THADOMAL SHAHANI TSEC ENGINEERING COLLEGE

ASSIGNMENT NO. 3

Q. List all the software vulnerabilities. How are they exploited to lauch an attack?

→ Software vulnerabilities are weakness or blows in software systems that can be exploited by attackers to compromise security, integrity or availability of system or data. These vulnerabilites can range from programming errors and design blows to the improper configurations and weak authentication mechanisms. Exploiting those vulnerabilities can lead to various cyber threats, including unauthorized access, data breaches, system crashes and execution of malicious code.

Following aresome of the vulnerabilities :-

1) Buffer Overflow :-

Occurs when an attacker modifies or writes more data to the buffer which leads to change in execution of program, system crashes and the execution of the malicious code.

2) SQL Injection :-

Exploit vulnerabilities in web applications that interact with databases, allowing attackers to manipulate SQL queries to gain unauthorized access.

3) Cryptographic Failures :-

Improper implementation of encryption hashing or key management mechanisms.

4) Cross-side Scripting (XSS) :-

Allows attackers to inject malicious scripts into web pages viewed by other users, comprising their security or stealing information.

5) Clickjacking :-

Tricks users into clicking as malicious links or buttons by disguising them as legitimate elements on webpage.

6) Denial of Service (DOS) :-

Overwhelms a system or network with excessive traffic, rending it unavailable to legitimate users.

7) Insecure Transport Layer (ILS) :-

Utilizes weak encryption protocols, letting attackers manipulate encrypted communications.

Clickjacking :-

It is an attack that tricks a user into clicking a webpage element which is not visible or disguised as another element.

It can cause users to unwillingly download the malware and visit malicious web pages, providing sensitive information to the stranger. Several variations such as - like jacking and cursorjacking.

For example :- The user visits the page and clicks the "Book my Free Trip" button.

Another example :- In reality, the user is clicking on the invisible iframe and has clicked the "Confirm Transfer" button. Funds are transferred then to the attacker.

Prevention Methods :-

1) Use "X-Frome-Options" HTTP response header.
2) Add a Frame killer to website
3) Empty a security policy to specify which domains are assured and allowed to frame your pages.
4) Keep your system patched.
5) Empty defensive code in user interface.

Phishing Attack :- It inoves tricking users into revealing sensitive information such as login credentials or financial details by reflecting as a legitimate entity via email, etc.

Prevention :-

i) Security Awareness :- Educate users about the risks of phishing attacks and how to recognize them.

ii) Two-factor Authentication :- Implement (2FA) to add an extra layer of security beyond passwords reducing risks of compromised credentials.

iii) URL Inspection :- Carry all inspecting URLs to avoid clicking on suspicious links.

iv) Email Filtering :- Use spam and email authentication mechanisms to detect and block the phishing emails.