

Rihik Rana

Ans 1 Different types of vulnerability for hacking a website are :-

(i) sql injection - sql injection is a type of a web application security vulnerability in which an attacker attempts to use application code to access or corrupt database content. It allows attacker to create, read, update, alter or delete data stored in the back-end database.

(ii) Cross site scripting.

Cross site scripting (XSS) targets an applications user by injecting code usually a client-side script such as Java script into a web application output. The concept of XSS is to manipulate client-side scripts of a web application to execute in a manner desired by the attacker. XSS allows attackers to execute scripts in the victim browser which can hijack user session.

Rihik Rana

(ii) Broken authentication & session management :-

Broken authentication & session management encompasses several security issues, all of them having to do with maintaining the identity of a user. If authentication credentials and session identifiers are not protected at all times, an attacker can hijack an active session and assume the identity of user.

(iii) Insecure direct object References - It is when a web application exposes a reference to an internal implementation object. Internal implementation object include files, database records, directories and database keys. When an application exposes a reference to one of these objects in a URL, hackers can manipulate <sup>it</sup> to gain access to a user's personal data.

(iv) Security Misconfiguration - A secure configuration must be defined and deployed for application, framework, application server, web server, database server and platform. Security <sup>mis</sup>configuration gives hacker access to private data or features and can result in a complete system compromise.

*Rinkana*

```
Ans2 #include <stdio.h>
#include <string.h>
#include <ctype.h>

main()
{
    int i, j, len2, numstr[100], numkey[100], numcipher[100];

    char str[100], key[100], cipher[100];

    printf("Enter a string text to encrypt");
    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 a string of random text\n");
    gets(key);

    for (i=0; j=0, i < strlen(key); i++)
    {
        if (key[i] != ' ')
        {
            numkey[j] = key[i] - 'A';
            j++;
        }
    }

    for (i=0; i < strlen(str); i++)
    {
        numcipher[i] = (numstr[i] + numkey[i]) % 26;
    }

    for (i=0; i < strlen(str); i++)
    {
        cipher[i] = numcipher[i] + 'A';
    }

    cipher[strlen(str)] = '\0';

    printf("Encrypted string is: %s", cipher);
}
```

*Rihik Parra*





```
key[j] = toupper(key[i]);
    }
}
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");
}
```





```
C:\Users\ACER\Desktop\info.exe
Enter a string text to encrypt
i am ritik
Enter key string of random text
ranaji
One Time Pad Cipher text is
ZAZRRB#|
-----
Process exited after 11.27 seconds with return value 0
Press any key to continue . . .
```

Resources  Compile Log  Debug  Find Results  Close

Ans 4 Password management - Passwords are set of string provided by user at the authentication prompts of web account. Although password still remains as one of the most secure method of authentication available to date, they are subjected to a number of security threats when mismanaged. Password management is a set of principles and best practices to be followed by user by the user while storing and managing password in a efficient manner to secure password as much as they can to prevent unauthorized access.

#### Password management using free online tools.

- ① LastPass - offers unlimited storage on multiple device. It offers password auditing 2FA compatibility password sharing & built in authentication.
- ② Aura Password Manager - It give unlimited storage on unlimited devices, plus intuitive interface. It include biometric login built in 2FA authenticator and well functioning auto-saving and autofilling capability.

*Signature*

- ③ RoboForm - It is a user friendly and excellent form filler and unlimited password storage on one device. Check the vault for weak password receive emergency access organise bookmark. & send login to other user.
- ④ Bitwarden - It uses AES-256 encryption to protect the data stored in your password vault. Your information is only unencrypted & only locally on your device and you've logged into your vault with master key.
- ⑤ Sticky password - It provides USB portability and biometric login but we have to upgrade for multi-device sync.

*RIHK Rana*