IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

Database Security and Encryption

Suraj Tanwar
B.Tech Student, Department of Computer Science & Engineering
Dronacharya College of Engineering, Gurugram, India

Abstract: *Security in today's world is one of the most important challenges people are facing around the world in every aspect their lives. Similarly security in the electronic world has a great deal importance. In this paper, we check the security of the website. This is an area of great interest to a website for us note that, database usage becomes very important to modernbusiness and information details contain such information large business assets. This study is for diagnostic purposes issues and threats to website security, requirements for database security, and how encryption is used differently rates to provide collateral.*

Keywords: Security, Database

I. INTRODUCTION

Information or data is an important asset in any organization. Almost every organization regardless of social, governmental, education etc., now they have made their own details systems and other operational functions. They have it maintain a database containing important information. Web site security is therefore a major problem. Moving forward, we will he first discuss what database security really is? Protect confidential / sensitive data stored in storage actually website security. Works with database creation you are protected from any kind of illegal access or threat at any level.
Website security requirements that enable or disable the user actions on the website and its contents. Organizations effective operations require the privacy of their database. They do not allow unauthorized access to it their data / information. And they want assurance that their data is protected from any malicious or malicious conversion.

Database security is: privacy, integrity and availability.
As mentioned earlier, confidentiality limits time to retrieve secure data and as a result of that unauthorized avoidance data access. Integrity means data will not be available polluted in any way. Timely data availability is a factor for secure information.
There are four types of controls mentioned by Denning get database protection, including: access control, information flow control, cryptographic flow control and thinking control.

II. SECURITY RISK TO DATABASES

The organization of the launched website is less than amazing various threats. Other serious threats are considered in this regard document. This list is taken from a white paper presented by Imperva Application Protection Center

2.1 Legitimate Privilege Abuse

Violation of a legal right can be a form of abuse by website users, administrators or system administrator do anything illegal or unethical work. That's right, but it doesn't end there, anywhere misuse of sensitive data or unforgivable use of rights.

2.2 Excessive Privilege Abuse

When users are specified access permits performing other tasks that are not included in their work, which are dangerous the purpose can be achieved through such activities thus earning abuse of such rights. When we talk about such harassment, a university example can be cited when the administrator who is granted access to all databases and is entitled to this change the records of any student. This can lead to abuse such as grade change, student marks or conversion of the amount of the fine charged to any student. As a result, all users those who perform different tasks are given this standard rights grant excessive access

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

2.3 Higher Rights

Excessive exposure leads to the detection of defective errors profit by invaders and may cause change rights e.g. normal user given administrative access rights. Losses that may result in fraudulent accounts, money transfers, misinterpretations of other sensitive material analytical information. Such cases are also found to exist database functions, agreements and SQL statements.

2.4 Endangerment of the Website

Vulnerability to previous applications such as Widows 98, Windows 2000, etc. can cause data loss from website, data corruption or service denial conditions. Because for example, blaster worm has created a denial of service conditions from the vulnerability found in Windows 2000.

2.5 SQL Injection

Random SQL queries used by server maliciously the invader. In this attack the SQL statement is followed by a series identifier as input. That is verified by the server. If it happens can be confirmed it may be killed. With these unrestricted rights may be acquired by the aggressors as a whole database.

III. DATABASE SECURITY CONSIDERATION

3.1 Website Security Consideration

In order to eliminate security threats all organizations must explain the security policy. And that security policy should be the same strict enforcement. Strict security policy must be well contained defined safety features. Figure 2 shows the critical areas what needs to be considered is outlined below. [1] [3] [4]

3.2 Access Control

Access control ensures all connections to the site and other system components comply with policies as well controls defined. This ensures that no disturbances occur by any intruder outside or inside and thus, protects the database from potential errors - potential errors make a big impact like stopping factory operations. Access control also helps to reduce potential risks contributes to website security on large servers. Because for example, if any table was deleted by mistake or access fixed results can be supported or in specific files, access control can limit their removal.

3.3 Idea Policy

Idea policy is needed to protect data in a particular area level. It is possible when descriptions from specific data are in the type of analysis or facts that need to be protected from a certain high level of security. It also determines the method of protection information that can be disclosed.

3.4 User ID / Verification

User identification and verification is a basic requirement for ensure safety as the identification method defines a set of people are not allowed access to the data and it provides complete accessibility method. Ensuring security, ownership verified and keeps sensitive data safe and secure edited by any normal user.

3.5 Accountability and Auditing

Accountability and auditing are required to verify physical integrity of data that requires defined access data stored and controlled by research and recording to keep. It also helps to analyze the information stored on it verification servers, accounting and user access.

3.6 Encryption

Encryption is the process of concealing or converting information using cipher or code to be unreadable to all other people except those who hold the key information. The result of coded information is called as encrypted information. Data is an important asset of an organization. So its safety it is always a big challenge for the organization. In recent times the security of shared information was researched cryptographic view. A new framework was proposed in different keys used

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

by different groups for encryption data stored in a variety of ways labeled as hybrid cryptography database (MCDB). [6] The various forms of government, non- governmental, and private as well many other organizations have sensitive data on web servers which really need protection from the invader or the invaders. To make the site secure with different security strategies improved. One of them is the encryption method. However encryption enhances protection but your implementation decisions are also very important. Like you, how, when and where it should be nailed. . The following figure 4 shows where it is crucifixion occurs. Developing encryption techniques comes from something important questions and, such as how, when and where the encryption will be performed.

IV. CONCLUSION

Data to any organization is the most important area. Security Sensitive data remains a major challenge for the organization at any level. In today's world of technology, the database at risk of mob violence. In this study great security The relevant information sites are identified along with other encryption discusses ways to help reduce the risk of seizures and protect sensitive data. It has concluded with encryption provides privacy but does not guarantee that integrity unless we use a specific digital signature or Hash function. Using strong encryption algorithms reduces it performance. Future work can be done encryption is more efficient and effective.

REFERENCES

[1]. C. J. Date, A. Kannan and S. Swamynathan, An Introduction to Database Systems, Pearson Education, Eighth Edition, 2009.
[2]. T.Connolly, C. Begg. “Database Systems A Practical Approach to Design, Implementation, and Management”, 4th ed., Ed. England: Person Education Limited, 2005, pp. 542-547, 550-551.
[3]. Burtescu, E. (2009). Database Security-Attacks and Control Methods. Journal of Applied Quantitative Methods, 4(4), 449-454.
[4]. Kayarkar, H. (2012). Classification of Various Security Techniques in Databases and their Comparative Analysis. arXiv preprint arXiv:1206.4124.
[5]. Kahate, A. (2013). Cryptography and network security. Tata McGraw-Hill Education.
[6]. Stallings, W., & Brown, L. (2008). Computer security. Principles and Practice.