iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** IX **Month of publication:** September 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Database Security

Neha Gupta[1], Jyoti Chandel[2], Jyoti Yadav[3]
Dronacharya College of Engineering
Gurgaon

Abstract: ***Database security concerns the increase in the number of reported incidents as per evidenced by growing in terms of loss or unauthorized exposure to the sensitive data . The amount of data is collected, retained and shared by such electronically expands, such that database security is necessary to understand .The US Department of Defense (2004) i.e, The Defense Information Systems Agency in its Database Security Technical Implementation Guide, it basically states that security of database should provide controlling, protecting and access to the basic contents of a database, as well as it also preserve the integrity of data, consistency of data, and overall quality of the data. Students are in the computing disciplines they develop an understanding of the discussed issues and challenges as per related to database security and also they must be able to identify possible more solutions.***

As the knowledge base related to database security continues to grow, so do the challenges of effectively conveying the material. This paper addresses those challenges by incorporating a set of interactive software modules into each sub-topic. These modules are part of an animated database courseware project designed to support the teaching of database concepts. The courseware covers the domains of Database Design, Structured Query Language, Database Transactions, and Database Security. The Security Module, presented in this paper, allows students to explore such areas as access control, SQL injections, database inference, database auditing, and security matrices.

Keywords: Database security, Database vulnerability, Access control.

I. INTRODUCTION

Database technologies are the main component of many computing systems. These technologies are allowed the data to be retained and shared electronically and thus the amount of the data which contained in these systems are continuous to grow at a certain rate. So that there is a need to insure that the integrity of the data is secured from the unlimited access. According to the Privacy Rights Clearing House (2010) reports that there are more than 345 million customer records have been lost somehow they are stolen since 2005 when the tracking data had been began breach incidents, and the Ponemon Institute reports that the average cost of a data breach has risen up to $202 per customer record (Ponemon, 2009). In August 2009, In United States criminal indictments were handed down to three perpetrators accused of carrying out the single largest data security breach recorded to date. .Over 130 million credit and debit card numbers these hackers were stoled and by exploiting a well known database vulnerability, a SQL injection (Phifer, 2010). Since 2004, the Verizon Business Risk Team, who have been reporting data breach statistics , during the year 2008 they examined that there are 90 breaches. They reported that there are more than 285 million record had been compromised, a number exceeding the combined total from all prior years of study. They found that how they provide insight data into and who commits these acts and how these acts are occured. Consistently, they have found that almost 75% incidents that the data breaches originate from due to external sources and they are coming from the organization as they are compared to 20% coming from inside sources. Also they found that about 91% of the compromised records were greatly linked to the organized criminal groups. Further, they also cite that hacking is the result of the majority of breaches and by errors malware are also often facilitated committed by the victim, i.e., we say that the database owner. The two most common form s of hacking are found and they are Unauthorized access and SQL injection ,and between these two the interesting finding given between these two that these exploits are well known and often they are preventable also. Now the increasing numbers of breaches are given and there is also a great need to increase awareness of how we can properly protect and monitor our database systems. Database security is now included as a topic in an inductor database course or introductory computer security course. However database security is related to as per the knowledge based systems related as they continues to grow, so they can do all do all the

challenges of effectively conveying the material. Further, there are certain topics that these are related to database security these are complex and also students are required to engage in active learning.

II. DATABASE SECURITY TOPICS

ACCESS CONTROL

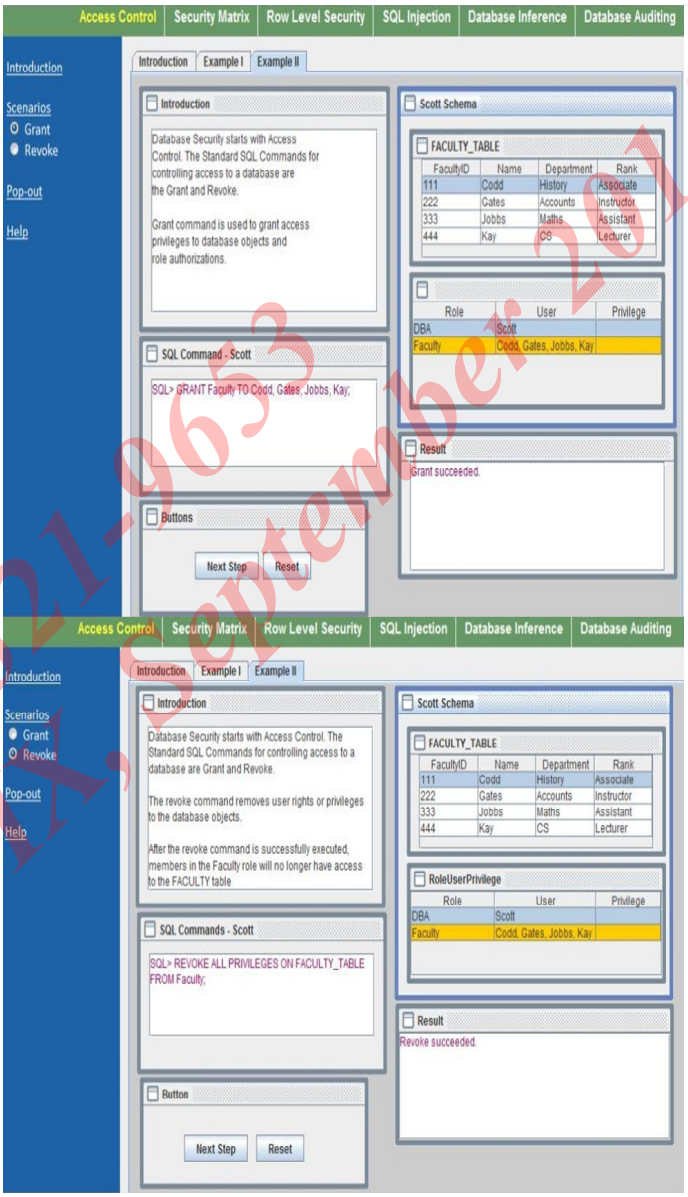
The method which is used to primary protect the data is limiting access to the data. Now this method can be done through many ways such that access control ,authorization and authentication. Now for instance, mostly database systems are used in some form of authentication, such as password and username, to the access to the system. Further mostly users are assigned or authorized to defined privileges to their specific resources. In a database , the objects which is included in a database usually include tables ,rows,columns and views.

Now at this Level of access control, students now have to proved their ability to offerings browser course but these are not to persue their grades which they assigned to their classmates.

III. ACCESS CONTROL -GRANT/REVOKE

In database security , there are certain objects which are pertained to some data objects such as tables and columns and also SQL objects which included views and these procedures are stored. Now they perform some data actions which include read (select), insert, update , delete and execute these are used for such stored procedures. For instance Dr. Smith , a faculty member, may be given and read certain privileges to the Student table. Now what is Access Control – Aces Control is basically a concept which is related to security. Specific users are accessed to obtained objects due to Access control limits actions. Perhaps access control is defend in generally three ways : Mandatory Access Control (MAC) , Discretionary Access Control (DAC) , and Role Based Access Control (RBAC). Specified users or groups are assigned to various privileges and these are provided by MAC and DAC. MAC rules are totally based on system applied and these are considered into static and these are more secure.

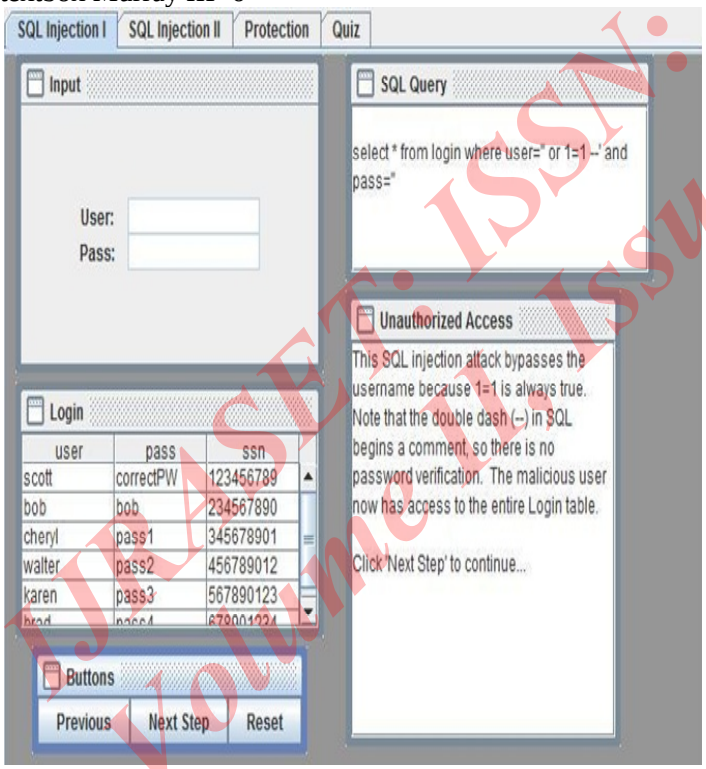
Another example for DAC rules are user supplied , and it would be considered so confused and dynamic.



IV. DATABASE VULNERABILITY

The phenomenon Security breaches is an increasing phenomenon Security.Now a days databases are more vulnerable and made accessible through Internet and it is totally web based applications, security threats will rise to their exposure. According to these threats the objective is to reduce susceptibility. The most important database application vulnerability is to be SQL injection. For discussing Security SQL injections are now provided great examples as they are

one of the most important database security issues, as risks are hereby inherited to non validated user input. Using user Input when SQL statements are created then SQL injections can happen.When users enter wrong code then the threat will occurred, that is "tricks" the database into executing wrong commands. It happens primarily because only due to the features of the SQL language it certainly allows things which usng double hyphens (--), semicolons are separated by SQL concatenating statements, and from the database data dictionaries have the ability to query metadata . For an SQL injection the solution for stopping an SQL is input validation .An example occurs on a webpage what might occurs when a login process is employed and that validates a password and a username against the data which retained in a relational database Now for user entry of text data the web page provides input forms. To search the database for matching records the user-supplied text is used to create a SQL statement. From this the valid username and password will be authenticated and this is the valid intension for that and for the system the user permitted access.Now these invalid passwords and username will not be authenticated.. For instance, the following string, ' OR 1=1 -- entered into the username textbox Murray IIP-6



V. CONCLUSION

There is a great need to secure our computer and systems and is well understood also and data must be secured securing data will be a part for an overall computer system plan . Through internet the amount of growing amounts of data are being retained and are being made for most of the databases are retained via the internet. It must be assumed that vulnerabilities and threats to the integrity of that data will be increase as well as more the data is electronically available. The most important topic for students is Database Security it becomes an increasingly important topic, students need to develop their understanding in this field. The main objective for database security are to prevent unauthorized tampering of data, prevent unauthorized access to data and modification of data and also to insure when needed data remains available. The multifaceted concepts are related to database security. Thus it can make challenges how to teach the material when database security is one of the main component of a larger course. However this is just how when mostly students are exposed to the topic database security.This paper suggested a set of sub-topics in a database security course component and introduced a set of interactive software modules mapped to each sub-topic presented. Engaging students in interactive learning activities enhances the learning experience and provides the opportunity for students .

REFERENCES

[1] Bertino, E., Byun, J., & Kamra, A. (2007). Database security. In M. Petkovic & W. Jonker (Eds.), security, privacy, and trust in modern data management (Data-centric systems and applications) (pp. 87-102). New York: Springer-Verlag.

[2] Bertino, E., & Sandhu, R. (2005). Database security—concepts, approaches, and challenges. IEEE Transactions on Dependable and Secure Computing, 2(1), 2-18.

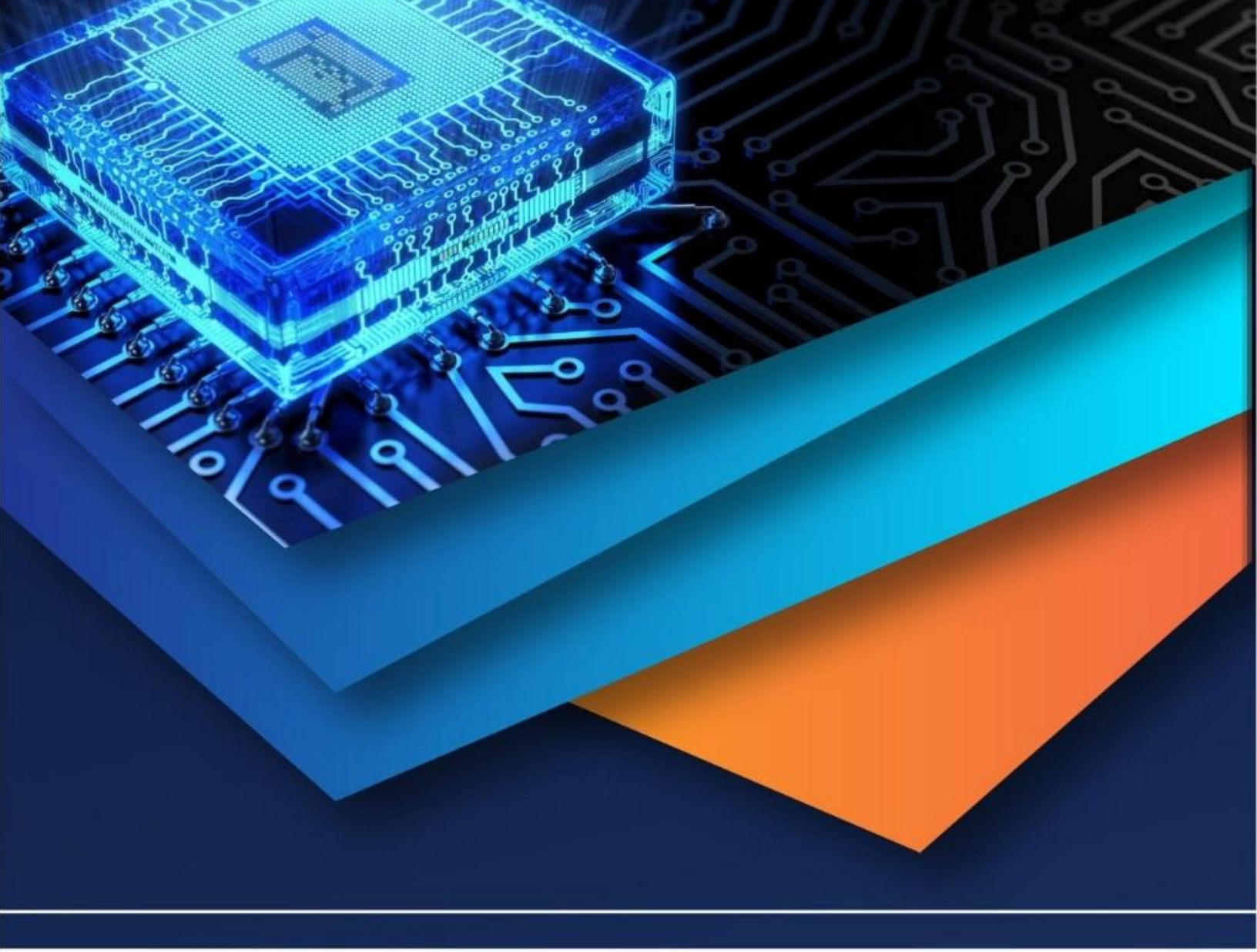
[3] Defense Information Systems Agency. (2004). Database security technical implementation guide, 7(1). Department of Defense. Retrieved January 31, 2010,fromhttp://www.databasesecurity.com/dbsec/database-stig-v7r1.pdf

[4] Guimaraes, M. (2006). New challenges in teaching database security. Proceedings of the 3rd Annual Conference on Information Security Curriculum Development, Kennesaw, GA, USA, 64-67.

[5] Jaquith, A. (2007). Security metrics: Replacing fear,

uncertainty, and doubt. Redwood City, CA: Addison-Wesley Professional.

[6] Knox, D. C. (2004). Effective Oracle database 10g security by design. New York: McGraw-Hill/Osborne. Phifer, L. (2010). Top ten data breaches and blunders of 2009. eSecurity Planet, February 10. Retrievedfrom http://www.esecurityplanet.com/features/article.php/3863556/Top-Ten-Data-Breaches-and-Blunders-of-2009.htm Privacy Rights Clearing House (2010). Chronology.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY