medya
                // içeriklerinin otomatik oynatılması ve kullanıcıyı bıktırmanın)
                // önüne geçmek için kullanılabilir. Not: Verilen örnek, örneğin
                // sayfa içerikleri manipule edilebilmiş ve sunucudan çıkılmış
                // bir saldırıda sunucu konfigurasyon ayarları sayesinde yapılan
                // şakanın önüne geçilebilmesini ifade etmektedir.

camera          // Uygulama görüntülenirken video girdisinin kullanılıp
                // kullanılamayacağını kontrol eder.

geolocation     // Uygulama görüntülenirken kullanıcı konum bilgisinin alınıp
```

// alınamayacağını kontrol eder.

microphone // Uygulama görüntülenirken kullanıcı mikrofon girdisinin
// alınıp alınamayacağını kontrol eder.

speaker // Uygulama görüntülenirken ses içeriklerinin dışarı herhangi
// bir metotla verilip verilemeyeceğini kontrol eder.

usb // Uygulama görüntülenirken “WebUSB” api’nın kullanılıp
// kullanılamayacağını kontrol eder.

...

Allowlist anahtar kelimeleri (tamamı) ise şu şekildedir:

Allowlist:

*	Direktifte belirtilen feature * (yıldız) allowlist anahtar kelimesi ile bu dökümanda ve bu dökümanın içerisindeki kaynak adresi fark etmeksizin taranabilir tüm alt içeriklerde (iframe’lerde) izinli / kullanılabilir olur.
'self'	Direktifte belirtilen feature ‘self’ allowlist anahtar kelimesi ile bu dökümanda ve bu dökümanın adresiyle aynı olan bu döküman içerisindeki taranabilir tüm alt içeriklerde (iframe’lerde) izinli / kullanılabilir olur.

'src'	(*Bu anahtar kelime kullanılırsa sadece <iframe> html etiketleri ndeki html attribute’u olan allow üzerinde izin çalışması / düzenlemesi yapar*). Direktifte belirtilen feature ‘src’ allowlist anahtar kelimesi ile bu dökümanın içerisindeki yalnızca taranabilir alt içeriklerde (iframe’lerde) izinli / kullanılabilir olur. Not: Eğer ‘src’ yerine bir url adresi girilirse dökümandaki tüm alt içeriklerde (iframe’lerde) src attribute’u bu url adresi ile eşleşmekteyse direktif izinli / kullanılabilir olur. Örneğin;
	
	// Feature Policy başlığı
	// ((Feature-Policy: fullscreen 'src'))
	// şeklindeyken istemci tarafında aşağıdaki <iframe> ile gelen
	// içerik tam ekran modunda gösterilebilirdir. Çünkü direktifte
	// allowlist olarak src belirtilmektedir ve böylece iframe’in src’un
	// daki url adres izinli denmektedir. Dolayısıyla iframe’den gelen
	// içerik için fullscreen (tam ekran) direktifi kullanılabilirdir / izinlidir.
	
	<iframe id="frame" src="https://example.net/" ></iframe>
	
	(*implicitly*)
	
	<iframe id="frame" allow="fullscreen 'src'"
	src="https://example.net/" ></iframe>

	// Feature Policy başlığı
	// ((Feature-Policy: https://example.com))
	// şeklindeyken istemci tarafında aşağıdaki <iframe> ile gelen
	// içerik tam ekran modunda gösterilemezdir. Çünkü direktifte
	// allowlist olarak belirli bir url (https://example.**com)** belirtilmek
	// tedir ve iframe'in src'undaki url adres ile eşleşme olmamaktadır.
	// Eşleşme olmadığından iframe'den gelen içerik için fullscreen
	// (tam ekran) direktifi kullanılabilir / izinli değildir.
	
	<iframe id="frame" src="https://example.net/" ></iframe>
	
	(*implicitly*)
	
	<iframe id="frame" allow="fullscreen https://example.com"
	src="https://example.net/" ></iframe>

'none'	Direktifte belirtilen feature 'none' allowlist anahtar kelimesi ile bu dökümanda ve bu dökümanın içerisindeki kaynak adresi fark etmeksizin taranabilir tüm alt içeriklerde (iframe'lerde) kapalı / kullanılamaz olur.
<origin(s)>	Direktifte belirtilen feature <origin(s)> kısmında belirtilen url'ler ile bu dökümanda ve bu dökümanın içerisindeki taranabilir tüm alt içeriklerde (iframe'lerde) kaynak url eşleşmeleri olduğu takdirde kullanılabilir / izinli olur. Not: Direktife birden fazla izinli url eklemek için url 'ler arasına boşluk konur.

Aşağıda örnek bir Feature Policy başlığı gösterilmiştir;

Nginx sunucular için /etc/nginx/conf.d/security.conf dosyasına eklenen konfigurasyon satırı

...
add_header Feature-Policy "geolocation none;midi none;notifications none;push none;sync-xhr none;microphone none;camera none;magnetometer none;gyroscope none;speaker self;vibrate none;fullscreen self;payment none;";

Kaynaklar

https://w3c.github.io/webappsec-feature-policy/
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy
https://www.openprogrammer.info/2019/02/06/how-to-secure-web-application-headers-with-nginx/