VIT®

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

NASSCOM REVIEW 1

SQL INJECTION

LITERATURE SURVEY

Fall Semester 2020-21

NAME: Muskan Rastogi

REGNO. : 18BIT0287

SUBMITTED TO: Prof. Sumaiya

COURSE CODE: CSE3501

Muskan Rastogi

1. SQL Injection: A Sample Review

TECHNIQUE IMPLEMENTED AND AS TO WHY IT WAS CHOSEN

A. *SQLUnitGen*:

It was proposed by Shin and colleagues. It stands for "SQL Injection Testing Using Static and Dynamic Analysis". Their technique uses analysis which is static to note down the flow of the input generated by the user for testing. Most of their tools and techniques utilize "JCrasher". JCrasher is a tool which is used to obtain test cases where attack inputs are made and further analysis is produced and thus, concrete conclusions are drawn.

B. *String Analyzer:*

The idea was first inculcated by Wassermann and Suo They aimed for an algorithm which is grammar based and which strategizes the string values as CFGs (Context Free Grammar) and operations based on strings as language transducers following minimization. This solution then highlights the input strings and assign them a particular tag and then works on them accordingly.

SQL ATTACK MODEL

In today's world, SQL Injection is a serious security threat over the Internet for the various dynamic web applications residing over the internet. These Web applications conduct many vital processes in various web-based businesses. As the use of internet for various online services is rising, so is the security threats present in the web increasing. There is a universal need present for all dynamic web applications and this universal need is the need to store, retrieve or manipulate information from a database. Most of systems which manage the databases and its requirements such as MySQL Server and PostgreSQL use SQL as their language. Flexibility of SQL makes it a powerful language. It allows its users to ask what he/she wants without leaking any information about how the data will be fetched.

ALGORITHM/ PSEUDOCODE

A. *Tautologies:*

This is the most basic type of SQL injection attack. It is done, by simply making the "WHERE" clause always true for every query, which results in bypassing the condition inside the SQL statement.

For instance, SELECT * FROM User jnfo WHERE Username 'MARONIA' and Password='1205002 '. In this query attacker can inject OR 1= '1'.

The resulting query will be:
SELECT * FROM User jnfo WHERE Username = '' OR 1= 'J '; -- and Password= '1 don 't care''.

B. *Logically Improper Queries*:

The aim of the attacker is to gather all possible information about the structure and the schema of the tables and their fields inside the database. This belongs to the SQL manipulation attack where the error message generated by the database provides the attacker with an advantage.

C. *Union Queries*:

This is a kind of code injection and SQL manipulation attack. In SQL language, UNION operator is used to merge two independent queries together. Here, the UNION operator is used by the attackers for data extraction from different tables.

The attacker sends a SELECT query and UNION the original SQL statement with it, but for that to happen successfully the attacker needs to have a clear idea about the structure of the database schema and there tuples like table name etc, so that he can have maximum impact from his second part of the query when he joins it with the original.

PERFORMANCE ANALYSIS

EXISTING MODEL	SUGGESTED MODEL
According to the OW ASP studies, SQL injection holds the first position in the list of top 10 web application vulnerabilities. These attacks are not just limited to the web applications, they can also hit desktop applications as their databases are powered by SQL. The amount of financial losses every year as a result of such attacks is enormous.	It is a technique for the prevention of SQL injection by using arbitrary SQL query to check if there is any suspicious statements or not and then terminate them. For this they use proxy server between webserver and database server to de-cipher the template query inside the CGI script and the database parser which are received from client to database server. Later the designer will intercept the traffic between the application and the database, by using a proxy that will intercept and if any keywords without randomization are found then it is considered a SQL injection.

2. SQL injection attack and guard technical research

TECHNIQUE IMPLEMENTED AND AS TO WHY IT WAS CHOSEN

With C/S (client/server) model development, use this technique writing web applications will be more and more. Web server as now enterprise and individual information exchange, the main media access to any of the personnel are available to the general public, plus due to current network programmers safety consciousness is uneven, quite part of server code without considering the input information security filters, make the Web server and database server program there are serious security hidden danger.

A malicious user can use this to obtain server front-end and back-end control privileges, injection attack is held the present server exist interactive interfaces characteristics, through the client browser submit carefully constructed deformity statement, a server interaction analytical processing to achieve the purpose of attack.

SQL ATTACK MODEL

With the spread of the Internet and the WEB's rapid development, WEB applications not only improved the efficiency of work and enterprise strengthens the enterprise market competitiveness. Web platform have flexible, efficient, low cost and other information superiority has greatly improved the related department work efficiency, and promote the actual business thorough development, enhance the department and the outside world exchange, service and interaction.

Our country's computer industry after more than ten years of development, the national industry production management system, are based on the Internet architecture, in the country's defense engineering, government office, financial systems, to network games, online banking, network transactions, is inseparable from the network.

ALGORITHM/ PSEUDOCODE

(1) *Website unauthorized access*:

Internet is an open, no control agency network, based on TCP/IP protocol Internet protocol families own open great place show various computer networking and interconnection and directly, and promoted the rapid development of Internet technology. But as in the early network protocol design neglect the safety, cause Internet in use and management of chaos, and gradually make the Internet itself of safety and security has been threatened.

Hackers (Hacker) often get the chance to intrude into the computer on the network system, or stolen confidential data and theft privilege, or destroy the important data, or make the system function not fully exert until paralysis.

(2) *Information security management*:
Information security management including physical protection and application of protection. Physical protection referred for information in network of physical equipment installed in the physical environment barriers, prevent from physical lines of electromagnetic signals eavesdropping. In network management center, important data exchange and data storage place, according to confidential construction requirements, and set up standard, relatively independent network exchange center and important switching nodes, adopt anti-static grounding.

(3) *Of network virus spread*:
With the expanding of network size, computer network virus to site the threat of a bigger role. Network virus spread on the Internet very fast, and its harm is enormous.

PERFORMANCE ANALYSIS

EXISTING MODEL	SUGGESTED MODEL
Due to the various Web server vulnerabilities and procedure of the rigor leads to a Web server script for attacks was increasing, its are mostly through the ASP or PHP scripting injection such as a major attack means, plus Web site rapid expansion of today, based on both the SQL injection also slowly become the mainstream way. Attack SQL injection is to use the insert harmful character attack technology. The attacker using programmers to user input data legitimacy detection.	The use of parameterized lactobacillus colonisation statement. To defense SQL injection, user input is absolutely cannot directly to be embedded SQL statements. On the contrary, the user input must be filtered, or use of parameterized statement. Parametric statements and not use parameters user input into the statement. In most cases, the SQL statement was fixed. Then, the user input will be limited to a parameter.

3. STUDY ON SQL INJECTION ATTACKS: MODE, DETECTION AND PREVENTION

TECHNIQUE IMPLEMENTED AND AS TO WHY IT WAS CHOSEN

The working of proposed methodology is defined in two kinds:

1) New Client Registration:

A new client enters the log in details like distinctive name and secret key on client side to get registered. As indicated by the proposed design, the distinctive name and secret key is prepared at the center level.

Below are the stages:
1. To discover hash value of log in name by secret key as cow.
2. To discover hash value of secret key by log in name as cow.
3. Linking the result of step1 and step2 to discover final hash code.
4. Login name, Secret key and final hash code are to be put away into the client table.

2) Login and verification:

The login structure must be filled by the client to get signed into the database.

Below are the given stages:-
1. A distinctive name and secret key is to be entered at client side.
2. The name put away in client table is matched with the entered client name.
3. As per proposed system to discover final hash code at run time, the client name and secret key is handled after the client name is being matched.
4. Final hash code and secret word is checked with stored values in the database.
5. In the event that client is legitimate then he/she can get to data from database or else incorrect text is shown.

SQL ATTACK MODEL

The proposed framework notices on how SQLIA on Web applications by tokenization and encryption for detection and prevention. The tokenization process changes over the input query in fruitful token and dynamic table stores it at the user end. Name of field, name of table and information are encoded by AES algorithm is connected by recognizing spaces on the data query, double dashes and single quotes, and so on. The initial encrypted query and table which is tokenized is being sent on the server side.

Now the query is decrypted and generated into number of tokens which are then stored into other dynamic table at the server end. After comparing both the dynamic tables, if they are same then it is evaluated that there was no injected query, henceforth the query is carried to the central database for fetching the output. In the event that they are distinctive, query is dismissed and not sent to the server of the database.

ALGORITHM/ PSEUDOCODE

Tautologies:
These kinds of attacks inject SQL tokens to the conditional query statement which are constantly assessed to be genuine. This type of attack uses WHERE clause to extract the valuable information from the input fields which are easily accessible that leads to the failed authenticity of control.

Logically Incorrect Queries:
At the point when a query is not required, an incorrect text from the database, including required data is returned. These incorrect texts help attackers to find parameters in the application and in this manner the application's database. Without a doubt attackers garbage info or SQL token injected into query language structure mistake, to deliver logical error, syntax error, or type mismatches purposely.

Union Query:
By this strategy, the attacker provides the incorrect data with the few correct fields, the SQL query is sent with the ‘Union’ of both correct and incorrect fields. As the result, the dataset from the database is fetched with the correct fields.

PERFORMANCE ANALYSIS

EXISTING MODELS	SUGGESTED MODELS
Web applications deals with complex user information. Unauthorized access can lead to collapse of a system; even can harass the existence of a company or a bank or a branch. SQL Injection Attacks (SQLIA) is a standout amongst the most hazardous security dangers to Web applications. Researchers are working to control SQLIA at the application layer, but beforehand they are trying to prevent SQLIA.	A strategy to change over SQL query into number of helpful tokens by applying tokenization and after that encoding all literals, fields, table and information on the query by AES-algorithm to avoid SQLIA. Our exploratory results demonstrate that a wide range of SQLIA can successfully be prevented by this methodology. It can likewise be effectively connected to some other dialect and database stage without significant changes.

4. Review of SQL Injection : Problems and Prevention

TECHNIQUE IMPLEMENTED AND AS TO WHY IT WAS CHOSEN

The definition of the literature is the report of the information which is evaluative that found in the literature relevant to our elected area of the study. The review should be specify, summarize, classify and interpret the literature. The review should provide the theoretical, analytical base for the research. Database is depository of the most significant and valuable data and information in the company.

In the database there different of security layers which is the security officers, system administrator, database administrator, the employees and the developers. The attacker can crack this security layers. Some reviewed papers were studied for avoiding the attacker can crack this security layers

SQL ATTACK MODEL

In SQL Injection attacks, these are some of the methods of SQL injection attacks such as Using Unauthorized Queries, Stored Procedures, UNION Query and Bypassing Web-based Application. Firstly, the purpose of hackers use Unauthorized Queries technique is because of they want to know the structure of the table. They first input the illegal queries to the web based application. Then, the web based application will detect the error and display the error. From the errors, hackers can know a little bit about the structure of the table.

After they had known the structure of the table, they can attack the web based application by SQL injection. Secondly, in Stored Procedures, most of the web based application saved the stored procedures and use it for data transmission. As the developers, they thought that by saving the stored procedures, it will prevent SQL attacks.

ALGORITHM/ PSEUDOCODE

Attack which is achieved by the direct hitting is the direct attack. If the database is does not contain any security system, the attack is successful. If the attackers change to the next attacks that means the attacks are failed. The meaning of the indirect attack is not directly executed on the objective but the information and data from the objective can be collected through other transitional object for the security system to be trick. The indirect attack is difficult to be track. For the further types of attacks are passive attack and the active attack. For passive attack, clear text passwords and important data and information which can be used in other types of attack and it is also unencrypted traffic to be guide. It is also display of information and data to the attackers beyond the permissions of the users. The active attack is the attackers had performed many attempts to breach the secured system to get the information and data which is stored in the database. The attack can be completed through many ways such as viruses, worm, stealth and others. The information can be accomplished in electronically attack illegal beyond user knowledge.

PERFORMANCE ANALYSIS

EXISTING MODEL	SUGGESTED MODEL
Database normally contains data definition language and data manipulation language for allowing result retrieval. Meanwhile, Injection is an action of injecting something into an organism. SQL injection is a technique for hackers to execute malicious SQL queries on the database server. It can be executed over a web-based application to access over the databases that contain sensitive information.	This SQL injection is frequently happen because of the vulnerability of the web based application and the lack of awareness regarding the security of the database. There are a lot of ways for the SQL injection to be performed by the hackers outside there. So, to prevent this from happening, as a developer of a web based application, must be put an important priority to the security of web based application to ensure that all of the data in the database is kept safe and sound. The security of the web based application should be tested to check the either the security is vulnerable to SQL injection or not.

5. Analysis of SQL Injection Detection Techniques

TECHNIQUE IMPLEMENTED AND AS TO WHY IT WAS CHOSEN

We have taken different techniques which can be used in order to detect and prevent the attacks. These techniques will help the researchers and security professionals to take proper action or use the specified techniques to solve the crises arisen inside the organization due to an attack. The techniques described here can be used to develop a system with the optional functionality in order to protect the system from any kind of these modern attacks that corresponds to the Compounded SQL Injection and Fast Flux SQL Injection attacks.

According to the survey performed, we observed that the Static Code Analysis and Machine Learning are the best among the others but other techniques has various other advantages.

SQL ATTACK MODEL

There are numerous types of SQLIA's and each has different approach for attacks onto the website. The complex formation occurs with the combination of SQL Injection and XSS attacks which lead to retrieval of the Database information. Even the SQL Injection attacks are taking place in the Rich Internet Application by finding the vulnerability in cross domain policies. Most of the modern websites extensively use Rich Internet Application such as Adobe Flash and Microsoft Silver light, for increased user defined functionality. If the care is not taken during the coding of cross site scripts,it can lead to the vulnerability of XSS and SQL Injection Attacks.

ALGORITHM/ PSEUDOCODE

1. Piggy Backed Queries:

Intent of Attack: Retrieval of Information, Denial of Service In this type of attack the attacker "Piggy Back" the query with the original query in the input fields present on the web application.The piggy backed can be defined as "on or as if on the back of another". The database receives the multiple queries.

2. Stored Procedure:

Intent of Attack: Escaping Authentication, Denial of Service, More freedom on Database Stored Procedures are widely used as a subroutine in a relational database management system. They are compiled into single execution plan and extensively used for performing commonly occurring tasks.Its used in businesses as it provides single point of control while performing the business rules.

3. Union Query:

This type of attack uses Union Operator (U) while inserting the SQL Query. The two sql query are joined with the Union Operator. The first statement is a normal query after which the malicious query is appended with union operator.

PERFORMANCE ANALYSIS

EXISTING MODELS	SUGGESTED MODEL
SQL Injection is one of the vulnerabilities in OWASP's Top Ten List for Web Based Application Exploitation. These types of attacks takes place on Dynamic Web applications as they interact with the databases for the various operations. Current Content Management System like Drupal, Joomla or Wordpress have all the information stored in their databases. A single intrusion into these types of websites can lead to overall control of websites by the attacker. Researchers are aware of the basic SQL Injection attacks but there are numerous SQL Injection attacks which are yet to be Prevented and Detected. Over here, we present the extensive review for the Advanced SQL Injection attack such as Fast Flux Sql Injection	These tools are ready made and some are open source which can be downloaded from the internet. Most of these tools were developed for the research purposes but due to its significant advantages they are being used in the commercial sectors. The tools are discussed giving the broad overview that which of these tools can be used for the particular type of attacks. According to our survey performed we observe that the Noxeus and SQLMap are latest and have better prevention and detection mechanism

[illegible] Rastogi