**Bilgi Sistemleri ve Güvenliği**

**170541061**

**-**

**Tahir Bayraktar**

**[Possible] Cross-site Request Forgery (Siteler Arası İstek Sahteciliği)**



Suçlu, olası bir Siteler Arası İstek Sahteciliği tespit etti. CSRF çok yaygın bir güvenlik açığıdır. Kullanıcıyı, o anda kimliğinin doğrulandığı bir web uygulamasında istenmeyen eylemler yürütmeye zorlayan bir saldırıdır.

**TANIM**

CSRF (Cross Site Request Forgery) genel yapı olarak bir web sitesinin açığından faydalanarak site kullanıcılarının istekleri dışında sanki o kullanıcıymış gibi erişerek işlem yapılması sürecini içerir. Genellikle GET requestleri ve SESSION işlemlerinin doğru kontrol edilememesi durumlarındaki açıklardan saldırganların faydalanmasını sağlamaktadır.

**ETKİ**

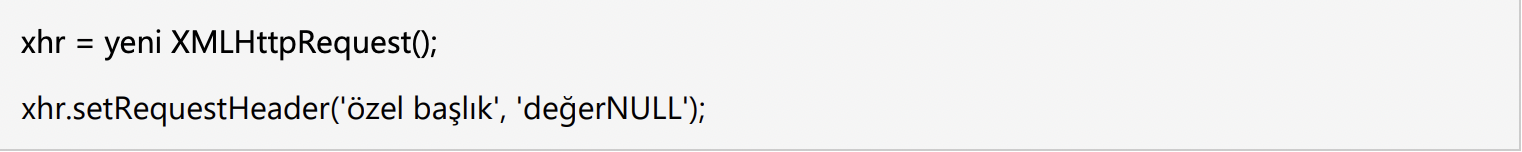
Saldırgan, uygulamaya bağlı olarak, kullanıcı ekleme, içerik değiştirme, veri silme gibi kullanıcı tarafından yapılabilecek eylemlerden herhangi birini yükleyebilir. Kurbanın kullanabileceği tüm işlevler saldırgan tarafından kullanılabilir. Bu kuralın tek istisnası, yalnızca meşru kullanıcının bilebileceği (kullanıcının şifresi gibi) ek bilgiler gerektiren bir sayfadır.

**ÇÖZÜM**

• İsteğin yetkili bir kaynaktan gelip gelmediğini belirlemek için kullanılabilecek her HTTP isteğinde ek bilgiler gönderin. Bu "doğrulama belirteci", kullanıcının hesabına halihazırda erişimi olmayan saldırgan için tahmin edilmesi zor olmalıdır. Bir istekte doğrulama belirteci eksikse veya belirteç beklenen değerle eşleşmiyorsa, sunucu isteği reddetmelidir.

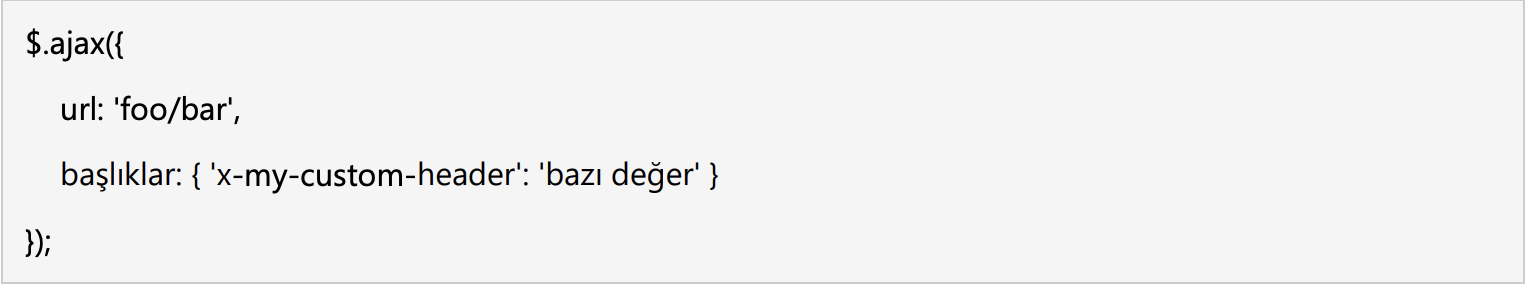
• Ajax isteğinde form gönderiyorsanız, tarayıcı sitelerin başka bir siteye özel HTTP üstbilgileri göndermesini engellediği, ancak sitelerin XMLHttpRequest kullanarak kendilerine özel HTTP üstbilgileri göndermesine izin verdiği için CSRF'yi önlemek için özel HTTP üstbilgileri kullanılabilir. o JavaScript'teki yerel XMLHttpRequest (XHR) nesnesi için;

.



JQuery için, özel bir başlık (veya başlık kümesi) eklemek istiyorsanız,

a. bireysel istek



b. her istek

