**Missing X-Frame-Options Header (Eksik X-Frame-Options Başlığı)**

Zaafiyet riski : düşük

**Bu Zaafiyet Nedir ?**

Headerlar, HTTP'nin hem istek hem de yanıt mesajlarında yer alan ve mesajın meta bilgilerini taşıyan bölümlerdir.

Bu meta bilgileri, istekler için, talep edilen mesajın dili, tipi, browserın sakladığı yetki bilgileri, önbellekte tutulan içeriğe ait bilgiler olabileceği gibi; yanıt yani response mesajlarında ise, içeriğin boyutu ve tipi, bellekte saklanma tercihleri, sunucu bilgileri, tarih ve saati, istemci tarafında set edilecek credentials gibi, bir takım bilgilerdir.

Eksik X-Frame-Options başlığı, bu web sitesinin bir clickjacking saldırısı riski altında olabileceği anlamına gelir. X-Frame-Options HTTP başlık alanı, tarayıcının iletilen kaynağı bir çerçeve içinde mi yoksa bir iframe içinde mi oluşturması gerektiğini belirten bir ilkeyi belirtir.

**Clickjacking nedir ?**

UI Redress Attack olarak da bilinen Clickjacking saldırısı **sızma testlerinde sık karşılaşılan bir zafiyettir**. Siber saldırgan, güvenli olarak görünen web sayfası kullanıcılarını güvensiz bir sayfaya yönlendirerek manipüle ettiği bu kullanıcıların işlem yapmasını hedef alır.

**Sitede hangi istek’te header’in kısmının eksik olduğu keşfedildi?**





**Çözüm Önerisi:**

1. Tarayıcıya diğer alanlardan gelen çerçevelemeye izin vermemesi talimatını veren HTTP yanıt başlıklarında uygun X-Frame-Options'ın gönderilmesi.
2. ALLOW-FROM URLIBelirli bir URL'ye kendisini bir iframe içinde yüklemesi için izin verir. Ancak lütfen buna dikkat edin, tüm tarayıcılar bunu desteklemez.
3. Geçerli çerçevenin en üst düzey pencere olmasını sağlamak için kullanıcı arayüzünde savunma kodu kullanmak.