Kullanıcı Hesap Adlarının Tespiti

Onur Yılmaz, Ağustos 2010, WGT E-Dergi 6. Sayı

Uygulamada kayıtlı bulunan kullanıcı adlarının 'neden' tespit edilmek istendiğini maddelerle sıralamaya çalışırsak;

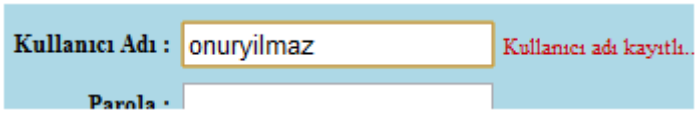
- Öncelikle gizli / kişisel bir bilgi olan kullanıcı adlarının saldırganlar ya da başka kişiler tarafından öğrenilebilmesi, güvenli yazılım geliştirme döngüsünde kabul edilemeyecek bir davranıştır.
- Kullanıcı hesap adlarının bir şekilde öğrenilebilmesi, uygulamanın kullandığı form tabanlı kimlik doğrulama mekanizmasına gelecek olan kaba kuvvet (deneme yanılma / brute force) saldırılarının başarı oranını da arttıracaktır.
- Sıraladığımız iki madde haricinde ayrıca kaba kuvvet saldırılarında kullanmak amacıyla wordlist hazırlamak için de uygulamanızın kimlik doğrulama mekanizması hedef alınmış olabilir.

Görüleceği üzere elde edilen kullanıcı hesap adları farklı amaçlar için kullanılabilmekte. Bu bilgileri elde etmek için ise tek hareket noktamız olacak; uygulamadan sızan hata mesajları ve son kullanıcıyı uyarmaya / yönlendirmeye yarayan bilgi mesajları.

Form tabanlı kimlik doğrulama mekanizmasının genel kullanımını göz önüne alarak ilk adımdan son adımına kadar çeşitli modüllerden nasıl bilgi toplanabilir noktasını farklı senaryolar ile göstermeye çalışacağız.

Birinci Senaryo – Yeni Üye Kaydı

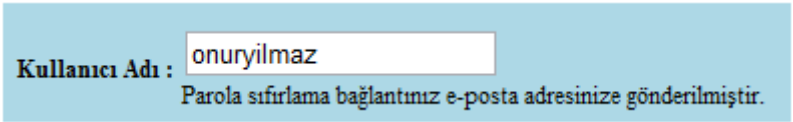
Uygulamada kayıtlı bulunan kullanıcıların birbirinden bağımsız olması ve aynı kullanıcı adının bir çok defa kullanılamamasından hareket ile çok basit bir şekilde uygulamada kayıtlı bulunan kullanıcı adlarının toplanabilmesi mümkündür.



Çözüm önerisi olarak söylenebilecek tek şey, eğer uygulamanızın yapısı müsait ise uygulamaya giriş esnasında "e-posta adresi, kullanıcı adı ve parola" üçlüsünü isteyebilir, e-posta adresini ise benzersiz yaparak kullanıcı adlarının öğrenilmesini zorlaştırabilirsiniz.

İkinci Senaryo - Parolamı Unuttum

Uygulamanızdaki kayıtlı kullanıcıların parolaları unutması durumunda kullanabilecekleri bir 'parolamı unuttum' modülünüz mevcut ise, başınız dertte olabilir !

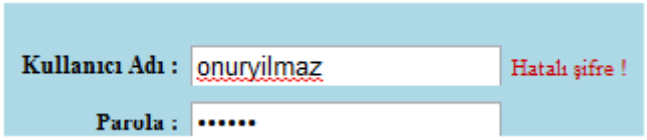


Parolamı unuttum modülü üzerinden uygulamanızda kayıtlı bulunan kullanıcı hesap adlarının öğrenilmemesi için daha genel bir bilgilendirme / hata mesajı kullanabilir (talebiniz işleme

alınmıştır) ya da gizli soru / cevap kontrolü başarı ile doğrulanırsa kullanıcı adı bilgisi istenerek gerekli işlemler yapabilirsiniz.

Üçüncü Senaryo - Kullanıcı Girişi

Uygulamada bulunan form tabanlı kimlik doğrulama mekanizmasının giriş ekranından dönen hata ve bilgilendirme mesajları sayesinde, uygulamadaki kayıtlı kullanıcı adlarının öğrenilebilmesi mümkündür.



Yukarıdaki resimde görüldüğü üzere kullanıcı adının doğru, parolanın yanlış olduğu durumlarda 'hatalı şifre' şeklinde bir mesaj dönmekte ve böylece saldırgan uygulamada böyle bir kullanıcının var olduğunu anlamaktadır.

En basit şekilde bu saldırıyı bertaraf etmek için ilgili durumda 'Hatalı kullanıcı adı / şifre' şeklinde daha genel bir mesaj verilebilir.

Sonuç

Uygulamanın kullanılışlığını arttırmak ya da kolaylaştırmak ve son kullanıcının her ihtimal sonucunda bilgilendirilmesini amaçlamak, bu durumda görüldüğü üzere uygulamanızda potansiyel güvenlik zafiyetlerinin oluşmasına neden olabilmektedir.

Uygulamanızın yapısı izin verdiği müddetçe tarafınızdan hazırlanan bilgilendirme mesajlarının daha 'genel' içeriğe sahip olmalıdır. 'Kullanıcı Hesap Adlarının Tespiti (User Enumaration)' [1] noktasında uygulamanızın yapısı önlemler almanızı engelliyorsa, elde edilen bilgilerin kullanılacağı ve bir sonraki adım olan 'Kaba Kuvvet Saldırılarına' [2] yönelik önlemler almanız gerekecektir.

Referanslar

[1] http://www.owasp.org/index.php/Testing_for_user_enumeration_(OWASP-AT-002)
[2] websec/31-burp-suite-ile-deneme--yanilma-denetimi.wgt