HTML Form without CSRF Protection

a. Cross Site Request Forgery Nedir?

Cross Site Request forgery saldırısı kullanıcının oturum açtığı bir web sitesi yan sekmedeyken saldırganın sitesine uğraması ya da saldırgandan gelen mail'i açması sonrası gelen linki tıklamasıyla (ya da tetiklemesiyle) beraber oturum açtığı web sitesinde istemediği bir eylemi gerçekleştirmesine denir. Örneğin kullanıcı bir bankacılık sitesinde oturum açmış olabilir ve yan sekmede ise saldırganın sitesine ya da mail'ine yönlenmiş olabilir. Saldırganın sayfasında ya da mail'inde img tag'ına eklenmiş form submit'leme linki ile istemeden bankacılık web sitesine bir talepte bulunabilir ve belki de saldırganın hesabına para transfer edebilir.

Ayrıntılı bilgi için bkz. 19. CSRF Nedir ve Nasıl SameSite ile Tamamen Önlenir.docx

b. CSRF Token Nedir?

CSRF Token html form'ları içerisine konan bir hidden alanındaki değerdir. Kullanıcı her form submit'lemesinde html formdaki token'ı da gönderir ve sunucu gönderdiği token'ı aldığını görünce submit işlemini gerçekleştirir. Eğer gönderdiği token değil de başka bir değerde veri geri dönerse de submit işlemini gerçekleştirmez.

c. HTML Form without CSRF Protection Zafiyetini Kapama [Severity: Medium]

Bu zafiyet csrf token'ları ile kapanır. CSRF Token html form'ları içerisine konan bir hidden alanındaki değerdir. Kullanıcı her form submit'lemesinde html formdaki token'ı da gönderir ve sunucu gönderdiği token'ı aldığını görünce form submit işlemini gerçekleştirir. Eğer gönderdiği token değil de başka bir değerde token geri dönerse de submit işlemini gerçekleştirmez. Böylece saldırganlar bir web sayfası ya da mail aracılığıyla kullanıcılara form submit'lemesi yaptıramayacaklardır ve istenmeyen sonuçların önüne geçilmiş olacaktır.

Not: Form submit'leme işlemi eğer ajax talepleri ile gerçekleştiriliyorsa token'lar ajax kodlaması ile taleplere başlık olarak eklenmelidir ve sunucu, kontrolü ajax taleplerinin başlığına bakarak sağlamalıdır.

Not: Aşağıdaki False Positive Ayrımı başlığını oku.

d. False Positive Ayrımı

Login formları için token olmasa da olur. Önemli olan oturum açmış bir kullanıcının karşılaşabileceği yetkiye dayalı bir formda token'ın olmasıdır. Çünkü saldırganın isteyeceği şey zorla kullanıcıyı çereziyle beraber bir yetki isteyen formu submit'leştirmesidir. Dolayısıyla yetkiye dayalı form'lar bulursan ve hidden olarak token yoksa bu durumu raporla.

Kaynak

https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/cross-site-request-forgery-in-login-form/