* Attack can exploit it and execute arbitrary code on the server

* An application has an input ↓

<input type="text" search="input" maxsize="12">

in search form parameter = aaaaaa .....

you can try an an sign up page :

example :

email : long text @ gmail.com
password : long password

* types of Buffer overflow
  1. Stack overflow
  2. heap overflow
  3. integer overflow
  4. format string overflow

① Stack overflow :

* Overflow araised when a user use unbounded copy operation

example

I am taking an input from the user.

username :

password :

② heap overflow

login page < username
password

```
char * var = (char*) mallac(32);
strcpy(var, username)
```

③ integer Buffer overflow

you just have to supply large string of data into string parameter.
there is:

username:
password:

and there is len = strlen(username)

```
unsigned short = len + 1;
char * var = (char*) malloc(len);
strcpy(var, username)
```