ISSN (Online): 2456-0448
International Journal of Innovative Research in Management, Engineering and Technology
Vol. 3, Issue 3, March 2018

Development Of Scanning Mechanism For User Developed Applications From Vulnerabilities

[1] T.Nivetha (M.E), [2] Dr.G.Srinivasan M.E Phd
[1] Department of Cse MNM Jain Engineering College, Chennai, India
[2] Assistant. Professor of Cse Department MNM Jain Engineering College Chennai, India

Abstract: ***The 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. The 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). The proposed system of firewall fingerprinting methods can achieve quite high accuracy against all web vulnerability. All web applications can be made secure against web attacks. Firewalls are most important and critical devices which provide securities against all vulnerabilities. Firewall handles all the traffic in and out of the network. Hackers / intruders exploit the firewall using malicious scripts and access the server / applications. Analyze Denial of Firewalling and SQL injection attacks are discussed. Denial of Firewalling is attacker overloads the firewall and SQL injection is bypassing the security protocol by malicious scripts.***
Firewalls are most important and critical devices which provide securities against all vulnerabilities. Firewall handles all the traffic in and out of the network. Hackers / intruders exploit the firewall using malicious scripts and access the server / applications. Analyze Denial of Firewalling and SQL injection attacks are discussed. Denial of Firewalling is attacker overloads the firewall and SQL injection is bypassing the security protocol by malicious scripts.

Keywords: ***SQL injection, CSRF, Firewalls, Security Protocol, Vulnerabilities, Intruder.***

I. INTRODUCTION

Network security is the security provided to a network from unauthorized access and risks. It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats. Network security starts with Authentication, commonly with a username and a password. Since this requires just one detail authenticating the user name—i.e., the password—this is sometimes termed one-factor authentication. With two-factor Authentication, something the user 'has' is also used (e.g., a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' is also used (e.g., a finger print or retinal scan). Communication between two hosts using a network may be encrypted to maintain privacy. The computer network technology is developing rapidly, and the development of internet technology is more quickly, people more aware of the importance of the network security. Network security is main issue of computing because many types of attacks are increasing day by day. In mobile ad-hoc network the nodes are independent. Protecting computer and network security are critical issues. The malicious nodes create a problem in the network. This malicious nodes acts as selfishness, It can use the resources of other nodes and preserve the resources of its own.

II. RELATED METHODS

A. SQL Injection is a method where the intruder injects a contribution to the SQL Query with a specific end and goal to change the structure of the Query proposed by the programmer and picking up the access of the database which results modification or deletion of the client's information. In the injection it misuses a security weakness (vulnerability) happening in database layer of an application. SQL injection attack is the most well-known attack in web based sites and application nowadays. Some malicious codes get inject to the database by unapproved clients and get the entrance of the database due to absence of information approval. Information validation is the most critical portion o f programming security that is not appropriately secured in the outline period of programming advancement life-cycle bringing about numerous security vulnerabilities. This proposed technique displays the procedures for identification and avoidance of SQL injection attacks. There are no any known full verification protections accessible against such sort of assaults. In this paper some predefined strategy for identification and the some current systems of preventions are examined. In here we use the 448 bit Blowfish along with the some security algorithms to enhance the existing model, to prevent the SQL Injection attacks. In

Existing model we use RC4 and Normal Blowfish to Encrypt and secure the web data from the SQL Injection attack but now we enhance using the 448 bit Blowfish Encryption technique with less execution overhead.

B. In this Internet age, web applications have become an integral part of our lives, but security and privacy of our sensitive data has become a big concern. Over last several years, SQL Injection has been the most prevalent form of attack on web databases. Much research has been done in this area, but most of the approaches in the literature have high computational overhead or difficult to deploy in practical scenarios. In this paper we have proposed a lightweight approach to prevent SQL Injection attacks by a novel query transformation scheme and hashing. We implemented it on a prototype e-commerce application and the results of our experiments show that it can successfully and efficiently block a variety of SQL Injection attempts.

C. SQL Injection Prevention Using Tokenization: A model exclusive of tokenization technique is used to prevent SQL Injection Attack by blocking the malicious input query in query execution phase. SQL Injection Prevention Using Tokenization Model detects SQLIA by applying tokenization process on input query. Tokenization process is applied by detecting spaces, single quotes and double dashes etc. This process converts the input query into the fruitful tokens and these tokens are then converted into hierarchical form. After applying tokenization, model validates each token by analyzing the value of left and right child of individual token. As soon as SQLIA detected it permanently block the input query. This model is seems to be able to detect and prevent all types of SQL Injection Attacks and does not trap in the case of appending set operators and Additional query attacks. It increases database security as well as contributes to maintain the confidentiality of sensitive data of web applications.

D. SQL injection is a technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed.SQL injection is a trick to SQL query or command as an input possibly via the web pages. They occur when data provided by user is not properly validates and is included directly in a SQL query. By leveraging these vulnerabilities, an attacker can submit SQL commands directly access to the database. In this paper we present all SQL injection attack types and also different technique and tools which can detect or prevent these attacks .Finally we assessed addressing all SQL injection attacks type among current technique and tools.

E. Along with the increasing growth of computer networks, security threats multiply and accordingly improving and enhancing the network security devices and methods become necessity. Firewalls as the first line of defense have irrefutable importance in securing a network; therefore improvement in this technology ensures higher level of security in computer networks. Any improvement or novel ideas are not achieved unless a deep analysis of the existing methods and current needs takes place. In this paper the vulnerabilities of firewalls according to their natures and also various types of firewalls are classified in order to create a better perspective for future research. Also some of the current approaches to mitigate these vulnerabilities are mentioned and firewall fingerprinting as a technique which makes attackers able to obtain more precise information about firewalls` vulnerabilities in order to exploit them is presented.

F. Off-path packet injection attacks are still serious threats to the Internet and network security. In recent years, a number of studies have discovered new variations of packet injection attacks, targeting critical protocols such as TCP. We argue that such recurring problems need a systematic solution. In this paper, we design and implement Packet Guardian, a precise static taint analysis tool that comprehensively checks the packet handling logic of various network protocol implementations. The analysis operates in two steps. First, it identifies the critical paths and constraints that lead to accepting an incoming packet. If paths with weak constraints exist, vulnerability may be revealed immediately. Otherwise, based on "secret" protocol states in the constraints, a subsequent analysis is performed to check whether such states can be leaked to an attacker.

G. In this paper, we present a detailed review on various types of SQL injection attacks, vulnerabilities, and prevention techniques. Alongside presenting our findings from the survey, we also note down future expectations and possible development of countermeasures against SQL injection attacks.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 3, March 2018

III. PROPOSED SYSTEM

- The proposed system focus on automatic intrusion detection (IDS) and
- Automatic intrusion prevention system (IPS) for denial of firewall and SQL injection attacks.

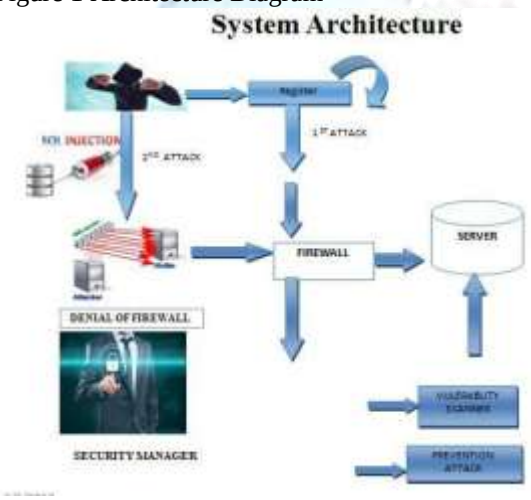
The proposed system, describes detection and prevention techniques for Denial of firewall, SQL injection queries, Blind SQL injection, Cross site request forgery attacks.

- SQL Injection: The tokenization process is applied on the input query by detecting spaces, single quotes and double dashes etc.
- To prevent DDOS attack The Firewall works by filtering the outgoing packets from a network and does a deep packet inspection (DPI). If any malicious entity is been identified the respective request is been blocked and the respective IP is blocked.
- The proposed system provides alert SQL injection, Cross site scripting attack.

A. Arichitecture

This paper describes detection and prevention techniques for Denial of firewall, SQL injection queries, Blind SQL injection, Cross site request forgery attacks. The overall Architecture of the proposed work is presented in Figure 1.

Figure 1 Architecture Diagram



B. Standard Sql Injection Attack

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection 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 typed 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.

C. Blind Sql Injection

In this module, we propose with the blind, timing- based SQLi, it's still possible to exhilarate data. This is because you're retrieving data one character at a time by asking Boolean questions about each character. Example: If the first letter of the first table name is between A and L, pause X seconds before responding back to me. Boolean blind SQLi is the same way but faster since you're looking at response content rather than response timing to read out of the db.

D. Denial Of Firewall.

Denial of firewall is where attackers use carefully crafted traffic to effectively overload a firewall. Another method of overloading is that making all virtual machines send dummy packets with no payload to the target firewall as the background traffic.

E. Deep Packet Inspection.

In this module automatic Intrusion detection system (IDS), encryption, deep packet inspection (DPI) and report the results to the controller. The main goal of this module is to allow network operators to describe security policies for specific flows. The policies include a description of the flow, a list of security services that apply to the flow and how to react in case malicious content is found. The reaction can be to alert only, or to quarantine traffic or even block all packets from a specific source.

F. Blocking Ip Address

In this paper, we propose **IP address blocking** prevents the connection between a server or website and certain IP addresses or ranges of addresses. IP address blocking effectively bans undesired connections from hosts using affected addresses to a website, mail server, or other Internet server.
IP address blocking prevents the connection between a server or website and certain IP addresses or ranges of addresses. IP address blocking effectively bans undesired connections from hosts using affected addresses to a website, mail server, or other Internet server. IP address blocking is commonly used to protect against brute force attacks.
Here we are blocking the request if more than 7 continuous request from the client side to server then that IP users can't access the original page of the server. So we stop the DDOS attack happened.

*G. 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 test tool for the developers.

IV. RESULT AND DISCUSSION

In this paper, the result is proposed by providing alert for SQL injection, Cross site scripting attack. Provide prevention techniques from DDOS attack. Integrating automatic prevention technique for **Denial of firewall, SQLinjection, DPI and web vulnerability scanner** provides 99.9% security and accuracy for all web application against intruders.

Figure 2 SQL Injection Attacks

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 3, March 2018

SQL Injection attack is visually shown by injective malicious query **or '1'='1** in the login page.

Figure 3 SQL Injection Attacks 2**.**

SQL Injection attack is visually shown by injective malicious query **or 'a'<'b** in the login page.

Figure 4 SQL Blind Attacks And Result

SQL Blind attack is visually shown by injective malicious query **or '1'='1** in the login page.

Figure 6 DDOS Attack

DOS attack is shown by sending continuous request to the server**.**

Thus our proposed system provide alert of SQL injection, Cross site scripting attack and Provide prevention techniques from DDOS attack.

It emerged for integrating automatic prevention technique for **Denial of firewall, SQLinjection, DPI and web vulnerability scanner** provides 99.9% security and accuracy for all web applications against intruders.

CONCLUSION

The proposed system is extensive in the execution of its detection mechanism against web application vulnerabilities. Testing of web applications for weaknesses is a significant step in safeguarding web applications. the proposed shows how attackers will attack our database through web applications. And also the proposed system scans only the URL of the applications and detect it will be affect or not. If users use the scanning mechanism will safe from vulnerabilities.

References

[1] Avireddy. S, Perumal.V, Gowraj.N,Kannan R.S, Thinakaran.P, Ganapthi .S, Gunasekaran J.R, Prabhu.S, Random4: An Application Specific Randomized Encryption Algorithm to prevent SQL injection, ieee transactions on communications, vol. 60, no. 5, may 2012.

[2] Debabrata Kar, Suvasini Panigrahi, Prevention of SQL Injection Attack Using Query Transformation and Hashing, IEEE International Advance Computing Conference (IACC), 2013.

[3] Gaurav Shrivastava, Kshitij Pathak, SQL Injection Prevention using Tokenization: Technique and Prevention Mechanism, IJARCSSE, Volume 3, Issue 6, June 2013.

[4] V.Nithya,R.Regan,J.vijayaraghavan.,"A Survey on SQL Injection attacks, their Detection and Prevention Techniques". International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 4 Page No. 886-905. April, 2013.

[5] "Cisco Firewall Services module DOS Vulnerability",http://www.netsecurity.org/secworld.php?id =10673, 2011.

[6] Zhiyun Qian and Z. Morley Mao, "Off-path tcp sequence number inference attack - how firewall middleboxes reduce security", in Proceedings of the IEEE Symposium on Security and Privacy, Oakland, California, May 2012, pp. 347 – 361.

[7] Diallo Abdoulaye Kindy and Al-Sakib Khan Pathan" "A Survey on SQL Injection: Vulnerabilities, Attacks, and Techniques" IEEE 15th International Symposium on Consumer Electronics, 2011.