**DETECTION AND PREVENTION OF**

**SQL INJECTION ATTACKS**

***B.TECH SEM – VII Mini PROJECT***

***Dept. of Computer Science & Engineering***

By

**Karansinh Vaghela 18BCP048**

**Rachit 18BCP089**

**Vyomesh Jethava 18BCP152D**

**Under the Supervision**

**Of**

**Dr. Payal Chaudhari**



**SCHOOL OF TECHNOLOGY**

**PANDIT DEENDAYAL ENERGY UNIVERSITY**

**GANDHINAGAR, GUJARAT, INDIA**

**July – December, 2021**

**ABSTRACT**

Personally identifiable information (PII) is information regarding things such as bank accounts, retirement or stock investments accounts, credit card accounts, medical records, or insurance claims. There is a need to protect the PII in databases that are connected to the ubiquitous, global network that is the Internet. If there is any vulnerability in the protection in a system that holds PII, then it presents an opportunity for an unauthorized person to access this PII. One of the techniques available to would be information thieve is SQL injection (SQLI). In this project, a system is developed to analyze the values submitted by users through HTML forms and look for possible attack patterns. Once the systems find such a pattern, it blocks the attack and makes a record of the activity. If an attacker continues to pass such attack patterns, the system blocks access by this user together. A mechanism is included to block users who attempt to log in at abnormally high rates. This provides a combination of pattern-based detection and anomaly-based detection to create a reasonably robust intrusion detection system, with respect to SQLI attacks.

**Introduction**

**What is SQL Injection?**

SQL injection is a technique used to exploit user data through web page inputs by injecting SQL commands as statements. Basically, these statements can be used to manipulate the application’s web server by malicious users.

SQL injection is a code injection technique that might destroy your database.

SQL injection is one of the most common web hacking techniques.

SQL injection is the placement of malicious code in SQL statements, via web page input.

**SQLI Attack Sources**

Injection through user input

Injection through cookies: Recent web applications use cookies to store users preferences.

Injection through server variables : Server variables are a set of parameters that contain network headers, HTTP metadata, and environmental variables.

Stored injection: In stored injection (called also second-order injection), attackers embed malicious inputs into a database to indirectly launch an SQLIA each time that input is used.

**Attack Goals**

Identifying injectable parameters: As a first step, hackers try to identify which parameters could be used to inject malicious code.

Performing database fingerprinting: To construct a query format supported by the target database engine, the attacker needs to know the database finger-print.

**Literature Review**

In this paper, author proposed an overview of the SQLI attack. The different attack sources, goals and types are described and discussed. A classification of the different SQLI attack detection and prevention countermeasures are presented. A comparative table between the different proposed SQLI attack countermeasures was presented.

With the rapid development of Web technology, network applications have become part of our lives. At the same time, Web applications are confronted with more challenges. As announced by the OWASP organization, injection attack has been the first of the top 10 security vulnerabilities in 2013 and 2017, and SQL injection attack is one of the most important types among the injection attacks.

SQL is a standard database programming language for accessing and manipulating data in database. WEB programming languages (such as PHP, JAVA) provide various methods for constructing and executing SQL statements. Developers usually construct statements by concatenating string which is submitted by users from web page

**EXISTING TOOLS**

There are a number of existing tools available, both hardware and software based, to deal with SQL-Injection attacks. Tools exist to detect SQL-Injection attacks while others try to identify and fix SQL-Injection vulnerabilities. The following are a few software ones we will discuss.

• GreenSQL

• dotDefender

• CodeScan Labs: SQL-Injection

GreenSQL is a free Open Source database firewall that sits between the web server and the database server and is used to protect databases from SQL injection attacks. The logic is based on evaluation of SQL commands using a risk scoring matrix as well as blocking known database administrative commands (e.g., DROP, CREATE, etc). Reports are generated on timestamp, query pattern, reason blocked (e.g., true expression, has 'or' token). It has a white list of approved SQL patterns. However, only MySQL database is currently supported. In comparison, the IDPS in this project may be used with any relational database, not just MySQL. The IDPS has both black and white list pattern features.

Applicure’s dotDefender is a web application firewall that offers a SQL-Injection solution. dotDefender is a multi-platform solution running on Apache and IIS web servers. Central management ensures a single point of control and reporting for all servers. There is an application layer firewall in front of web applications. It has a set of security rules that enable it to be a powerful solution. However, the cost is prohibitive.

The annual license costs $1,810 while a perpetual license is $3,995, which are both pricy for personal use.[4] While dotDefender is an expensive product, IDPS is a free product. Another product is CodeScan Labs’ SQL-Injection detection product. It has the capability to scan web application source code that you selected for code syntax vulnerabilities. It subsequently generates a "debug style" report. The speed depends on how large the web application is and its complexity. The CodeScan software does not fix the code, however; it only points out the issues. The company offers a 21-day free trial, but normally it requires a yearly subscription to be maintained. The actual price is not advertised and one must contact sales representative to find out the cost. A separate activation key is required for different programming languages and additional capabilities.

**PROPOSED WORK:**