

Ans 1 Different types of vulnerability for hacking a website or web application - .

- 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 to create, read, update, alter, or delete data stored in the back-end database. SQL injection is one of the most prevalent types of web application security vulnerabilities.
- 2) Cross Site Scripting (XSS) - Cross-site scripting (XSS) targets an application's user by injecting code, usually a client-side script such as Java Script, into a web application's output. The concept of XSS is to manipulate client-side scripts of a web application to execute in the manner desired by the attacker.
- 3) Broken Authentication and Session Management - Broken authentication and 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.

Day 2 Apr

- 4) Insecure Direct Object References - Insecure direct object reference is when a web application exposes a reference to an internal implementation object. Internal implementation objects include files, database records, dictionaries and database keys. When an application exposes a reference to one of these objects in a URL, hackers can manipulate it to gain access to a user's personal data.
- 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. A secure configuration must be defined and deployed for the application, frameworks, application server, web server, database server and platform.
- 6) Cross-site request forgery (CSRF) - Cross-site Request Forgery (CSRF) is a malicious attack where a user is tricked into performing an action he/she didn't intend to do. A third-party website will send a request to a web application that a user is already authenticated against (by their bank).