CSS_Practical Exam_TECOMPA_26_YASH GUPTA

Aim:- Simulation of SQL Injection Attack.

Theory:-
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server. Since an SQL injection vulnerability could possibly affect any website or web application that makes use of an SQL-based database, the vulnerability is one of the oldest, most prevalent and most dangerous of web application vulnerabilities.

⇒ Examples:-
i) Retrieving hidden data, where we can modify an SQL query to return additional results.
ii) Subverting application logic, where we can change a query to interfere with the application's logic.
iii) Union attacks, where we can extract information about the version from different database tables.
iv) Blind SQL injection, where the results of a query you control are not returned in the application responses.

Results and discussion:-
A successfully SQL injection attack can result in unauthorized access to sensitive data, such as passwords, credit card details or personal user information.

* Viva Questions:-

i) Any applications that as an attack of SQL injection.

→ a) GhostShell attack - hackers from APT group Team GhostShell targeted 53 universities using SQL injection, stole and published 36,000 personal records belonging students, faculty and staff.

b) Turkish government - hackers breached the Turkish government website and erase debt to government agencies.

c) Tesla vulnerability - in 2014, security researchers publicized that they were able to breach the website of Tesla using SQL injection gain ~~as~~ administrative privileges and steal user data.

ii) How to prevent SQL injection?

→ a) Submitting the single quote character ' and looking for errors or other anomalies.

b) Submitting Boolean conditions such as OR 1=1 and OR 1=2, and looking for differencies in the time taken to respond.

iii) what is firewall attack?

→ A firewall is a network security device that monitors incoming and out going network traffic and decides whether to allow or block specify traffic based on a defined set of security rules.