ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 4, June 2012

# Tool to Detect and Prevent Web Attacks

**Nilesh Khochare**
*nileshkhochare@gmail.com*
Computer Department
VJTI, Mumbai

**Dr.B.B.Meshram**
*bbmeshram@vjti.org.in*
Computer Department
VJTI, Mumbai

***Abstract*— A Web Application Firewall (WAF) is a security tool that protects the web application and web application server from various attacks. Application protection is a valuable security layer to add because it can protect against a number of application layer security threats which is usually not protected by a typical network layer intrusion detection system. The Web Application can easily be attacked by the hackers even though with the existence of the normal firewall in the system. This is due to the limitation that the normal firewall does not work in the application layer. The hackers will attack the Web Application using the methods like structured Query Language (SQL) Injection, Cross Site Scripting (XSS), Command Injection, or Session Manipulation, cookie poisoning, Directory traversal, Forceful browsing. This paper addresses these problems by presenting a methodology for the automatic detection of vulnerabilities in web application and preventing web application from various attacks. The proposed methodology, implemented in this paper monitors all the incoming and outgoing data in the web application and blocks web related attacks like SQL injection attacks, Cross Site Scripting attacks, Buffer Overflow attacks, Cookie poisoning ,Forceful browsing and Directory traversal attacks.**

***Index Terms*—Application Firewall, SQL injection, Cross Site Scripting, WAF.**

## I. INTRODUCTION

Today applications are becoming the prime target for cyber attacks. A recent research showed that approximately 80% of all successful web attacks exploit application vulnerabilities and there is no shortage of vulnerabilities to go after, all of them require some skill to exploit. The traditional firewalls block packets effectively at the network layer; they are ineffective against attacks which point to application weaknesses. Web application firewalls detect application vulnerabilities and whether sensitive data, such as account information or credit card number, is being hacked and can take suitable action accordingly. [2]

Various web applications such as online branch of a bank, an online-shop, a customer, partner, or employee portal, all are available to their customers as well as to their attackers around the clock due to the *always on* nature of the internet. Attacks such as SQL injection, cross-site scripting or session hijacking and many more are aimed at vulnerabilities in the web applications itself. Web application firewalls are specialized tools whose purpose is to increase security in web applications. Figure 1 show the basic working of the web application firewall, where only normal user can access the web application or web server and access is denied for an attacker. [18]

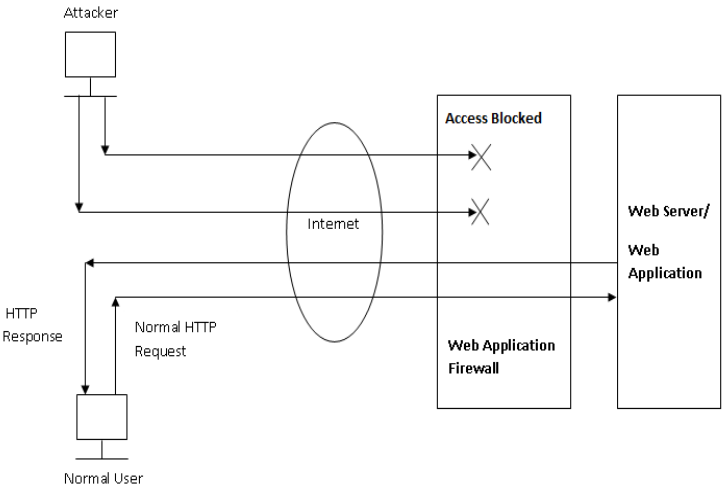


Fig 1. Basic working of Application Firewall

Application firewall is a set of application-specific policies that gives you granular control over network traffic on the level of users. The primary functionality of this application-layer tool is to regulate Web browsing, file transfer, email, and email attachments. Using application firewall, you can restrict transfer of certain file names, file types, email attachments, attachment types, email with certain subjects, and email or attachments with certain keywords or byte patterns. You can deny internal or external network access based on various criteria.

## II. RELATED WORK

This paper describes a methodology and a tool for the detecting and preventing attacks on web application. Now we describe various approaches to securing Web applications from web-based attacks.

### *A. Open source Tools*

IronBee is an open source tool designed by Qualys. IronBee implements a robust framework for application security monitoring and defense. It provides a layered set of features at different levels of abstraction, enabling its users to choose the approach that works best for the work they need to accomplish. It provides security from DoS and DDoS attacks, Cookie related attacks, Brute Force attacks, SQL injection attacks and cross site scripting attacks. [11]

AQTRONIX WebKnight is an application firewall for IIS and other web servers and is released under the GNU General Public License. WebKnight scans all requests and processing them based on filter rules, set by the administrator. These rules are not based on a database of attack signatures that require regular updates. WebKnight filters buffer overflow,

SQL injection, and directory traversal, character encoding and other attacks. [17]

Guardian@JUMPERZ.NET is an open source application layer firewall for HTTP/HTTPS. It works as a reverse proxy server. It analyzes all HTTP/HTTPS traffic against rule-based signatures and protects web servers and web applications from attack. When unauthorized activity is detected, Guardian@JUMPERZ.NET can disconnect the TCP connection before the malicious requests reach the web server.[18]

ModSecurity is an application firewall which makes copies of the data, place it into memory and then apply all data transformations, etc, and it would then decide what disruptive action to take if there was a rule match on the data. While this process works well in defense of the vast majority of web application security issues, there are still certain situations where it is limited. Client-side security issues are difficult to address in this architecture since the WAF has no visibility on the client. [19]

### *B. Commercial Tools*

Barracuda Web Application Firewall protects Web sites and Web applications from attackers leveraging protocol or application vulnerabilities to instigate data theft, denial of service, or defacement of an organization's Web site. Unlike traditional network firewalls or intrusion detection systems that simply pass HTTP, HTTPS, or FTP traffic for Web applications, the Barracuda Web Application Firewall proxies this traffic and inspects it for attacks to insulate Web servers from direct access by hackers. [10]

Imperva Secure Sphere Web Application Firewall protects applications from current and future security threats by combining multiple security engines into a cohesive Web defense. Imperva Secure Sphere provides ironclad protection against the OWASP Top Ten attacks, including SQL Injection, Cross Site Scripting and Cross Site Request Forgery. [16]

The Citrix Application Firewall protects web servers and web sites from misuse by hackers and malware, such as viruses and Trojans, by filtering traffic between each protected web server and users that connect to any web site on that web server. The Application Firewall examines all traffic for evidence of attacks on web server security or misuse of web server resources, and takes the appropriate action to prevent these attacks from succeeding. [9]

FortiWeb web application firewall provides specialized, layered application threat protection. FortiWeb integrated web application and XML firewalls protect your web-based applications and internet from various attack and data loss. FortiWeb helps you prevent identity theft, financial fraud, SQL injection, cross site scripting. [14]

## III. THE PROPOSED APPROACH AND TOOL

### *A. Proposed Architecture of Firewall*

The proposed approach to prevent web applications and web servers consist of various modules which is shown in figure 2 and aimed at (i) Monitoring the incoming and outgoing request of web application (ii) Matching all the request and response with the firewall rules, policies and the attack definitions present in database (iii) Block the malicious request or response (iv) Alert the user regarding detected attack.

Module I – **User Interface Module**

This module provides robust user interface through with user can interact with the Application Firewall tool. Through this module user can set or change the policies of the firewall.

Module II – **Database Module**

This module provides the database which stores the patterns and signatures of various attacks which is useful in detection and prevention of the attacks.

Module III – **Detection Module**

Detection module implement the algorithm to detect the SQL injection attacks, Cross Site Scripting attacks, Buffer Overflow attacks, Cookie poisoning ,Forceful browsing and Directory traversal attacks.

Module IV – **Prevention Module**

Prevention module implement algorithm to prevent the SQL injection attacks, Cross Site Scripting attacks, Buffer Overflow attacks, Cookie poisoning, Forceful browsing and Directory traversal attacks.

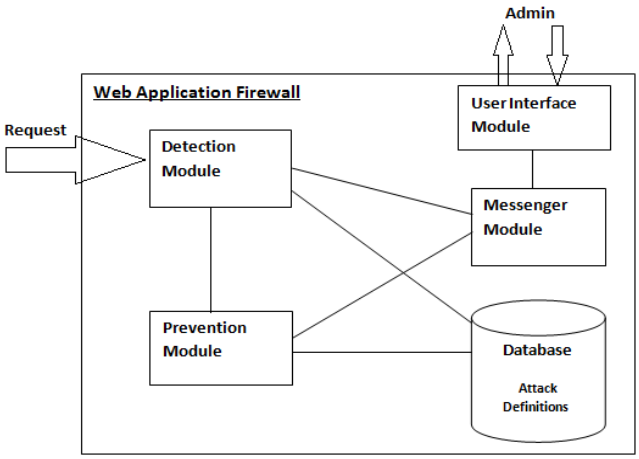


Fig 2.proposed Architecture of Application firewall

Module V- **Messenger Module**

Messenger module provides warning messages and alert messages to user time to time

### *B. Proposed Working of Application Firewall*

The proposed Application Firewall is a filter which sits between web applications and users, examining requests and responses and blocking dangerous or inappropriate traffic. This tool protects web servers and web sites from unauthorized access and misuse by hackers and malicious programs, such as viruses and trojans (or malware). To secure our web application and web servers, application firewall must be installed in a location where it can intercept traffic between the web servers and web application you want to protect and network devices through which users access those web servers. You then configure the network to send requests to the Application Firewall instead of directly to your web servers, and responses to the Application Firewall instead of directly to your users as shown in figure 3. Then application firewall filters the traffic before forwarding it to

its final destination and examines each request and response using its rule set.

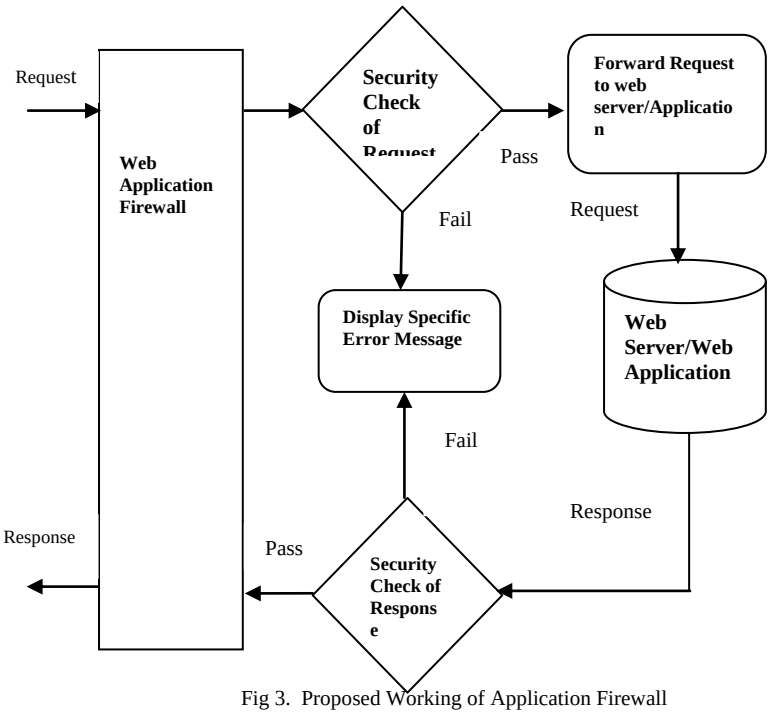


Fig 3. Proposed Working of Application Firewall

As the Figure 3 shows, when a user requests a URL on a web server, the application firewall first examines the request in "Security Check of Request". These rules check for various types of attacks on the web servers. Application Firewall also checks to see if the request needs further filtering. If the request passes the Application Firewall security checks, it is passed to the Web Server. The web site or web service sends its response back to the Application Firewall, which examines the response in "Security Check of Response". If the response does not violate any security checks, the Application Firewall forwards the response to the user. This process is repeated for each request and response.

## IV. COMPARISON WITH OTHER TOOLS

TABLE I
COMPARISON WITH OTHER TOOLS

| Sr. No. | Name of Tool | Type | Features and prevented attacks |
|---|---|---|---|
| 1 | Iron Bee | Open Source | • Dos, DDoS attack<br>• Cookie attacks<br>• Brute force attack<br>• SQL injection<br>• Cross Site Scripting<br>• Information leakage<br>• Error message detection<br>• Behavioral monitoring |
| 2 | AQTRONIX WebKnight | Open Source | • Buffer Overflow<br>• SQL injection<br>• Directory Traversal |
| 3 | Guardian @JUMPER Z.NET | Open Source | • Rule based signature detection<br>• SQL injection<br>• Cross Site Scripting |
| 4. | ModSecurity | Open Source | • SQL injection<br>• Cross Site Scripting<br>• Cookie attacks |
| 5. | Barracuda | Commercial | • DoS attacks<br>• Information Leakage<br>• OWASP Top Ten attacks<br>• Data theft protection<br>• Brute Force Protection<br>• SQL injection<br>• Cross Site Scripting<br>• Cookie and form tampering |
| 6. | Imperva Secure Sphere | Commercial | • SQL Injection<br>• Cross site scripting<br>• Cross Site Request Forgery<br>• OWASP Top Ten attacks[20] |
| 7. | Citrix | Commercial | • Buffer Overflow<br>• Cookie Poisoning<br>• XML related attacks<br>• SQL injection<br>• Cross Site Scripting<br>• Credit card theft |
| 8. | FortiWeb | Commercial | • SQL injection<br>• Cross site scripting<br>• Financial fraud protection<br>• Prevent Identity Theft<br>• XML related threats<br>• Cross Site Request Forgery<br>• Information Leak |
| 9 | Proposed Tool | Open Source | • SQL injection<br>• Cross Site Scripting<br>• Cross site Request |

| | | | |
|---|---|---|---|
| | | | Forgery<br>• Information leakage<br>• Data theft Protection<br>• Buffer Overflow<br>• Incorrect Input Handling<br>• Cookie Poisoning<br>• Error handling problems<br>• DoS, DDoS<br>• Forceful Browsing<br>• Directory Traversal<br>• XML related attacks<br>• Session hijacking<br>• OWASP Top Ten attacks<br>• Robust GUI |

Table 1 shows the comparison of the present tools with the proposed tool. The tool presented in this paper is able to prevent more number of attacks because it combines all the attack prevention methods from present tool and it is very easy to use as it provides Robust GUI.

## V. Conclusion and Future Work

The spectra of online identity threat was never so real as it is today, primarily due to rapid growth of the internet and increase in web application which offer a cost effective method to service providers such as banks, retailers etc., to reach their customers. This has also provided the hacking community an excellent tool to try and fool the organizations and peoples. There are many popular attack techniques on Web applications such as SQL injection, Cross Site Scripting, Brute Force Attack, Cross Site Request Forgery, Session Hijacking, Buffer Overflow etc. Web Application Firewall gives huge benefits to network security as it is uncomplicated and considered as one of the effective tool to prevent the attacks at the application layer. This paper proposes an Application Firewall tool to protect web application from hackers. This tool analyzes the incoming request towards the web application and outgoing response from web application or web server. The business logic module of this tool maintains all the database of attacks, rules and policies for detection and prevention of the attack. This tool prevent web application from SQL injection attacks, Cross Site Scripting attacks, Buffer Overflow attacks, Cookie poisoning ,Forceful browsing and Directory traversal attacks.

Work in progress aims at (i) Further validating this tool and comparing the result with other open source and commercial tools and (ii) improving this tool by adding anomaly detection module.

## REFERENCES

[1] Chong Hee Kim and Jean-Jacques Quisquater, "FAULTS, INJECTION METHODS, AND FAULT ATTACKS", Journal IEEE Design & Test archive Volume 24 Issue 6, November 2007.
[2] Hironao Takahashi, hafiz farooq Ahmad, Kinji Mori ,"Application for Autonomous decentralized multi layer cache system to web application firewall", 2011 Tenth International Symposium on Autonomous Decentralized Systems.
[3] MichaelMeike , Johannes Sametinger and Andreas Wiesauer, "Security in Open Source Web Content Management Systems", Journal IEEE Security and Privacy archive Volume 7 Issue 4, July 2009
[4] HORSTEN HOLZ, SIMON MARECHAL, FRÉDÉRIC RAYNAL, "New Threats and Attacks on the World Wide Web, Journal IEEE Security and Privacy archive Volume 4 Issue 2, March 2006
[5] Elizabeth Fong and Vadim Okun,"Web Application Scanners: Definitions and Functions" Proceedings of the 40th Hawaii International Conference on System Sciences – 2007
[6] Angelo Ciampa,Corrado Aaron Visaggio,Massimiliano Di Penta ,"A heuristic-based approach for detecting SQL-injection vulnerabilities in Web applications", Proceeding SESS '10 Proceedings of the 2010 ICSE Workshop on Software Engineering for Secure Systems
[7] Frank S. Rietta,"Application Layer Intrusion Detection for SQL Injection ",Proceeding ACM-SE 44 Proceedings of the 44th annual Southeast regional conference
[8] Ryan Riley,Xuxian Jiang,and Dongyan Xu, "An Architectural Approach to Preventing Code Injection Attacks", Proceeding DSN '07 Proceedings of the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks
[9] Citrix Applicaton Firewall www.citrix.com/appfirewal
[10] Barracuda Application Firewall http://www.barracudanetworks.com/ns/products/web-site-firewall-overview.php
[11] IronBee - Open Source Web Application Firewall. https://www.ironbee.com/
[12] Profence Application Firewall http://www.armorlogic.com/web-application-firewall.html
[13] ThreatSentry Application Firewall http://www.privacyware.com/intrusion_prevention.html
[14] Fortiweb Application Firewall http://www.fortinet.com/products/fortiweb/index.html
[15] OWASP,WebScarab http://www.owasp.org/software/webscarab/
[16] Imperva Web Application Firewall www.imperva.com/
[17] AQTRONIX WebKnight Application firewall http://www.aqtronix.com/?PageID=99
[18] Guardian@JUMPERZ.NET - Open Source Web Application http://guardian.jumperz.net/index.html
[19] Modsecurity Web application firewall. www.modsecurity.org/
[20] OWASP Top Ten attacks. https://www.owasp.org