INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

Detection and Prevention of SQL Injection Attacks

Harsh Joshi, Abhay Mishra, Sujal Vishwakarma, Jash Mehta

Diploma Students, Dept. of I.T., Thakur Polytechnic, Maharashtra State Board of Technical Education, Kandivali East,

Mumbai, Maharashtra, India

ABSTRACT: Web sites are dynamic, static, and most of the time a mix of both. websites would like protection to their database to assure security. An SQL injection attacks interactive internet applications that offer database related services. These applications take user inputs And use them to make an SQL query at run time. In AN SQL injection attack, AN attacker may insert a malicious SQL question as input to perform AN unauthorized database operation. Using SQL injection attacks, AN attacker will retrieve or modify confidential and sensitive data from the database. it should jeopardize the confidentiality and security of websites that all depends on databases.Database driven internet application are prone to SQL Injection Attacks which attempt to access the sensitive information directly. They work by injecting malicious SQL query through the online application and cause surprising behavior from the info. There are different Techniques that are pro- posed by researchers to forestall or find these style of attacks. This project presents a code that implicitly protects the applications that are written in PHP from SQL injection attacks. It uses an approach that combines static similarly as dynamic analysis. In this project, we have discussed an automated technique for moving out SQL injection vulnerabilities from website.

KEYWORDS: Sql Injection, Sqlquery.

I. INTRODUCTION

Many of the online applications use database as their back-end data store. Although new programming languages offer new ways that of more safer database programming options, still there are several applications that are vulnerable to SQL injection attack. Due to the character of this attack which is unauthorized access to the confidential data and inserting or modifying it, this type of attack is incredibly in style among attackers and once more because of the mentioned reason it's vital to create internet applications secure against them. The SQL injection attack happens typically once AN attacker tries to achieve access to a info by inserting malicious inputs to the queries that amendment the logic, syntax or linguistics of the legitimate question. There are many types of SQL injection attacks like, tautologies, alternate encodings, UNION, ORDER BY, HAVING.

And reciprocally there are several instructed ways attempting to find the vulnerabilities within the applications and stop the attacks. To be a lot of specific, this project presents with many projected ways and tools to find and prevent the SQL injection attack to be ready to get a large vary of ideas in this way and compare them against one another. we have a tendency to outlined a technique in our analysis to be ready to get a lot of data from every paper. So, after that it had been a lot of easier to check the ways and analyzing them. we focused on main components and phases of every technique projected in each paper and then I found the benefits and limitations of them at the top.

The project in the main focuses on protective on the personal information of users organizations. For that we've outlined a technique that contains 3 layers of protection

SCRIPTING LANGUAGES USED

❖ **What is PHP?**
- PHP is an acronym for "PHP: Hypertext Preprocessor"
- PHP is a widely-used, open source scripting language
- PHP scripts are executed on the server
- PHP is free to download and use

❖ **Why PHP?**
- PHP runs on various platforms (Windows, Linux, Unix, Mac OS X, etc.)
- PHP is compatible with almost all servers used today (Apache, IIS, etc.)
- PHP supports a wide range of databases
- PHP is free. Download it from the official PHP resource: www.php.net
- PHP is easy to learn and runs efficiently on the server side

❖ **What is SQL?**

SQL (Structured Query Language) is a domain-specific language used in programming and designed for managing data held in a relational database management system (RDBMS), or for stream processing in a relational data stream management system (RDSMS). It is particularly useful in handling structured data, i.e. data incorporating relations among entities and variables. SQL offers two main advantages over older read–write APIs such as ISAM or VSAM. Firstly, it introduced the concept of accessing many records with one single command. Secondly, it eliminates the need to specify *how* to reach a record, e.g. with or without an index.

❖ **Why SQL?**

- Faster Query Processing
- No Coding Skills
- Standardized Language
- Portable
- Interactive Language
- Multiple data views

❖ **What is HTML?**
- HTML stands for Hyper Text Markup Language
- HTML is the standard markup language for creating Web pages
- HTML describes the structure of a Web page
- HTML consists of a series of elements
- HTML elements tell the browser how to display the content
- HTML elements label pieces of content such as "this is a heading", "this is a paragraph", "this is a link", etc.

❖ **What is CSS?**
- CSS stands for Cascading Style Sheets
- CSS describes how HTML elements are to be displayed on screen, paper, or in other media
- CSS saves a lot of work. It can control the layout of multiple web pages all at once
- External stylesheets are stored in CSS files

II. RELATED WORK

Planning the Structure of the website
In this system we have a tendency to 3 main protection techniques that facilitate US to forestall the sql injection attacks and also to build the web site safer.
1.   **PhpFilters :**
It contains a function which has a query as input. It verifies whether or not the query is vulnerable for database, if affirmative then it restricts the access.
2.   **JavaScript Filters :**
The keywords or vulnerable queries are detected through string associate array in this part and are prevented.
3.   **Data Protection :**
If a attacker passes through each this levels or parts then this phase will stop them as during this part the information is keep in encrypted for- mat. For this encryption method we've used MD 5 cryptography algorithmic rule(MD5 algorithm).

❖ **Proposed Work**

• **Problem Definition**

This system aims to find illegal SQL queries before being ex- ecuted on the database. It supported the mix of static and dynamic analysis technique to verify the correctness of SQL queries. In its static half it use a program analysis to make a model of the right queries that may be generated by the on- line application, and within the dynamic half this system use the run-time observation to ascertain the generated queries against the statically designed model. If the queries don't match with model, it will be rejected and contemplate that as the SQL injection attack, but just in case of matching with the model, it'll continue execution into the database.

• **Project Objects**

➢ To develop a system that may forestall the sql injection attack.
➢ To protect the info of user by permitting solely authenti- cated user.
➢ To find malicious code once anyone tries to input with the help of SQL Injection.

III. PROPOSED METHODOLOGY

All the members agreed to this topic and we planned our project in detail such as, what should be included, what would be features and functionalities, etc. Everyone collectively come up with new ideas. We also took guidance of our teachers as they helped us and tried to solve our problems. They informed us about the changes to be made. After the discussion phase, we Started working on our project. Many problems occurred but we all overcame the obstacles and Successfully developed our project.

IV. CONCLUSION AND FUTURE WORK

In proposed system we are going to develop a system that can prevent sql injection attacks.The proposed system gives new technique for preventing SQL Injection attack. Normally attacker tries to complicate the middle layer technology by reforming the SQL queries.The system that is totally secured from injection attacks.In future, the proposed project can be automated by developing some algorithm and real time application to facilitate web developers in more efficient manner. The whole research is done on PHP based projects, in future it can be extended to some other programming languages like Python, ASP etc.

REFERENCES

1. www.wikipedia.org
2. http://en.wikipedia.org/wiki/SQLinjection.
3. https://ieeexplore.ieee.org/document/9022833
4. https://www.w3.org/standards/webdesign/htmlcss
5. https://www.w3schools.com/html/html_css.asp

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.165

doi crossref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

NISCAIR
निस्केयर

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

📱 9940 572 462 🟢 6381 907 438 ✉ ijircce@gmail.com

Scan to save the contact details