

Web Uygulamalarında DoS Denetimi

Bedirhan Urgun, Mayıs 2010, WGT E-Dergi 5. Sayı

Hizmet Dışı Bırakma (DoS) saldırıları sistem kaynaklarının hedef servis hizmet veremeyecek şekilde harcanmasıdır. Genellikle ağ tabanlı olan bu saldırılar (mesela, syn flood) web uygulamalarında da etkili olabilmektedirler.

Saldırının hedef uygulamadaki bir özelliği veya hatayı sömürerek gerçekleştirebildiği hizmet dışı bırakma saldırıları uygulama geliştiriciler tarafından etkileri büyük ölçüde kısıtlanabilir ve bazen tamamen yok edilebilir.

Saldırı Vektörleri

Web uygulamalarına yönelik DoS saldırılarının farklı varyasyonlarını aşağıdaki şekilde listeledik;

Kullanıcı Hesap Kilitlemesi

Kimlik doğrulama sürecini hedef alan bu saldırı vektöründe, saldırgan sistem üzerinde tanımlı kullanıcıların hesaplarını kilitleyerek, sisteme girmelerini engellemeyi amaçlar. Daha çok kullanıcı isimlerinin bulunması ve bu isimlere bir şifre deneme/yanılması yapılmış gibi gerçekleştirilen bu saldırıda, uygulama tarafında alınan güvenlik önlemleri sömürülür.

Şifre deneme/yanılma saldırılarına karşı alınan önlemlerden en geneli, şifresi denenen kullanıcının hesabının bir müddet kilitlenmesidir. Bu güvenlik kontrolü kullanılarak kullanıcıların hesapları kilitlenebilir.

Otomatik Form Gönderme

Web sitelerinde bulunan iletişim formları, başvuru formları, haber ver formları kullanıcılar tarafından doldurularak uygulamaya gönderilirler. Bu gönderimlerin otomatik bir script yardımı ile yapılabilmesi sistem kaynaklarının bitirilmesinde bir çok şekilde kullanılabilir.

Örnek bir saldırı, bu tür formlarının POST edilmesi sonucunda sorumlu bir gruba mail gönderilmesidir. Otomatik bir betik sayesinde gönderilen istekler, uygulama tarafında işlendikten sonra bir kişiye veya gruba mail/SMS atmak şeklinde değerlendirilirler. Bu geçersiz değerlerle dolu isteklerin sayısı arttıkça, mail/SMS gönderilen kişinin veya grubun çalışma süreçleri sekteye uğratılacaktır.

Veritabanı Wild Card Sorguları

MS SQL Server kullanan web uygulamalarında görülebilecek bir hizmet dışı bırakma senaryosu, SQL Server teknolojisinin sağladığı “joker karakterler” yardımı ile gerçekleştirilebilir. Joker karakterler, SQL sorgularında LIKE operatörü ile kullanılarak, tam olarak aranan kelimeler bilinmeden veritabanında kayıt aramaya yarar.

eşitleyerek, uygulamanın hafızasında çok büyük bir resim üretmeye çalışmasını tetikleyebilir. Bu da sunucuda hafıza kaynağının tüketilmesine neden olacaktır.