Securing Firewall Against Denial of Firewall And SQL Injection Attacks

B. Yamini[1], L. Brindha[2], S. Deepananda Arthi [3]
[1,]Assistant Professor, Dept of CSE
[2, 3]Dept of CSE
[1, 2, 3] Jeppiaar S.R.R Engineering College.

Abstract- *Firewalls are most important and critical devices which provides securities against all vulnerabilities. Firewall handles all the traffic in and out of the network. We think firewall is secure but it's not many vulnerabilities compromise the firewalls. Hackers / intruders exploit the firewall using malicious scripts and access the server / applications. In this paper, we analyze Denial of Firewalling and SQL injection attacks. Denial of Firewalling is attacker overloads the firewall and SQL injection is bypassing the security protocol by malicious scripts. Our proposed system provides efficient fingerprinting methods to prevent the attacks. Also the proposed system provides security against application as well. If the firewall is been compromised, intruder cannot access the files in the application or server because application is made secure against most common web vulnerabilities. This application security is achieved using web vulnerability scanner which scans all the scripts used inside the application for vulnerability injection scripts (CSRF and SQL injection).*

Keywords- Prepared statement, IP Address blocking, vulnerability scanner, Deep packet inspection.

I. INTRODUCTION

A. Motivation

The first line of defence in defending various activity among network is firewall. Which involves in protecting both the enterprise and backbone networks by examining the traffic in and out[2][3]. To exploit firewall vulnerabilities, the first step that attackers need to do is firewall fingerprinting, i.e., identifying the particular implementation of a firewall including brand name, software/firmware version numbered. For example, in the seminal work by Qian and Mao[3], the attack discovered by them assumes that the attacker knows the particular implementation of the firewall under attack. On the defence side, we first need to know how attackers possibly can fingerprint a firewall so that we can design counter measures accordingly; second, we need to know how attackers can possibly attack a firewall over the Internet.

. In this paper, first we investigate two methods for inferring firewall implementation. The first method is the firewall decision on the unusual flags of sequence of TCP packet used in identification as a firewall fingerprint .The second method is based on machine learning techniques. We further investigate on firewall defence mechanism. To our best knowledge, this paper represents the first study of SQL injection and Denial of Firewalling attacks.

B. Limitation of Prior Art

The prior art focused on defence mechanisms from the firewall administrators perspective[1], such as preventing attackers from gaining information about the firewall deployed and hence forcing attackers to use less-effective, blind attacks. Which increase the chance of incorrect firewall implementation inference by concealing firewall TCP flag fingerprints and obscuring the pattern in probe PPT.

C. Technical Challenges

To evaluate the effectiveness of defence mechanisms of firewall fingerprinting and to measure the impact on firewall performance, there needs extensive equipments and technique, therefore there leads to the expansion of tested software. Further there exists various parameters to be considered, one among them is SQL injection attack and DDOS attack and the defence mechanism for them varies, which as not yet considered.

D. Our Approach

In this paper, for first time, we propose a set of techniques to protect from SQL injection and DDOS attack. Denial of firewalling is attacker overloads the firewall and SQL injection is bypassing the security protocol by malicious scripts. Our proposed system provides efficient fingerprinting methods to prevent the attacks. In SQL injection, we detect and prevent the following malicious queries,

1. SQL login bypass
2. Blind injection

3. SQL sleep attack
4. Data fetching attack

Also the proposed system provides security against application as well. If the firewall is been compromised, intruder cannot access the files in the application or server because application is made secure against most common web vulnerabilities. This application security is achieved using web vulnerability scanner which scans all the scripts used inside the application for vulnerability injection scripts (CSRF and SQL injection). Thus our proposed system of firewall fingerprinting methods can achieve quite high accuracy against all web vulnerability. Thus all web applications can be made secure against web attacks.

II. STATE OF ART

The first study of SQL Injection and DDOS attack compares the prevention and detection approaches. For each vulnerability, the different attacks and the performances of each attack are described. The novel specification-based methodology for the prevention of SQL injection Attacks is proposed. The two most important advantages of this approach against existing mechanisms are 1) It prevents all forms of SQL injection attacks 2) This technique does not allow the user to access database directly in database server. "XPATH Authentication Technique" is the web application oriented technique to detect and prevent SQL Injection Attacks by generating functions of two filtration models 1) Active Guard 2)Service Detector[5]. The comparisons of different type of approaches and techniques and provided a list of the deployment requirements [6]. The filtering proxy server is used to prevent the SQL injection attack and analyses the performance impact of filtering process on web application [7]. For each technique, its strengths and weaknesses in addressing the entire range of SQL injection attacks are discussed [8].

The in-depth study of the denial of service in the Internet is provided with the survey of attacks and their countermeasure. The various DOS attack mechanisms are investigated and summarizes the challenges in DOS defence. The DOS defence, analysis of the strengths and weaknesses of different proposals are described [9].

III. PROPOSED SYSTEM

We prevents the intruder trying to access the database/application by analyzing vulnerable scripts. The denial of firewall and SQL injection attack is prevented by automatic intrusion detection (IDS) and automatic intrusion prevention system (IPS).. In our proposed system, detection and prevention techniques for Denial of firewall, SQL injection has been done.the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

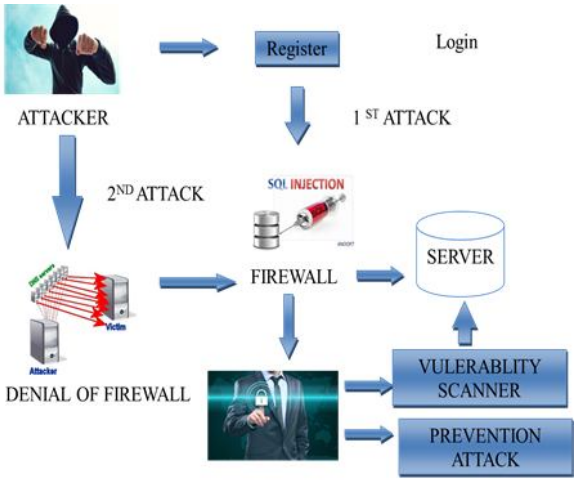

Fig1.Architechture Diagram

IV.ATTACK

There are various web-based attack types and vectors that affect every businesses, communities and individuals. The attacker find a point of entry where they can exploit(known as attack vector). These attack vectors come in a variety of forms two main categories are: Access Control and Software Vulnerabilities.

There are various attack, some of them are,

1. Remote code execution
2. SQL injection
3. DDOS attack
4. Format string vulnerabilities
5. Cross Site Scripting (XSS)
6. Username enumeration

In this paper we mainly focus on SQL injection and DDOS attack.

.

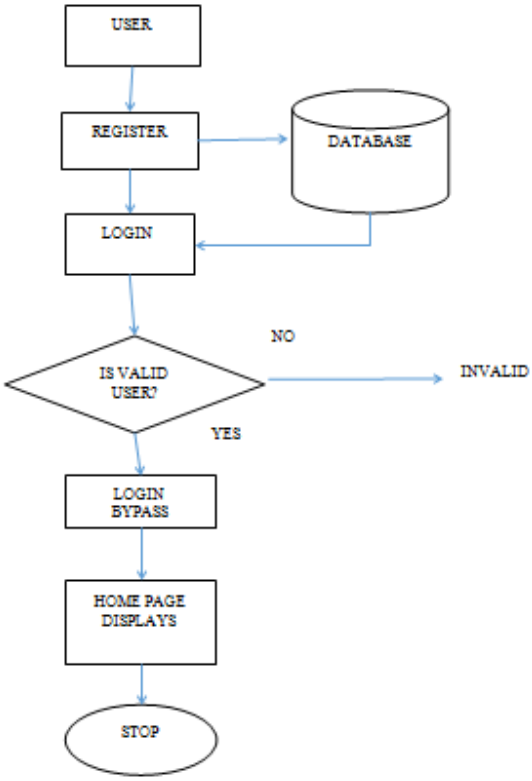

Fig 2.Data flow diagram of user login.

A.SQL injection

SQL Injection (SQLi) refers to an attack by injection of query. Where in attacker can execute malicious SQL statements (referred as malicious payload) where database of web application server is controlled (referred as Relational database management system-RDBMS).

Any website can be attacked by SQL injection. Which is most dangerous? A hacker uses this SQL injection attack on the web application by bypassing the authentication and authorization mechanisms to retrieve the entire database information. It can add, modify and delete of records in a database.

The major attacks through which the user information are retrieved are ,

1. SQL login bypass .
2. Blind injection
3. Error based attack
4. Union based attack

The sensitive information are retrieved by the hackers through unauthorized access.

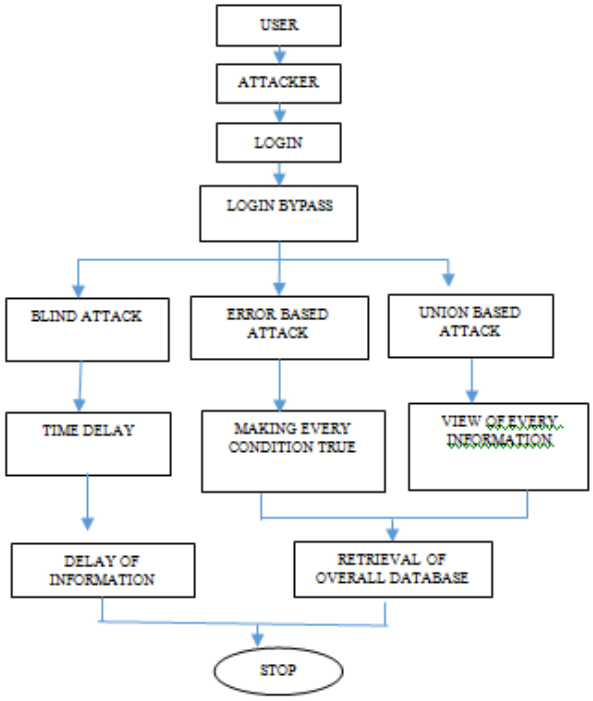

Fig 3.Data flow diagram of an attacker.

A.1SQL Login Bypass

SQL Login Bypass is the code injection technique, used to attack the web applications which contains user information, in which malicious SQL statements are inserted into an entry field for execution . SQL Login Bypass must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly interpreted and unexpectedly executed.

SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

A.2.Blind injection

Blind SQL injection occurs when no errors occur as a result of passing SQL commands, or when a generic error message is displayed as a result of passing SQL commands.

A.3.Error based attack

The error-based injection leads to the development of error generation. Where the generation of error is made in database by doing SQL injection in the query.

To enumerate the overall database the error based SQL injection is enough. During, the development phase the errors that are generated are very useful. Where they should be disabled on a live site, or logged to a file with restricted access instead.

A.4.Union based attack

Whereas, union-based SQL injection is one of the in-band SQL injection technique. Where the union based SQL injection involves the use of UNION SQL operator to combine the results of two or more SELECT statements into a one result which is a part of HTTP response.

The union based SQL injection involves in extracting the information from the database. Based on the same structure of the query the UNION based attack can be done by crafting the SELECT statements similar to the original query.

We need a table in order to undergo the following SQL injection for this there is a need to use a table name and to determine the number of columns in the first query and their data type.

B.DDOS Attack

The DDOS attack technique is that it undergoes packet flooding that originate from the client within the network. Therefore the DDOS attack makes the server to crash/slow down/malfunction. Normally, the Firewall works by filtering the outgoing packets in and out of the network.

Therefore, firewall plays an important role in a network security. During DDOS attack many number of request sent at the same time, thus making the firewall to compromise.

Finally, DDOS attack takes place. Thus the particular request is not sent to the server for processing.

V. **PREVENTION**

The prevention for the SQL injection is data sanitization and validation. Sanitization involves in running any submitted data through a function (such as MySQL's mysql_real_escape_string () function) and to ensure that any dangerous characters (like " ' ") are not passed to a SQL query in data.

Validation is different from sanitization, where it ensures whether the data submitted is in the expected form. whereas at the most basic level this includes ensuring that e-mail addresses contain an "@" sign, that only digits are supplied when integer data is expected, and that the length of the data submitted is not longer than the maximum expected length.

Validation is carried out in two ways: by blacklisting dangerous or unwanted characters (although hackers can often get around blacklists) and by white listing only those characters that are allowed in a given circumstance, which involves more work on the part of the programmer.

Although validation may even take place on the client side, hackers can modify or get data. so, it's essential to validate all data on the server side as well.

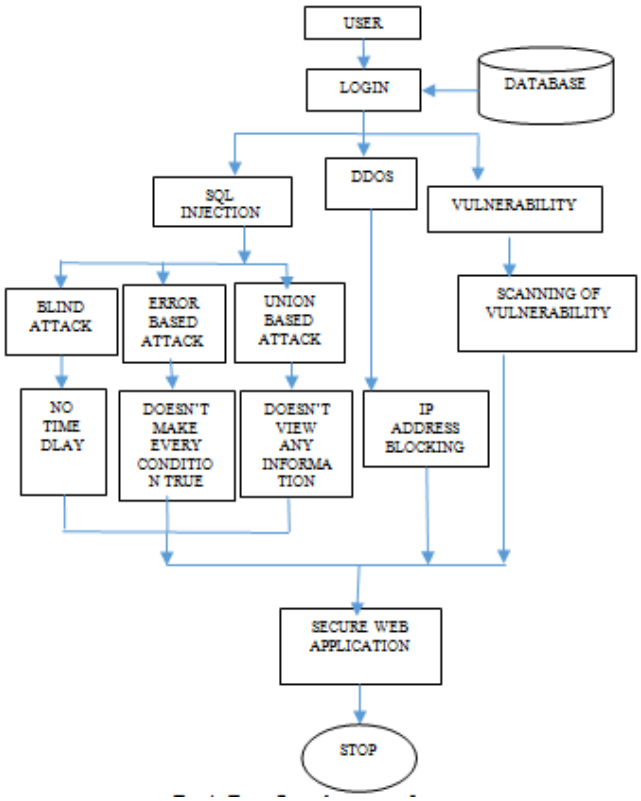

Fig 4: Data flow diagram of prevention.

A.PREPARED STATEMENTS

A prepared statement undergoes the execution of the same (or similar) SQL statements repeatedly with high efficiency. The prepared statements advantage is that it reduces the parsing time in preparation of the query .where it is done only once.(although the statement is executed multiple times as much as possible).

A.1 ALGORITHM

PREPARED STATEMENT REPLACEMENT:

INPUT: Source code

.

Step 1: Analyze the source code and generate the specific recommended code structure containing prepared statements.

Step 2: Separate the SQL statement's input from the SQL structure in the generated code structure.

Step 3: Create an additional string object for each string object used to create the SQL statement.

Step 4: The new string object is created with the raw string data and the identifiers found in the original string object.

Step 5: An assistant vector is created for each new string object and it contains SQL input found in the original string object.

Step 6: The assistant vector tree changes dynamically at runtime and ensures that the SQL input elements are in the proper order.

Step 7: The generated code is inserted and that loops through the vector.

Step 8: The generated code then executes the prepared statement and replaces the SQLIV execution.

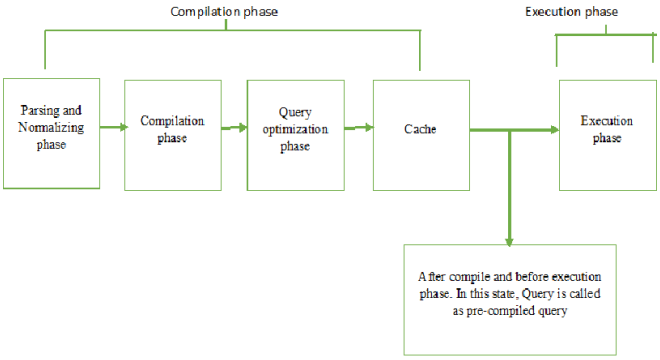

Fig 5: Diagrammatical process of PSR

B.VULNERABILITY SCANNER

Scans the given URL according to Anti-malware engines in Explore module, are to be called, in which URL has filtered and, finds the vulnerable links if available in those pages. This open source scanner identifies vulnerable scripts of Cross site request forgery and SQL injection attacks. Hence this would be a web based security testing tool for the developers.

C.DEEPPACKET INSPECTION (DPI)

Deep pack inspection undergoes the examination of packet contents passing through the given checkpoint. where it makes the decision in real-time based on rules assigned by an enterprise, internet service provider(ISP) network manager, depending on packet contains. Previous forms of packet filtering looks only the header information. Till now, firewalls did not have the processing power necessary to perform deeper inspections on larger traffic. Technological uses the DPI to perform more advanced inspections.

D.IP ADDRESS BLOCKING

IP address blocking prevents the connection between a server or website. Where certain IP address or range of IP address is blocked by this IP address blocking method. Where the IP address blocking effectively bans undesired connections from hosts using the information such as the affected addresses to a website, mail server, or other Internet server.

IP address blocking is commonly used to protect against attack. Normally, it prevents the brute force attacks. By blocking the IP address from the client side. Then that IP users can't access the original page of the server. So we stop the DDOS attack happened.

VI. EXPERIMENTAL RESULTS

The Experimental results for the proposed are deployed. The experimental results include both the SQL injection and DDOS attack prevention results. We would first examine SQL injection results.

A.SQL INJECTION EXPERIMENTAL RESULTS

The SQL injection experimental results include both the prevention accuracy table and execution time comparison for proposed technique.

Table 1:SQLi's Prevention Accuracy

SQL INJECTION ATTACK TYPES	UNPROTECTED DATA	PROTECETED DATA
Login By Pass	Not Prevented	Prevented
Union based Attack	Not Prevented	Prevented
Error based Attack	Not Prevented	Prevented
Blind Attack	Not Prevented	Prevented

The table 1 determines the prevention accuracy for the various SQL injection attack types for protected and unprotected data's.

Table 2: Execution Time comparison for proposed technique

Number of queries in a database	Execution time in milliseconds	
	Existing System	Proposed System
100	460	90
200	540	126
300	600	148
400	680	173
500	720	240
600	900	360

The Table 2 describes the execution time comparison among the existing and proposed technique for various number of input queries.

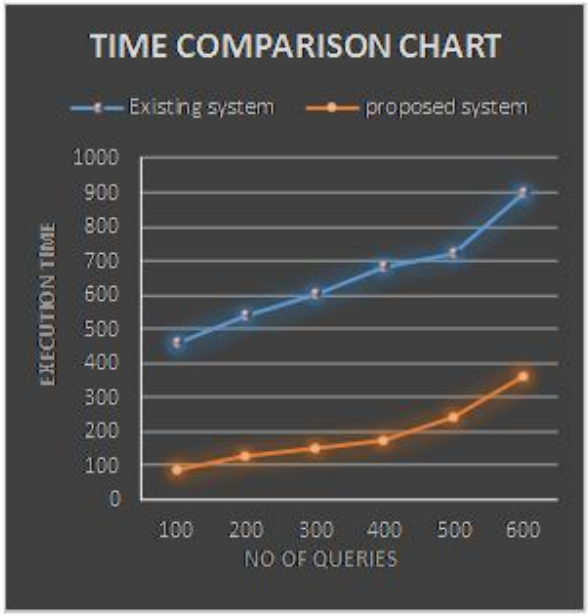

Fig 6:Time comparison chart among existing and proposed

The above give chart illustrate the execution time taken for the proposed technique with the existing technique.

A.DDOS ATTACK EXPERIMENTAL RESULTS

The DDOS attack experimental results include both the prevention accuracy table and execution time comparison for proposed technique.

Table 1: Prevention Time comparison for proposed technique

Firewall	Number of request to the server	Prevention time in milliseconds	
		Existing System	Proposed System
System firewall	50	450	120
	100	800	180
	150	960	320
	200	1050	450
	250	1200	520
	300	1600	600

The Table 1 describes the Prevention time comparison among the existing and proposed technique for various number of request to the server.

Fig 7:Time comparison chart among existing and proposed.

The above give chart illustrate the execution time taken for the proposed technique with the existing technique.

VII.CONCLUSION AND FUTURE WORK

The impact of DDOS attack inside the network is drastically reduced by Reverse Firewall technique. It also chokes off packet flooding attacks before they exit the network where they are originated. Prepared statements prevents from SQL injection and IP Address blocking prevents from DDOS attack. Integrating automatic prevention technique for Denial of firewall, SQL injection, DPI and web

vulnerability scanner provides 99.9% security and accuracy for all web applications against intruders.

It is easier for infrastructure providers of larger network and are more beneficial for them to incorporate these additional features within their network infrastructure in order to protect themselves from inside and the outside attack.

Therefore provides security on both outside and inside network with reverse firewall techniques and high level security is provided.

REFERENCES

[1] Amir R.Khakpour Alex X.Liu Joshua W.HulstZihuiGeDanPeiJiaWang,"Firewall Fingerprinting and Denial of Firewalling Attacks"
[2] Dan Goodin,"Hacker pierces hardware firewalls with webpage",http://www.theregister.co.uk/2010/01/06/webbased firewall attack/, 2010.
[3] "Cisco Firewall Services Module DoS vulnerability",http://www.net-security.org/secworld.php?id=10673, 2011.
[4] Fyodor, "Nmap: Free network security scanner", http://nmap.org.
[5] IndraniBalasundaram, Dr. E. Ramaraj, "An Approach to Detect and Prevent SQL Injection Attacks in Database Using Web Service" IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.1, January 2011.
[6] Sayyed Mohammad SadeghSajjadi and BahareTajalli Pour," Study of SQL Injection Attacks and Countermeasures".International Journal of Computer and Communication Engineering, Vol. 2, No. 5, September 2013.
[7] Elshazly, K., Fouad, Y., Saleh, M. and Sewisy, A. (2014) "A Survey of SQL Injection Attack Detection AndPrevention".Journal of Computer and Communications, 2014, 2, 1-9.Published Online June 2014 in SciRes.
[8] William G.J. Halfond, Jeremy Viegas, and Alessandro Orso "A Classification of SQL Injection Attacks and Countermeasures"College of Computing,Georgia Institute of Technology.
[9] MEHMUD ABLIZ ,"Internet Denial of Service Attacks and DefenseMechanisms".
[10] Stephen Thomas,Laurie Williams, Tao Xie, "On automated prepared statement generation to remove SQL injectionVulnerabilities".