Various Database Attacks and its Prevention Techniques

K.A.Varunkumar[1], M.Prabakaran[2], Ajay Kaurav[2], S.Sibi Chakkaravarthy[2]

S.Thiyagarajan[2#], Pokala Venkatesh[2#]

[12]M Tech Scholars, Dept. of Computer Science

[2#]M Tech Scholars, Dept of EEE

Veltech Dr RR & Dr SR Technical University, Avadi

***Abstract*-Increasing in the popularity of internet, the application of database also widely spread. There are some serious threats because of hackers done various attempts to steal the data in the database. Various attacks like Sql injection, Cross site scripting may change the information in the databases which decreases the truthfulness of the database. Intrusion detection system is used to detect whether the attack is carried on the database. In this paper we surveyed different types of database attacks carried by hackers and some of the prevention techniques to protect the database management system.**

***Keywords*-Database, sql injection, cross site scripting**

I. Introduction

Since the Usage and application of internet increases, communications and computer network technology has been rapid development, especially the emergence of the Internet, makes the computer used in government, business, business, education, health care and other areas of society at an unprecedented rate, which are profound impact on people's economic, work and live. Network brings you convenience while brings more and more malicious attackers. They target the network database; make the database information security under serious threat. The SQL attack is one of common attacks, the tool of the SQL attack is SQL statements. Attackers towards programming vulnerability of application developers, submit well-constructed SQL statement to the server to achieve the goal of attacking.

II. Database attacks

Threats on database security can be grouped into two different categories, physical and logical. Physical threats consist of revelation of passwords, demolition of storage devices, stealing of important data by hackers. Most common method to prevent this type of attacks is put backup of the every storage devices. Logical threats are unauthorized access to information. Mostly done by the hackers by using the vulnerabilities inside the software, using these Vulnerabilities hackers modified the data. Reveal the passwords, denial of service.

A. Insiders Threat

Insider's threat can be done by the legitimate user who had access to reveal the confidential information in the database. Information can be easily transferred through electronic medium, printout or by direct conversation. It is difficult to prevent the data from this type of attacks Mandatory access control methods have to be implemented in the database while user logged in to the database must follow the certain rules such as data's should not copy to the unclassified location. These type of attacks can be handled by allowing limited number of users and certain complicated procedures .Attacker who sell the information to other companies has to be submitted under the employee disciplinary act.

B. Login attacks

Another easy way to get access for the database is to successfully login as authorized user. It can be done by physically stealing the information or monitor the traffic which shares the data for login information through several softwares.By using software tools in market, Passwords stored in operating system can be easily accessible. Login information can be secured only by usage of standard password setting methods. But it does not solve the problem Authentication &

Encryption techniques used in database have to be ensured with new standard algorithms. Now a day's web servers could be setup with the user authentication information directly sent to database or authenticate the user and then use authentication of web servers to login to the database. In these Method, System is Vulnerable because if any one of web server or database is compromised then automatically another component has to be surrendered for attacker. In general, Encryption or one time password is used .In sample application a manager can easily manage network traffic of employee by using various tools. If he could change the details, the employee can be easily fired

C. Network attacks

There are number of attacks on a database if it has access over an internet, a number of preventions can be place such as firewalls & ids to protect the database and web server, The data sent over a internet is secure by a SSL(Secure Socket Layer).Certificate is produced for both client & Server to avoid data stealing or information gathering while transferring data Denial of service is a common attack. This type of attack is related to web server allow access to database.

D. Inference Control

Access control methods used in a database such as user having access to limited information but user infer to get supplementary information they don't have access to. In contrast, higher level access i.e. Security had a right to access lower level security. This can be very difficult threat. A statistical database plays a vital role in inference control. Information about individual or user information can be shared only by queries in statistical data. A naïve approach would be to move the lower level data to higher level data. There is a complication whether all the data cannot be moved to lower level to higher level. It is not acceptable. Techniques which has query restrictions, data perturbation & data perturbation. A solution for the query pattern to be audited before rather complicated data's or information in database is compromised.

E. Trojan horse

Trojan horses are vulnerable software application that leak confidential data's. There applications is part of normal user but if it is installed in a computer or server. It easily migrates & sends the sensitive information for the attacker. But victim not aware of that trojan in network then attacker can mange or monitor the network easily could change the important information used by higher authorities. Here access controls are main issue but it get clearance level whether it is in lower security level.

III. Sql attacks

It is a technique which attacker injects the input code in queries which change order in the query structure intend by administrator and gains the access to database which results in deletion of data or user information in database. If the injection happens it will exploit vulnerabilities in database layer. It is a common attack used to get access or diphase the website. Input validation is most critical part in database in software design phase; if it is not covered then things get worse & create lot of vulnerabilities & security issues occurred.

A. Sql Prevention Techniques

When we study the protective system against SQL attacks, we should understand the process of SQL attacks and the interaction between client and server. Following is a B/S or C/S structure interaction. Shown in Figure 2. Client send a dynamic request, web server accepts the request and passed to the application server.

- The application server replies to the request from client send the query request to the database which executes the query.
- The set of records which is found in the database is returned to the application server; application server inserts data into the page, and then passes the page to the web server.
- Web server sends the completed client request to the client browser; the client shows the requested page. Based on the above analysis, we divide the protection system into the following sections to study.

B. Protection for ordinary users:

Ordinary users are the general users of web page, ordinary users can get information what they want from the site, is the main service targets of the web site. Because of the large number of ordinary users, diverse membership, it is very important to do the protection work about this part. The current website generally uses dynamic background management,

according to the template technique producing a static front page, so the website presents to users

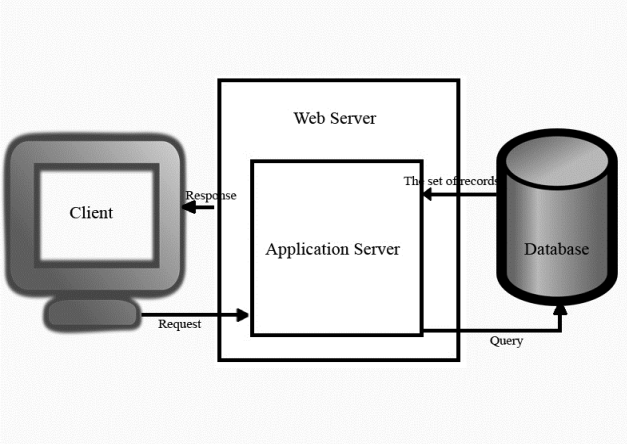

Fig1: B/S or C/S Structure interaction Process

most of static pages and some dynamic interactive pages, such as inquiries. For this situation, we propose the ordinary users protection model, mainly to protect dynamically constructed SQL occasions and prevent unauthorized users doing some damage work on the database which is shown in Figure 3.

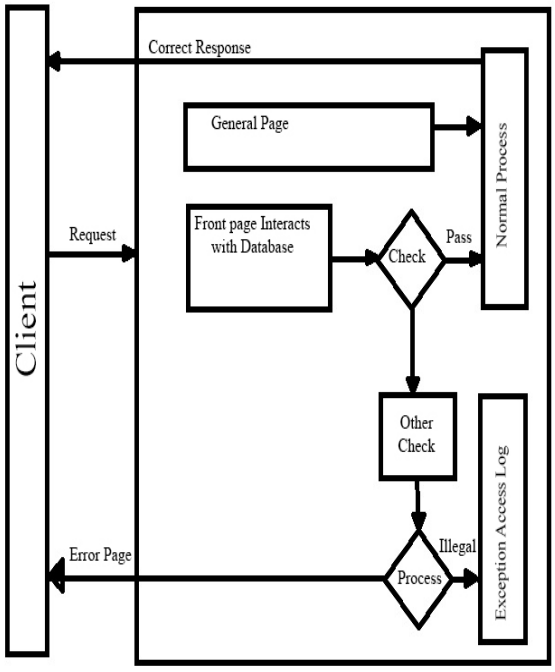

Fig2: Ordinary User protection Model

Server differentiate requests from the client, It directly goes to the normal process of general page, if the request is for the static page, if the request from the client needs to access the front page through database & then to check for the corresponds sql queries. If the sql queries passed checking, then go to normal process or to process ends with error handling

Significant methods of this protection model are as following:

Sifting illicit character, to prevent from an attacker to change the sql queries, if you don't check, then it will cause damage to database. For example, in a query page find product .asp? id=0.then original query resembles action to update the data but the attacker change the statement find product asp Id=1 as to drop The table from the database. Therefore filtering illegal characters plays an important role in protection model. In sql statements an occurrence of some illegal character will not pass the inspection while filtering & it will goes to exception handler.

- When the use of stored procedure to store the queries for execution. When a request of a client comes in .Then user call appropriate queries in the stored procedure & avoid dynamically constructed sql statements.
- Restricting the user access level, just we limit the privileges of high-level users. Sql statements who don't have correspondent privileges.
- We have to audit the records at regular intervals returned by the query if it doesn't match the results then query fails.

C. Protection for Administrators

If the administrator wants to upload some content in the site maintenance in the background level has to be done, so they should have data manipulation authorities, Therefore there is a good difference in between the privileges of administrators & ordinary Users. The sql statements checking for the administrators should be loose, so there is a key management protection in the background of the administrator. Login page for the background process have two factor authentication, Username plus password authentication & verification of hardware encryption lock. Administrator protection model shown in fig 4

Attacker gathers user information. Changes the user settings & show a false advertise for the user. Some of the attacks like cross site scripting, attacks comes from the http request form fields on webpage or cookies. If users can easily on trap by attacker set, Then data access sent to web application & then it comes back to user then the attacker starts execution,

So to detect cross site scripting on the website is predictably effective This paper proposed the detection algorithm for cross site scripting to achieve that we have to analyze the scenarios, Symbols which are used by attacker in method of cross site scripting

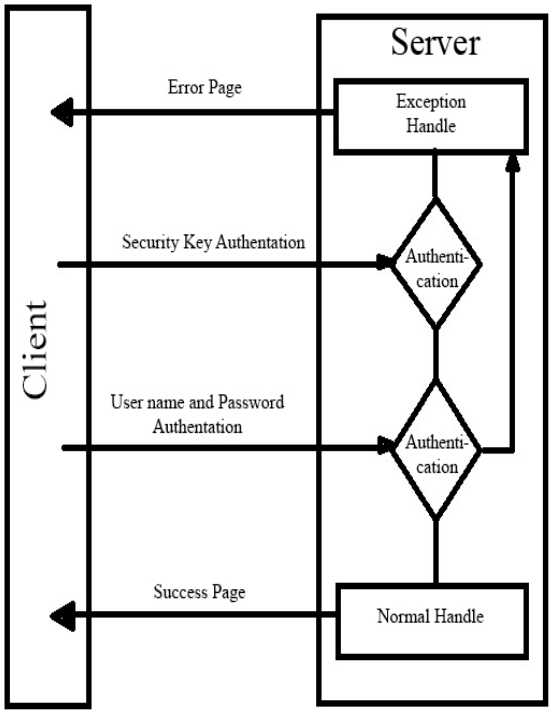

Fig 3:Administrator Protection Model

User name & passwords for the login has been used by the attacker.so we have to filter the user name & password entered by the user to avoid the cross site scripting events like 1='1' to login ,and encrypts the user information in database to avoid the attacker to find the administrators privileges by query knowledge database.

- By using Hardware encryption lock- Every hardware device has the encryption process which takes place. If the lock is inserted, the client sends the request to server, the server the reply packet, which have the information about the key. The client uses the key & process information & returns results to user, server validates key & process information is correct, then allows to continue, if not prohibit the operation of administrator.
- In the above steps, security of administrator account is a main concern. Administrators should be given more privileges They should follow to call the stored procedure .which are in system & It commands to felicitate the management of site maintenance, such as updating database such as deleting, adding data in the database

IV. Cross site scripting

Cross site scripting attacks are executed by injecting code such as JavaScript, VB Script, ActiveX or HTML. The purpose of attackers

A. Detection & Prevention Techniques

A. "Protecting Cookies from Cross Site Script Attacks Using Dynamic Cookies Rewriting Technique".(Rattipong Putthacharoen, Pratheep Bunyatnoparat) (2011)[8] This approach aims to change the cookies in such a way that they will become useless for XSS attacks. This technique is called "Dynamic Cookie Rewriting" implemented in a web proxy where it will automatically replace the cookies with the randomized value before sending the cookie to the browser. In this way browser will keep the randomized value instead of original value sent by the web server. At the web server end the return cookie from the browser again rewritten to its original form at the web proxy before being forwarded to the web server. So incase if XSS attacks steal the cookies from the browser's database, the cookies cannot be used by the attacker to impersonate the users. This technique is not tested with HTTPs connections.

B. "An Execution-flow Based Method for Detecting Cross- Site Scripting Attacks"(Qianjie Zhang, Hao Chen, Jianhua Sun)(2010) [9]Qianjie Zhang, Hao Chen, Jianhua Sun presents an execution-flow analysis for JavaScript programs running in a web browser to prevent Cross-site Scripting (XSS) attacks. In this approach they use Finite-State Automata (FSA) to model the client-side behavior of Asynchronous JavaScript and XML (AJAX) applications under normal execution. In this method, system is deployed in proxy mode. In this mode the proxy analyzes the execution flow of client-side JavaScript and checks them to be with compliance to the models generated by FSA. It stops potentially malicious scripts, which do not conform to the FSA before the requested web pages arrive at the browser. This method is evaluated against many real-world web applications and the result shows that it protects against a variety of malicious scripts to prevent XSS attacks and has an acceptable performance overhead.

C. "Automatic Creation of SQL Injection and Cross-site Scripting (XSS) Attacks (Ardilla)" (Adam Kie_zun, Philip J. Guo, Karthick Jayaraman, Michael D. Ernst)(2010) [10] Adam Kie_zun has suggested a technique for finding vulnerabilities in Web Application such as SQL injection attack and Cross site scripting (XSS).They implement this technique as an automated tool called Ardilla. This method uses static code analysis to find vulnerabilities. This technique works source code of the application, creates concrete inputs that expose vulnerabilities and operates before the application is deployed. It analyses application internals to discover vulnerabilities in the code. It is based on input generation, taint propagation, and input mutation to find variants of an execution that exploit vulnerability. This tool is designed for php applications.

V. Conclusions

This paper surveyed different types of Sql injection & cross site scripting is carried by attackers in web based environment .we provide some detection & prevention techniques provided in some articles & papers.Eventhough academic & industry researchers provide some strategies for protecting online environment. Keeping in view the emerging web technologies and extensive usage of highly interactive content over Internet, it is imperative for the software development houses and developers to frame a appropriate framework for protecting web environment is needed.

REFERENCES

[1] S. Inoue and T. Matsuda, On the attack feature extraction of SQL Injection Attacks by the Related Word Extraction Algorithm, 20 12-MPS-87(30), 1-2, 2012 (in Japanese).

[2] T. Oishi, S. Kuramoto, T. Mine, R. Hasegawa, H. Fujita and M. Koshimura, A Method for Query Generation Using the Related Word Extraction Algorithm, The Institute of Electronics Information and Communication Engineers, J92-D(3), pp. 281-292, 2009 (in Japanese).

[3] 1.Antunes, N. and M. Vieira, “Defending against Web Application Vulnerabilities.” Computer, 2012. 45(2): p. 66-72.

[4] (OWASP), “O.W.A.S.P. Top 10 Vulnerabilities.”; Available from: https://www.owasp.org/index.php/Top_10 2013.

[5] Shar, L.K. and T. Hee Beng Kuan, “Defeating SQL Injection.” Computer, 2013. 46(3): p. 69-77.

[6] Janot, E. and P. Zavarsky. “Preventing SQL Injections in Online Applications: Study, Recommendations and Java Solution Prototype Based on the SQL DOM.” in OWASP App. Sec. Conference. 2008.

[7] McClure, R.A. and I.H. Kruger. “SQL DOM: compile time checking of dynamic SQL statements. in Software Engineering, 2005.” ICSE 2005. Proceedings. 27th International Conference on. 2005.

[8] Rattipong Putthacharoen, Pratheep Bunyatnoparat “Protecting Cookies from Cross Site Script Attacks Using Dynamic Cookies Rewriting Technique" Feb. 13~16, 2011 ICACT2011. Method for Detecting Cross-Site Scripting Attacks".

[9] Qianjie Zhang, Hao Chen, Jianhua Sun “An Execution-flow Based Method for Detecting Cross-Site Scripting Attacks” China (2010)

[10] " Automatic Creation of SQL Injection and Cross-Site Scripting Attacks "ARDILLA (Adam Kie_zun, Philip J. Guo, Karthick Jayaraman, Michael D. Ernst)

[11] W. G. Halfond and A. Orso. AMNESIA: Analysis and Monitoring for Neutralizing SQL-Injection Attacks. In Proceedings of the IEEE and ACM International Conference on Automated Software Engineering (ASE 2005), 2005.

[12] G. T. Buehrer, B. W. Weide, and P. A. G. Sivilotti. Using Parse Tree Validation to Prevent SQL Injection Attacks. In International Workshop on Software Engineering and Middleware (SEM), 2005.

[13] Z. Su and G. Wassermann. The Essence of Command Injection Attacks in Web Applications. In The 33rd Annual Symposium on Principles of Programming Languages (POPL 2006), 2006.