Most common website security vulnerabilities

1) SQL Injections - 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.

2) Cross site scripting - (XSS) - targets an application's users by injecting code, usually a client-side script such as Java Script, into a web application's output

3) Broken authentication & session management - encompass several security issues, all of them having to do with maintaining the identity of a user.

Sunil

PAGE

DATE

"Rough & Fair"

4) Insecure direct object references - is when a web application exposes a reference to an internal implementation object. Include files, database records, directories and database keys.

5) 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. Targets include web application like social media, in browser email clients online banking, and web interfaces for network devices.