

Name:- Mayank Chauhan

Course:- BSC(IT) 6th sem.

Roll no:- 1022743

Subject:- Information security.


Date:- 17/06/21

Q-1:-

①:- SQL INJECTIONS:- SQL injection is a type of web application security vulnerability in which an attacker attempts to use application code to access or corrupt database content. If successful, this allows the attacker ~~the~~ to create, read, update, alter, or delete data stored in the back-end database.

②:- CROSS site scripting:- ~~to~~ targets an application's users by injecting code usually a client-side script such as JavaScript, into a web application, output.

③:- Broken authentication:- Broken authentication and session management encompass several security issues all of them having to do

with maintaining the identity of a user. 

④!- Insecure × direct × object × reference!-

Insecure direct object reference is when a web application exposes a reference to an internal implementation object. include fields database records, directories, ~~and~~ and database keys.

⑤!- Security × misconfiguration!-

security misconfiguration encompasses several types of vulnerabilities all centered on a lack of maintenance or a lack of attention to the web application configuration.

⑥!- Cross × site × request × forgery!-

is a malicious attack where a user is tricked into performing an action he or she didn't intend to do. A third-party website will send a request to a web application that user is already authenticated against.