# WGT Capture the Flag

**Etik Saldır, iPad Kazan, CTF v5**

08.03.2011, Onur Yılmaz, contact-at-onuryilmaz-info

Daha önceleri Etik Saldır, Kitap Kazan başlığı altında gerçekleştirdiğimizi CTF serisinin 5. sini, Biznet Bilişim Sistemleri sponsorluğunda iPad ödüllü olarak gerçekleştirdik. Yarışma süresince desteklerini esirgemeyen Biznet ve OWASP/TR ekibine şahsım adına teşekkür ederim.

## Senaryo

Kısaca senaryomuzu özetlemeye çalışırsak; katılımcılar için hedef olarak verilen ctf.webguvenligi.org adresindeki bir dizi zafiyet barındıran web uygulamasındaki zafiyetleri tespit ederek, bu zafiyetleri kullanmak ve uygulamanın veritabanı bağlantısı için kullandığı veritabanı cümlesinin ele geçirilmesi gerekiyordu. Ne yazık ki katılımcılarımız 5. CTF yarışmamızda başarı gösteremediler.

## Çözüm

İlk aşamada http://ctf.webguvenligi.org/Login.aspx adresine erişim sağlandığında uygulamaya giriş ekranı ile karşılaşan katılımcıların, daha sonra ipuçlarında da belirttiğimiz üzere Şifremi Unuttum sayfasına yönelmeleri gerekiyordu.

Şifremi unuttum sayfasında kullanmak üzere iki adet veriyi ele geçirmek gerekiyordu;

- Sistemde kayıtlı bir kullanıcının adı ve e-mail adresi.

Bu veriye de;

- Sayfanın kaynak kodundan; <meta name="Programmer" content="admin - webguvenligictf[at]gmail[dot]com" />
- Ya da uygulamaya, uygulamanın beklemediği davranışlarla hata verdirerek, yönlendiğiniz hata sayfasından

ulaşmak mümkündü.

Bu verilere ulaştıktan sonra şifremi unuttum sayfasında, kullanıcı adı alanına ‘admin’ yazmanız neticesinde de bu kullanıcı adının doğruluğunu teyit etmiş olmaktaydınız.

Asıl mevzu ise şimdi başlıyor. Katılımcıların hareket noktası; ‘sistemde kayıtlı kullanıcı adını ve mail adresini biliyorum, şifresine nasıl erişebilirim’ olmalıydı.

- Şifresini tahmin ederek.
- Login ya da Şifremi Unuttum alanlarındaki veritabanı bağlantılarında bulunabilecek olası SQL Injection zafiyetlerini kullanarak
- Vs.

Biz burada, daha sonraları ipucunda da belirttiğimiz üzere, Şifremi Unuttum sayfasına SQL Injection zafiyeti yerleştirmiştik.

http://twitter.com/owasptr/status/43747971258527745 adresinde yayınladığımız ikinci ipucunda mevcut olan exploit kodları incelendiğinde, ilgili SQL Injection zafiyetinin nasıl exploit edilebileceğini az çok tahmin etmişsinizdir.

- İlk olarak kullanıcı adı alanındaki değişken doğru olmalıydı; ‘admin’
- Daha sonra ise kullanıcı adı ile eşleşen doğru e-mail adresi kullanılmalıydı; ‘webguvenligictf@gmail.com’
- Bu iki bilgiye zaten sistem üzerinden erişmek gayet kolaydı.
- Son olarak da yapılması gereken, hem kullanıcının kendisine hem de saldırgana aynı şifreyi göndermesini sağlaması amacıyla arka plandaki veritabanı sorgusunu doğru bir şekilde manipüle etmekti.

Yukarıdaki şekilde hareket ile aşağıdaki SQL sorgusunu e-mail alanına yazmanız, kullanıcının şifresini ele geçirmenize yeterli olacaktı.

**webguvenligictf@gmail.com') UNION ALL SELECT 1,2,3,',contact@onuryilmaz.info',4—**

## Sonuç

Sonuç olarak yarışmayı kazanan olmadığından ötürü, yakın zamanda yine Biznet sponsorluğunda düzenleyeceğimiz CTF v6 ile karşınızda olacağınız. O güne kadar görüşmek üzere ☺

**Not:** CTF’in ikinci aşamasını v6 da kullanacağımızdan ve ikinci aşamaya geçen olmadığından dolayı çözümünü yayınlamıyoruz.