Assignment No : 3

Q.1 List software vulnerabilities. How they are exploited to launch an attack?

⇒
- Software vulnerabilities :
1) Buffer overflow
2) SQL injection
3) Cross-site scripting (XSS)
4) Code injection
5) Zero-day vulnerability
6) Privilege escalation
7) Denial of service (DoS)
8) Man-in-the-Middle

- Today it is hard to imagine any software without any vulnerabilities. Some vulnerabilities are found during software testing and others are found in the field.
- Software vulnerabilities that are found after the software has been released are mitigated by giving out software patches or updates.
- You would have seen your browser, operating system and apps updating multiple times in its course of lifetime.
- These updates include both feature updates and also security updates.

THADOMAL SHAHANI TSEC ENGINEERING COLLEGE

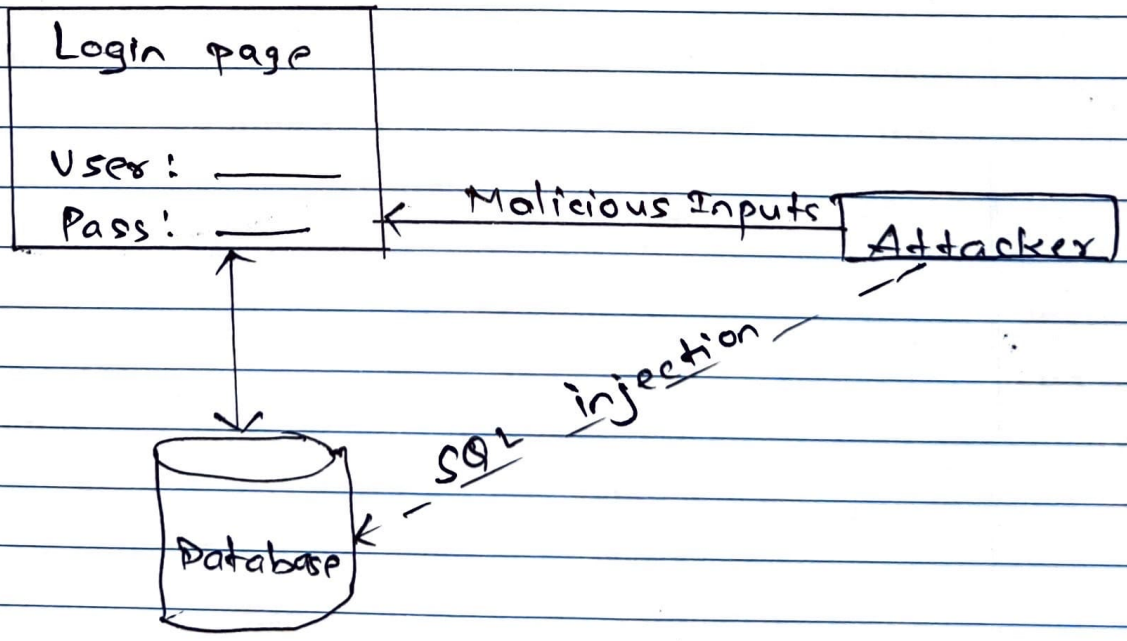
- Software developing companies have security vulnerabilities updated programs and teams that regularly investigate all reported security vulnerabilities from the field.
- As you learnt these companies also run bug bounty programs that help them find security vulnerabilities in their products and mitigate them before these vulnerabilities could be mass exploited.
- Let's see an example, depending on the type of vulnerability, it can be exploited either manually or using scripts or tools.
- Attackers has deep understanding of how the vulnerability works and what carries out the required steps in the right sequence to exploit vulnerability.

Q.2 What is SQL injection?

⇒ - SQL Injection (SQLi) is a vulnerability exploiting which an attacker can inject malicious SQL commands and cause the database server to execute them.
- Using SQLi the attacker can
1) Read sensitive and unauthorized data from the database,
2) Modify data
3) Execute admin commands on the database
4) And can also Issue commands to the operating system running the database

- Note that here the presence of SQLi attack does not mean that the SQL databases are inherently vulnerable or exploitable directly.
- This exploit only works if the application developer has programmed the application in such a way that the attack is possible.
- SQL databases just behaves as they should. So, even if the attack is called SQLi the fix for this exploit is not in the SQL databases.
- SQL is proven to be one of the most dangerous and impactful exploits on database based applications.

163



- There could be several non-malicious programming errors such as buffer overflow, SQL injection, cross-site scripting etc. that can be exploited by attacker.
- SQLi can potentially be exploited where the user input is directly used to form SQL database queries.