Semester : VI Subject : CSS Academic Year: 2023- 2024

DATABASE SECURITY ~~ATTACKS~~ REQUIREMENTS:

There are 10 dalābase securilȳ best practices that can assist you in enhancing the securilȳ of your sensitive dalā

(1) Put physical dalābase securilȳ in place:-

Physical attacks by outsiders or even threals from within might affect servers or dalā carlers.

Since these attacks can evade digilāl securilȳ syslems, it is challenging lō identify them without aadditional protection measures.

Make sure the provider you choose for web hosting has a reputation for treating securilȳ issues seriously.

(2) Tuoo distinct dalābase servers:

Keep your dalābase servers apard from other syslems lō reduce these securilȳ threals. Use realtime securilȳ information and Event monilōring (SEPM), which is dedicated lō dalābase securilȳ and enables enterprises lō respond quickly in the case of breach attempt.

(3) Configure a proxy server using HTTPS:

Set up an HTTPS server, however if you are working with sensitive dalā like passwoords, financial information or personal dalā. In this ~~matter~~, manner, you gain an additional degree of securilȳ because the dalā passing via the proxy server is likewise encrypted.

(4) Prevent utilizing standard network ports:-

It is a good practise of using new ports because

Semester : VI Subject : CSS Academic Year: 2023-2024

attackers always try to attack the default ports. To make sure the new port isn't already in use for other services, check the Internet Assigned Number Authority's port registers before issuing a new port.

(5) Employ real-time database surveillance:

The security is strengthened when database is actively examined for attempted breaches.

All actions performed on the database server can be tracked using monitoring software such as Tripwire's real-time File Integrity Monitoring (FIM) which can also notify you of any breaches.

(6) Employ firewalls for databases and web applications:

Install firewall to safeguard the database from many attack vectors. Configure the firewall properly to close any security gaps.

(7) Implement data encryption methods:

Encryption secures your data from the attackers.

(8) Frequently backup your database.

Frequently make backups of your database. This reduces the chance that private data will be comprised or lost because of malicious activity. Make sure the backup data is encrypted and kept on different server to further boost security.

(9) Maintain application updates :

All the applications has to be updated every now and then.

(10) Make use of reliable user authentication :

Most current analysis from Verizon indicates that passwords are stolen in 80% of data breaches. To avoid this set up a multi-factor authentication procedure to address this problem and increase database security. Restrict database access to only verified IP address.