Database security issues

Databases are very attractive targets for hackers because they contain valuable and sensitive information. This can range from financial or intellectual property to corporate data and personal user data. Cyber criminals can profit by breaching the servers of companies and damaging the databases in the process. Thus, database security testing is a must.

There are numerous incidents where hackers have targeted companies dealing with personal customer details. Equifax, Facebook, Yahoo, Apple, Gmail, Slack, and eBay data breaches were in the news in the past few years, just to name a few. Such rampant activities raised the need for cyber security software and web app testing which aims to protect the data that people share with online businesses. If these measures are applied, the hackers will be denied all access to the records and documents available on the online databases. Also, complying with GDPR will help a lot on the way to strengthening user data protection.

Database security issued that are commonly found in the database-driven systems :-

1. No security testing before deployment

One of the most common causes of database weaknesses is negligence on the deployment stage of the development process. Although a functional testing is conducted to ensure supreme performance, this type of tests can’t show you if the database is doing something that it is not supposed to. Thus, it is important that you test website security with different types of tests before complete deployment.

2. Poor encryption and data breach come together

You might consider the database a backend part of your set-up and focus more on the elimination of Internet-borne threats. It does not really work that way. There are network interfaces within the databases which can be easily tracked by hackers if your software security is poor. In order to avoid such situations, it is important to use TLS or SSL encrypted communication platforms. Thus, it is imperative that the companies hire professional dedicated teams for database development. There are various remote DBA services that can help you deal with your ventures.

3. Feeble cyber security software = broken database

Case in point, the Equifax data breach. Company representatives admitted that 147 million consumers’ data was compromised, so the consequences are huge. This case has proven how important cyber security software is to defend one’s database. Unfortunately, either due to lack of resources or time, most of the businesses don’t bother to conduct user data security testing and do not provide regular patches for their systems, thus, leaving them susceptible to data leaks.

4. Stolen Database Backups

There are two kinds of threats to your databases: external and internal. There are cases when companies struggle with internal threats even more than with external. Business owners can never be 100% sure of their employees' loyalty, no matter what computer security software they use and how responsible they seem to be. Anybody, who has access to sensitive data can steal it and sell to the third-party organizations for profit. However, there is a way to eliminate the risk: encrypt database archives, implement strict security standards, apply fines in case of violations, use cyber security software, and continuously increase your teams' awareness by corporate meetings and personal consulting.

5. Flaws in features as database security issue

Databases can be hacked through the flaws of their features. Hackers can break into legitimate credentials and compel the system to run any arbitrary codes. Although it sounds complex, the access is actually gained through the basic flaws inherent to the features. The database can be protected from third-party access by security testing. Also, the simpler its functional structure — the more chances to ensure good protection of each database feature.

6. Weak and complex DB infrastructure

Hackers do not generally take control over the entire database in one go. They opt for playing a Hopscotch game where they find a particular weakness within the infrastructure and use it to their advantage. They launch a string of attacks until they finally reach the back-end. Security software is not capable of fully protecting your system from such manipulations. Even if you pay attention to the specific feature flaws, it's important not to leave the overall database infrastructure too complex. When it's complex, there are chances you will forget or neglect to check and fix its weaknesses. Thus, it is important that every department maintains the same amount of control and segregates systems to decentralize focus and reduce possible risks.

7. Limitless administration access = poor data protection

Smart division of duties between the administrator and the user ensures limited access only to experienced teams. This way users that are not involved into the database administration process will experience more difficulties if they try to steal any data. If you can limit the number of user accounts, it's even better because hackers will face more problems in gaining control over the database as well. This case can be applied to any type of business but usually it happens in financial industry. Thus, it's good not only to care about who has the access to the sensitive data but also to perform banking software testing before releasing it.

8. Test website security to avoid SQL injections

This is a major roadblock on the way to the database protection. Injections attack the applications and database administrators are forced to clean up the mess of malicious codes and variables that are inserted into the strings. Web application security testing and firewall

implementation are the best options to protect the web-facing databases. However this is a big problem for online business, it's not one of the major mobile security challenges, which is a great advantage for the owners who only have a mobile version of their application.

9. Inadequate key management

It's good if you encrypt sensitive data but it's also important that you pay attention to who exactly has access to the keys. Since the keys are often stored on somebody's hard drive, it is obviously an easy target for whoever wants to steal them. If you leave such important software security tools unguarded, be aware that this makes your system vulnerable to attacks.

10. Irregularities in Databases

It is the inconsistencies that lead to vulnerabilities. Test website security and assure data protection on the regular basis. In case any discrepancies found, they have to be fixed ASAP. Your developers should be aware of any threat that might affect the database. Though this is not an easy work but through proper tracking, the information can be kept secret.

In spite of being aware of the need for security testing, numerous businesses still fail to implement it. Fatal mistakes usually appear during the development stages but also during the app integration or while patching and updating the database. Cyber criminals take advantage of these failures to make profit and as a result, your business is under the big risk of being busted. We are here to help eliminate these risks and prevent data breaches from happening. QArea software development outsourcing company is keen on security testing and offers a bunch of other IT services. Contact us if you want to protect your business.