Name- Aaryak Kaur
Rollno- 102211/01
Course- BSc IT 6TH
Date- 17/06/2021

subject- Infor & security (LAB)
End sem practical.

(1) The different types of vulnerability for hacking a website or web applications are:

(i) SQL Injection Attacks
(ii) Cross site scripting
(iii) Cross site Request forgery (CSRf)
(iv) Broken authentication & session Management
(v) Security Misconfiguration.

(1) SQL Injection Attacks

Injection is a ~~seq~~ security vulnerability that allows an attacker to alter backend SQL statements. by manipulating the user supplied data.

(2) Cross site scripting

It is also known as XSS.
XSS vulnerabilities target scripts embedded in a page that are executed on the client side. i.e. user browser rather than at the server side. These flaws can occur when the application takes untrusted data & send it to the web browser without proper validation.

(III) Cross site Request forgery (CSRF)

It is a forget request came from the crosssite.

CSRF attack is an attack that occurs when a malacious website, email, or program causes a user's browser to perform an unwanted action on a trusted site for which the user is currently authenticated.

(IV) Broken authentication & session Management:

The website usually create a session cookie & session ID for each valid session, & these cookies contain sensitive data like user name password, etc. When the session is ended either by logout or browser closed abruptly, these cookies should be invalidated i.e for each session there should be a new cookie.

(V) Security Misconfiguration:

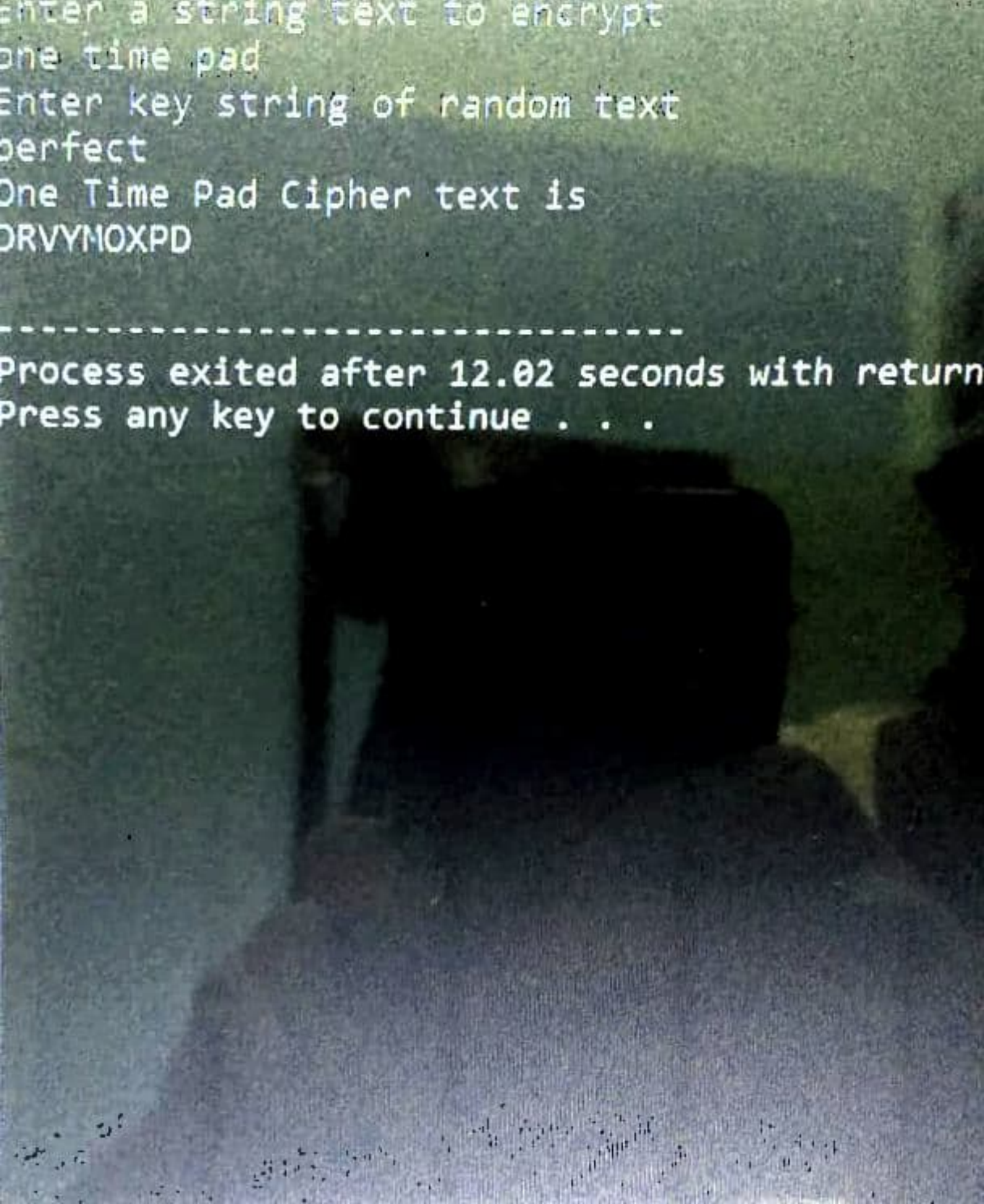
It must be defined & deployed for the application framework, application server, web server, database server, & platform. If these are properly configured an attacker can have unauthorized access to sensitive data or functionality.

Name - Aaryak Rana subject - Info & cyber security Lab
Rollno - 1022711/01 End sem practical
Course - BSc IT 6th sem
Date 17/06/2021

(2) WAcP to implement OTP.

```
#include <stdio.h>
#include <string.h>
#include <ctype.h>
int main()
{
int i,j, len1, len2, numstr[100], numkey[100], numcipher[100];
char str[100], key[100], cipher[100];
printf("Enter a string text to encrypt\n");
gets(str);
for(i=0 j=0; i<strlen(str); i++)
{
if(str[i]!='')
{
str[j] = toupper(str[i]);
j++;
}
}
str[j] ='\0';
for(i=0; i<strlen(str); i++)
{
numstr[i] = str[i] - 'A';
}
printf("Enter key string of random text\n");
gets(key);
for(i=0,j=0; i<strlen(key); i++)
{
if(key[i]!='')
{key[j] = toupper(key[i]);
```

```
j++;
}
}
key[j] = '\0';
for(i=0; i<strlen(key); i++)
{
  numkey[i] = key[i] - 'A';
}
 for(i=0; i<strlen(str); i++)
 {
  numcipher[i] = numstr[i] + numkey[i];
 }
for(i=0; i<strlen(str); i++)
{
  if(numcipher[i] >25)
  {
   numcipher[i] = numcipher[i] - 26;
  }
}
printf("One time Pad Cipher text is \n");
for(i=0; i<strlen(str); i++)
{
  printf("%c", (numcipher[i] + 'A'));
}printf("\n");
}
}
```


Enter a string text to encrypt
one time pad
Enter key string of random text
perfect
One Time Pad Cipher text is
DRVYMOXPD

Process exited after 12.02 seconds with return
Press any key to continue . . .

Name- Aaryak Rana
Rollno- 1022711/01
Course- BSc IT 6th sem
Date- 17/06/2021

Subject- Info. & cyber security (LAB)
End sem practical.

---

(4) Passwords are a set of strings provided by users at the authentication prompts of web accounts. Although password still remains as one of the most secure methods of authentication available to date, they are subjected to a number of security threats when mishandled. The role of password management come in handy there. Password management is a set of principles & best practices to be followed by users while storing & managing passwords in an efficient manner to secure passwords as much as they can be prevent unauthorized access.

There are many challenges in securing passwords in this digital era. when the no. of web services used by individuals are increasing years-over-years on one end, the no. of cybercrimes are also skyrocketing on the other end. Here are a few common threats to hack our passwords-

(i) Login spoofing

Passwords are illegally collected through a fake login page by cybercriminals

(ii) Sniffing attack

Passwords are stolen using illegal network access with tools like key loggers.

(iii) Brute force attack

stealing passwords with the help of automated tools & gaining access to user data.

(iv) Data Breach

stealing login credentials & other confidentiality data directly from the website database.