HTTP Güvenlik Başlıklarının Bir Tablosu

HTTP Güvenlik Başlığı	Açıklama	Örnek
Strict-Transport-Security (HSTS)	Web sitesinin yalnızca HTTPS üzerinden erişilen bilmesini sağlar.	`Strict-Transport-Security: max-age=31536000; includeSubDomains; preload`
X-Frame-Options	Web sitesinin başka bir web sitesi tarafından iFrame de yüklenmesini engeller.	`X-Frame-Options: DENY`
X-XSS-Protection	Web sitesinin Cross-Site Scripting (XSS) saldırılarına karşı korunmasına yardımcı olur.	`X-XSS-Protection: 1; mode=block`
X-Content-Type-Options	Web sitesinin içeriğinin yanlış türde yorumlanmasını önler.	`X-Content-Type-Options: nosniff`
Content-Security-Policy (CSP)	Web sitesinin hangi kaynaklardan içeriği yükleyebileceğini kontrol eder.	`Content-Security-Policy: default-src *; img-src *; script-src * 'unsafe-eval'; style-src * 'unsafe-inline'`
Public Key Pinning (PKP)	Web sitesinin hangi anahtarların kullanılarak şifrelendiğini tanımlar.	`Public-Key-Pins: pin-sha256="base64:<public_key_hash_1>; pin-sha256="base64:<public_key_hash_2>"`
X-Download-Options	Web sitesinin indirilen dosyaları engellemesini sağlar.	`X-Download-Options: noopen`
Referrer-Policy	Web sitesinin referans URL'sinin nasıl iletileceğini kontrol eder.	`Referrer-Policy: no-referrer` `Referrer-Policy: origin-when-cross-origin`
Expect-CT	Web sitesinin bir Content-Security-Policy (CSP) ihlali durumunda nasıl davranacağını tanımlar.	`Expect-CT: enforce`

Cache-Control	Web sitesinin önbelleğe alınma şeklini kontrol eder.	`Cache-Control: max-age=3600` `Cache-Control: no-store`
Clear-Site-Data	“Kullanıcı oturumu kapattıktan sonra uygulamanızdaki gizli bilgilerin tarayıcı tarafından kullanılmadığından emin olmak istiyorsanız Clear-Site-Data başlığını ayarlayabilirsiniz.” Web sitesinin çerezleri, önbelleği ve diğer verileri nasıl temizleyeceğini kontrol eder.	`Clear-Site-Data: cache, cookies, storage, executionContexts`