Name:- Akash Choudhary
Course:- BSc IT 6th Sem
Roll No:- 102717 (07)

A Kash

{Information security & cyber law endterm lab exam}

Ans :- (1)

SQL Injection

Injection is a security vulnerability that allows an attacker to alter backend SQL statement by manipulating the user supplied data. The SQL command which when executed by web application can also expose the backend data base.

Cross Site scripting

Cross site scripting is also shortly known as XSS. XSS vulnerabilites target scripts embeded in a page that are executed on the client side i.e. user browser rather then at the server side. These flaws can occur when the application take untrusted data and send it to the web browser without proper validation.

Broken Authentication and session Management.

The websites usually create a session cookies ~~sessi~~ and session ID for each valid session, and these cookies contain sensitive data Like username, password, etc. When the session is ended by either by logout or browser closed abruptly these cookies should be invalidated i.e. for each session there should be a new cookie.

Insecure Direct object References

It occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key as in url or as a form Parameter. The attacker can use this information to access other objects and can create a future attack to access the unauthorized data.

Cross Site Request Forgery

CSRF is a forged request come for the cross site.

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

Name :- Akash Choudhary
Course :- BSc IT 6th Sem
Roll No :- 1022717 (07)
Akash

{ Information Security & cyber law endterm lab exam

Ans (4) Password management :-

Password are a set of strings provided by users at the authentication prompts of web accounts. Although passwords still remain 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 comes in handy there. Password management is a set of principles and best practices to be followed by users while storing and managing passwords in an efficient manner to secure passwords as much as they can to prevent unauthorized access.

Few common threats to protecting our passwords

1) Login Spoofing :- Passwords are illegaly

collected through a fake login page by cyber criminals.

2) Sniffing attack:- Passwords are stolen using illegal network access and with tools like Key loggers.

3) Brute force attack:- Stealing passwords with the help of automated tools and gaining access to user data.

4) Data breach:- Stealing login credentials data directly from the website database.

Name :- Akash Choudhary
Course :- BSc IT 6th Sem
Roll No :- 1022717 (07)
(17/Jun/2021)

{ Info. security & cyber law end-term lab exam

Akash.

Ans :- (2) ONE time Password

```
#include<stdio.h>
#include<string.h>
#include<ctype.h>
main()
{ int i,j,len1,len2,numstr[100],numkey[100],
numcipher[100];
 char str[100],key[100],cipher[100];
 printf("Entera string text to encrypt\n");
 get(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");
  }
}.
```