

Name:- Akash Choudhary
Course:- BSc IT 6th Sem
Roll No:- 102277 (07)

{ Information security &
cyber law end term
lab exam

Ans :- ①

~~SQL~~ SQL Injection

Injection is a security vulnerability that allows an attacker to alter backend SQL statement by manipulating the user supplied data. ~~The~~ 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 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 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 ~~ses~~ 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 $00` as a form ~~Par~~ 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.

CSRF stands for Cross Site Request Forgery. It is a type of attack that tricks a user into performing an action on a website they did not intend to. This can be achieved by sending a request from a malicious website to a user's browser, which then sends the request to the target website without the user's knowledge. This can be done through various methods such as email, social media, or even through a compromised device. Once the user clicks on a link or interacts with a form on the malicious website, their browser sends a request to the target website, which then performs the desired action on behalf of the user. This can lead to sensitive information being stolen or modified, or even worse, financial loss.

Name :- Akash Choudhary

Course :- BSc IT 6th Sem

Roll No :- 1022717 (07)

Akash

} Information Security &
cyber law end term
lab exam

Q) Password management :-

Passwords 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 illegally

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 }

Aakash.

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 ("Enter a string text to encrypt\n");
    get(str);
    for (i = 0, j = 0; i < strlen(str); i++)
    {
        if (str[i] != ' ')
        {
            str[j] = topper (str[i]);
            j++;
        }
        str[j] = '\0';
    }
}
```

7

```

for (i=0; i<strlen(str); i++)
{
    numstr[i] = str[i] - 'A';
}
printf("Enter Key string of random text\n");
get(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 (numciphers[i] > 25)
{
    numciphers[i] = numciphers[i] - 26;
}
printf("One Time Pad Cipher text \n");
for (i = 0; i < strlen(str); i++)
{
    printf("%c", (numciphers[i] + 'A'));
}
printf("\n");
}
```

Enter 10 bits input: 1100011100

Your p10 key is :6,7,8,9,10,1,2,3,4,5,
Bits after p10 :1110011000
Output after LS-1 :1110011000

Your p8 key is :6,7,8,9,1,2,3,4,
Your key k1 is :11001110

Process exited after 24.95 seconds with return value 0
Press any key to continue . . .