# Analytical study of open source WAF for web application protection

Chokhawala Kirit I.[1], Dr. Vinit Kumar Chaubey[2], Dr. A. R. Patel[3]

[1] *Research Scholar, Mewar University, Chittorgarh, Rajasthan, India*

**ABSTRACT**

*Application protection is a valuable security layer to protect against a number of application layer security threats which is usually not protected by a typical network layer intrusion detection system. The hackers will attack the Web Application using the methods like SQL injection attacks, Cross Site Scripting attacks, Buffer Overflow attacks, Cookie poisoning ,Forceful browsing, Directory traversal attacks and some known and unknown attacks. This paper describe the an analytical study of open source web application firewall for web application protection and also present comparative study of existing open source web application firewall to protect web application form various web attacks like SQL injection attacks, Cross Site Scripting attacks, Buffer Overflow attacks, Cookie poisoning ,Forceful browsing, Directory traversal attacks and some known and unknown attacks.*

**Keywords**- *Web application, open source web application firewall, and web attacks.*

## 1. INTRODUCTION

The aim of this work is to study of Web Application Firewall that can help securing a web application. A Web Application firewall is an important building block in the network. It is a form of firewall which controls access to an service or application. It operates by monitoring and potentially blocking the input, output, or system service calls i.e. in simple words traffic, which do not meet the policy of the firewall. The application firewall is typically built to control all network traffic on any OSI layer up to the application layer. It is able to control applications or services specifically, unlike a stateful network firewall which is in general unable to control network traffic regarding a specific application without additional software.

Nowadays web applications have become ubiquitous. As the number of web applications increases the amount of traffic on the internet is also growing up. This results in the increasing threat of web applications being attacked. They continue to be a prime vector of attack for criminals, and this trend shows no sign of abating; attackers increasingly launch attacks like cross-site scripting, SQL injection and many other techniques aimed at the application layer. Web application vulnerabilities can have many things including poor input validation, insecure session management, improperly configured system settings and flaws in operating systems and web server software.

Certainly writing secure code is the most effective method for minimizing web application vulnerabilities. However, writing secure code is much easier said than done and involves several key issues.

First of all, many organizations do not have the staff or budget required to do full code reviews in order to catch errors. Second, pressure to deliver web applications quickly can cause errors and encourage less secure development practices. Third, while products used to analyze web applications are getting better, there is still a large portion of the job that must be done manually and is susceptible to human error. Securing an organization's web infrastructure takes a defense in depth approach and must include input from various areas of IT. The paper contains different open source web application firewall literature which has been surveyed and existing open source web application firewalls are studied and also comparative study of open source web application firewall to protect web application from various web attacks.

## 2. LITERATURE SURVEY

With the possible exception of TCP hijacking, none of the network level attacks described in the previous section are capable of leading directly to a server compromise1. In addition, many of these attacks can be effectively detected and blocked at the firewall − in particular, a proxy firewall will block most of these attacks automatically. Similarly, a good firewall (in particular proxy firewalls) will limit the effectiveness of active scanning techniques to the firewall and public services.

In this section we have discussed the various literatures about application level attacks, different pattern matching algorithms published previously and the existing WAFs (FROMDEV Top 10 Open Source Web Application Firewalls, 2011), such as ModSecurity, IronBee, AQTRONIX WebKnight, Gaurdian@JUMPERZ.NET, etc.

## 3. ANALYTICAL STUDY OF OPEN SOURCE WEB APPLIATION FIREWALL

### A. MODSECURITY

ModSecurity [3],[4] is one of the oldest and widely used open source web application firewall which can detect application level threats on internet, and provides security against a range of security issues to web applications. It provides non viral open sources license and it can be integrated to Apache programs. Recently, ModSecurity released the version 2.6.0 which provides features for safe browsing API integration, sensitive data tracking and data modification features. The ModSecurity has following features (Ristić, 2012).

- HTTP Traffic Logging
- Real-Time Monitoring and Attack Detection
- Attack Prevention and Virtual Patching
- Flexible Rule Engine
- Embedded-mode Deployment
- Portability
- Network-based Deployment
- Licensing

### B. IRON BEE

Qualys created cloud based open source web application firewall – IronBee[3],[5] which examines the HTTP instead of the traditional IP packets to evaluate a data. It can even track attacks on cross site scripting code. IronBee is published through Apache License version 2 and it provides no copyright assignment. It has modular structure and is quite easy to use. Features of IronBee are listed below (Ivan Ristic).

- Open Source
- Highly Portable
- Shared Library
- Own Configuration File
- Own Configuration Language
- Audit Log Redesigned
- Buffering not tied with traffic inspection
- Buffer can be used in circular fashion

### C. AQTRONIX WEBKNIGHT

AQTRONIX[3],[6] WebKnight is an open source application firewall designed specifically for web servers and IIS, and it is licensed through the GNU – General Public License.

It provides the features of buffer overflow, directory traversal, and encoding and SQL injection to identify / restrict the attacks ( AQTRONiX).

- Open Source
- Logging

- Customizable
- Compatible with Web-Based Applications
- HTTP Error Logging
- SSL Protection
- Third-Party Application Protection
- RFC compliant
- Low Total Cost of Ownership (TCO)
- Run-Time Update, Authentication scanning
- Connection control/monitoring, Blocking robots and Prevent hot linking

### D. GUARDIAN@JUMPERZ.NET

Guardian@JUMPERZ.NET[3],[7] is an open source application layer firewall for HTTPS / HTTP and it assesses the HTTP / HTTPS traffic to protect the web application from external attacks. It immediately disconnects the TCP connection when the application comes in contact with a malicious / unauthorized request. Its features are given below (guardian.jumperz.net).

- Open Source
- Standalone, Supports all kinds of web server
- Developed in Java
- CUI
- HTTPS
- Rule-based and Plugins

## 4. COMPARATIVE STUDY OF OPEN SOURCE WEB APPLCIATION FIREWALL

Table 1: show comparative study of open source web application firewall

| OPEN SOURCE WEB APPLICATION FIREWALL | FEATURES |
|---|---|
| **Iron Bee** | 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 |
| **AQTRONIX WebKnight** | Buffer Overflow<br>SQL injection<br>Directory Traversal |
| **Guardian @JUMPERZ.NET** | Rule based signature detection<br>SQL injection<br>Cross Site Scripting |
| **ModSecurity** | SQL injection<br>Cross Site Scripting<br>Cookie attacks |

**Iron Bee** does detect and prevent Dos, DDoS attack, Cookie attacks, Brute force attack , SQL injection, Cross Site Scripting, Information leakage, Error message detection, Behavioral monitoring etc. **AQTRONIX WebKnight** does detect and prevent Buffer Overflow, SQL injection, DirectoryTraversal etc. **Guardian @JUMPERZ.NET** does detect and prevent Rule based signature detection , SQL injection, Cross Site Scripting etc. **ModSecurity** does detect and prevent SQL injection, Cross Site Scripting, Cookie attacks etc.

## 5. CONCLUSIONS

This paper includes the current scenario in the Internet, web application vulnerabilities and how WAFs are useful to shield the web applications from attacks. It includes an analytical study of different existing open source WAFs, such as ModSecurity, IronBee, AQTRONIX WebKnight, Gaurdian@JUMPERZ.NET, etc. And form the comparison table, We then extracted the best features from these WAFs.

## 6. REFERENCES

[1] OWASP Top Ten attacks. https://www.owasp.org

[2] Imperva Web Application Firewall www.imperva.com/

[3] (2011) FROMDEV Top 10 Open Source Web Application Firewalls. [Online]. http://www.fromdev.com/2011/07/opensource-web-application-firewall-waf.html.

[4] Ivan Ristić, MODSECURITY HANDBOOK -The Complete Guide to the PopularOpen Source Web Application Firewall. U.K.: Fiesty Duck, 2012.

[5] Brian Rectanus Ivan Ristic, IronBee Reference Manual.: Qualys, Inc.

[6] AQTRONiX. [Online]. http://www.aqtronix.com/?PageID=99.

[7] guardian.jumperz.net. [Online]. http://guardian.jumperz.net/manual/en/body.html.

[8] WebCastellum Team, User Manual WebCastellum Web Application Firewall.: itanius informatik GmbH..

[9] OWASP,WebScarab http://www.owasp.org/software/webscarab/

[10] AQTRONIX WebKnight Application firewall http://www.aqtronix.com/?PageID=99