Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 7, Issue. 3, March 2018, pg.43 – 50

WEB APPLICATION FIREWALL-DOT DEFENDER

Sanghita Saha

School of Computer Science & Engineering, Vellore Institute of Technology, India

Email: sanghita123saha@gmail.com [1]

Abstract—In the recent years, web applications are the number one source of vulnerabilities targeted by Hackers. The fact is, hackers are constantly probing the Web for vulnerabilities. Although traditionally companies have used intrusion detection and prevention systems which monitor the network in general, there is now a widespread use of Web Application Firewalls as a security solution that monitors and protects only web applications. A web application is a software application that is accessed over the Internet using HyperText Transfer Protocol (HTTP). In a typical web application a client, such as a browser, interacts with a web server by exchanging a series of messages that are made up of HTTP requests and responses. An attacker often exploits vulnerabilities that exist in a web application to launch attacks. DotDefender is a web application security solution (a Web Application Firewall, or WAF) that offers strong, proactive security for websites and web applications. DotDefender can handle .NET Security issues. DotDefender provides great application security, flexible integration & management tools, automatic deployment and simple maintenance - which saves everyone valuable time.

Keywords: -Web application firewall, Sql Injection attack, Dos Attack, HTTP, Path Traversal.

I. INTRODUCTION

Over the past few years, a clear trend has emerged within the information security landscape; web applications are under attack. The threats of web based attacks from hackers are getting more frequent and more sophisticated. Web application vulnerabilities can be attributed to many things including poor input validation, insecure session management, improperly configured system settings and flaws in operating systems and webserver software. Most attacks are “stealth-like”. Many companies do not even know they

have been attacked. Cyber criminals are looking at obtaining credit card information, social security numbers, addresses and other sensitive information while exploiting the vulnerability for as long as they are undetected. One technology that can help in the security of a web application infrastructure is a web application firewall. A web application firewall (WAF) is an appliance or server application that watches http/https conversations between a client browser and webserver [1].

A web application firewall (WAF) protects web application much in the same way a traditional firewall protects a network. It controls the input and output, as well as the access to and from the asset it is protecting. However, traditional network firewalls evaluate IP packets or protocols without an awareness of the application payload so they cannot provide protection to the application layer. Without an awareness of the HTML data payload these layer 3 devices cannot recognize and overcome the types of application layer threats that make web applications vulnerable to attack. Attacks such as SQL injection, cross-site scripting or session hijacking and many more are aimed at vulnerabilities in the web applications itself. over 70% of all web sites are contain vulnerabilities that make them susceptible to Cross-Site Scripting, SQL Injection, Path Traversal, and many other exploits. Web application firewalls are a perfect solution to the problems with code reviews and vulnerability assessments because they actively and constantly protect web applications against threats using Pattern Recognition to detect and thwart zero-day exploits and other evolving threats, Session Protection to help prevent impersonation, and a Signature Knowledgebase to block known vulnerabilities and known attackers. With Dotdefender web application firewall can avoid many different threats to web applications because Dotdefender inspects HTTP traffic and checks their packets against rules such as to allow or deny protocols, ports, or IP addresses to stop web applications from being exploited. Architected as plug & play software, Dotdefender provides optimal out-of the-box protection against DoS threats, Cross-Site Scripting, SQL Injection attacks, path traversal and many other web attack techniques. Dotdefender's unique security approach eliminates the need to learn the specific threats that exist on each web application. The software that runs Dotdefender focuses on analyzing the request and the impact it has on the application. Effective web application security is based on three powerful web application security engines: Pattern Recognition, Session Protection and Signature Knowledgebase.

The Pattern Recognition web application security engine employed by Dotdefender effectively protects against malicious behavior such as the attacks mentioned above, and many others. The patterns are regular expression-based and designed to efficiently and accurately identify a wide array of application-level attack methods. Dotdefender apart is that it offers comprehensive protection against threats to web applications while being one of the easiest solutions to use [2].

The reasons Dotdefender offers such a comprehensive solution to your web application security needs are:

- Easy installation on Apache and IIS servers
- Strong security against known and emerging hacking attacks
- Best-of-breed predefined security rules for instant protection
- Interface and API for managing multiple servers with ease
- Requires no additional hardware, and easily scales with your business.

II. WEB APPLICATION FIREWALL

A Web Application Firewall is software or an application placed between the network firewall and the web server. Some Web Application Firewalls look for certain 'attack signatures' to try to identify specific attack that an intruder may be sending, while others look for abnormal behaviour that does not fit the websites normal traffic patterns.

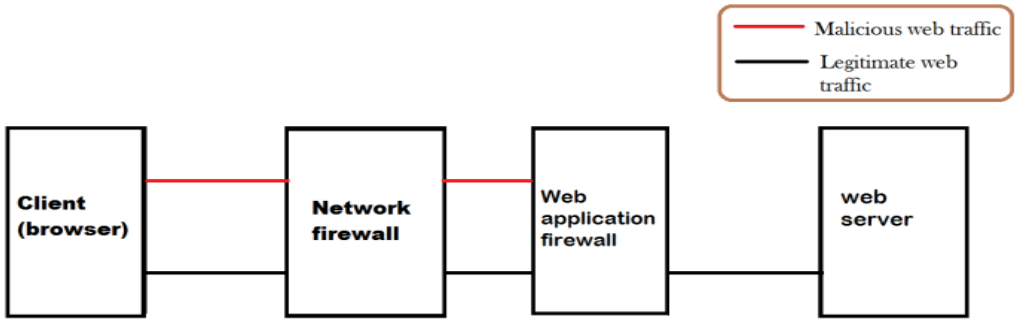

Fig. 1 web application infrastructure

A Web Application Firewall (WAF) is a security device that protects the web application and web application server from various attacks such as SQL Injection, cross site scripting, code injection, etc. WAF protects web application against detected vulnerabilities and prevents them from being exploited by attackers [1]. Fig.1. shows Web Application Firewall infrastructure. WAFs are specifically designed to inspect HTTP(s) traffic and regulate data contained within headers, URL parameters, and web content. With a WAF in place, malicious hackers may target insecure websites, but attacks are intercepted and denied Before reaching the custom web application code. WAFs at their core are designed to separate safe web traffic from malicious traffic before it's received by the website.

III. WORKING OF WEB APPLICATION FIREWALL

The proposed Web Application Firewall not only detects attacks that are known to occur in web application environments, it also detects and prevent new unknown type of attacks. It supports two approaches to secure the web application. First one is the Signature Based Model and second one is Normal Behavior Model. The Signature Based Model defines all the attack patterns or signatures of known attacks which exploits weaknesses in system and application software. Signature Based Model uses pattern matching techniques against the frequently updated database of attack signatures. It is useful to detect known attacks but not the new ones whereas the Normal Behaviour Model defines normal behaviour of the web application. This Model uses the rule based techniques or data mining techniques to detect unknown attacks without signatures.

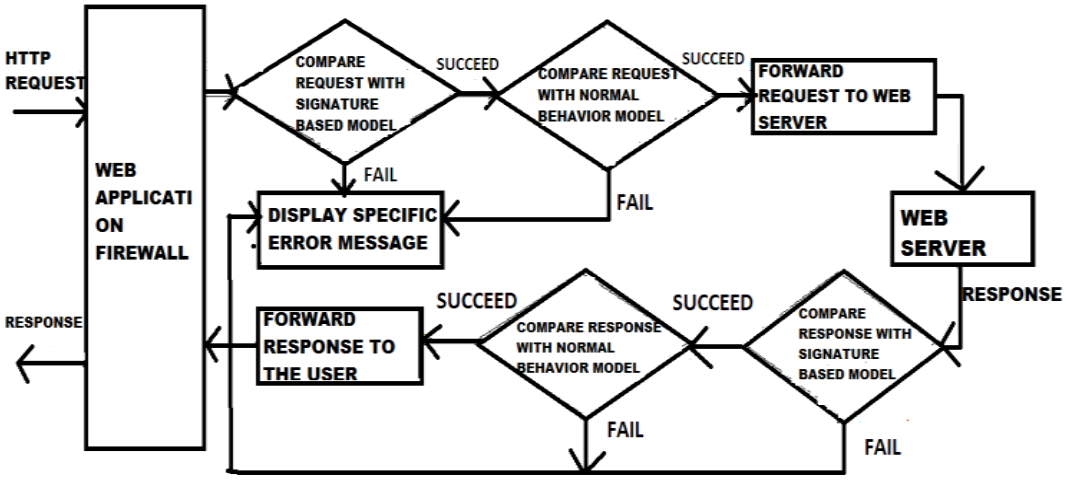

Fig .2 Web application firewall working

The incoming HTTP request is compared with the signatures already stored in the database. If the request matched with the signature then forwarded to the next comparison method. Pattern matching techniques can be used to detect known attacks. If the request does not matched with the signatures, it will be compared with the Normal Behaviour Model. If it matches then request is forwarded to the web server. Web server sends response back to the Web Application Firewall which will again compare it with the signature based model. If the response matched with the signature then forwarded to the next comparsion model.If matched with the normal behaviour, then safe response is forwarded to the user otherwise Display an error message. Thus it protects from SQLinjection, cross site scripting, buffer overflows, forceful browsing and various kinds of attacks [1].

IV. WEB APPLICATION ATTACK

Web based attacks are considered to be the greatest and oftentimes the least understood of all risks related to confidentiality, availability, and integrity. The purpose of a web based attack is significantly different than other attacks; in most traditional penetration testing exercises a network or host is the target of attack. Web based attacks focus on an application itself and functions on layer 7 of the OSI. That nearly 70% of all attacks occur at the application layer. Application vulnerabilities could provide the means for malicious end users to breach a system's protection mechanisms typically to take advantage or gain access to private information or system resources. Information gathered can include social security numbers, dates of birth, and maiden names, which are all often used in identity theft. Another popular target for attackers is credit card data which left unprotected and unencrypted can be used to cause significant damage to organizations most valued assets, their customers. Different types of attack are as follows-

A. Dos Attack

Denial of Service attack is intended to disrupt a web site's ability to serve pages to its visitors. Usually, these attacks are carried out by overloading the server with requests. Mostly the following tactics are used in a DoS attack:

1) *Ping Flooding:* Also known as ICMP flood, Smurf attack, Ping of death, or SYN flood. Ping flood works by sending the target an overwhelming number of ping packets, usually using the "ping" command. It is very simple to launch and by creating traffic that exceeds the web site's bandwidth availability, the attack is a success.

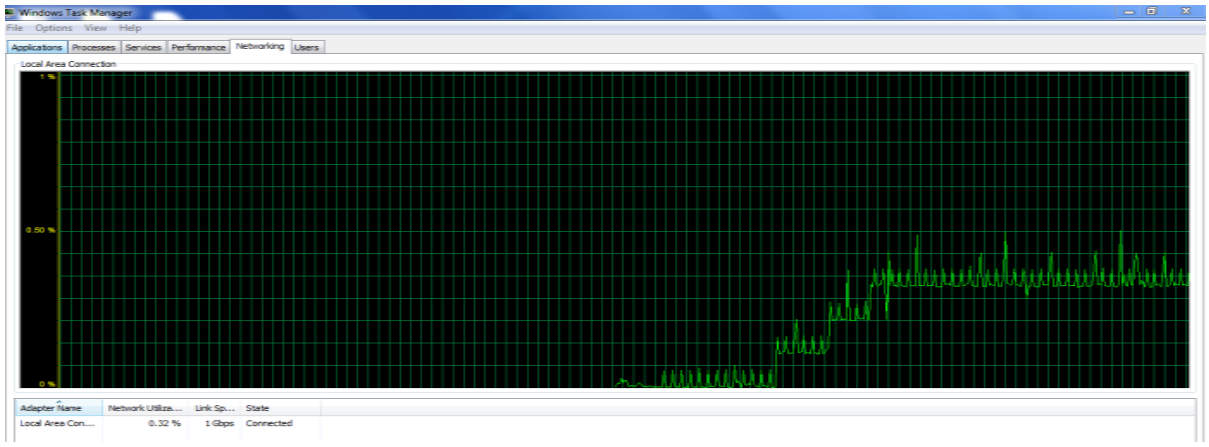

Fig .3 Ping Flooding

A SYN flood sends a flood of TCP/SYN packets using a forged sender address. Since the sender addresses not correct, the response in the form of a TCP/SYNACK packet never comes leaving a half-open connection. As these connections begin to accumulate, the number of available connections becomes saturated keeping legitimate requests from successfully connecting [2].

2) Peer to Peer attack: Peer to Peer attacks are launched when the attacker causes users to disconnect from their peer to peer network and to connect to the victim's website instead. Like a zombie or botnet attack, several thousand computers may be trying to connect to the victim's site at once. If enough machines are controlled by the Attacker, the overflow of connection requests can easily bring down a web application. Unlike zombie attacks, there is no botnet so the attacker does not have to communicate with the Computers he uses to launch his attack.

3) Application level floods: While most Denial of Service attacks exploit bandwidth, some rely on software related exploits such as buffer overflows. These attacks cause confusion in the application causing it to fill the disk space or consume all available memory or CPU cycles.

B. Sql Injection Attack

SQL Injection works by the attacker finding an area on a web site that allows for user input that is not filtered for escape characters. User login areas are often targeted because they have a direct link to the database since credentials are often checked against a user table of some sort. By injecting a SQL statement, like ') OR 1=1--, the attacker can access information stored in the web site's database. Of course, the example used above represents a relatively simple SQL statement. Ones used by attackers are often much more sophisticated if they know what the tables in the database are since these complex statements can generally produce better results [2].

C. Path traversal

Path Traversal vulnerabilities give the attacker access to files, directories, and commands that generally are not accessible because they reside outside the normal realm of the web document root directory. Unlike the other vulnerabilities discussed, Path Traversal exploits exist due to a security design error - not a coding error.

D. Cross Site scripting

Cross Site Scripting (XSS) attacks occur when an attacker is able to inject malicious client-side script into a vulnerable web page. When these scripts are run, they can be used to install malicious software on the visitor's computer, steal a visitor's cookie, or hijack a visitor's session.

V. PREVENTION OF WEB ATTACK BY DOTDEFENDER

Dotdefender is a software-based Web Application Firewall, which is installed as a webserver plug-in. It works cross-platform, and supports Apache or Microsoft IIS web-servers. It's also suitable for shared, hosting environments with central management capabilities. It uses a pattern recognition Engine to detect actions that could indicate an attack, and a session protection engine to deal with session spoofing and denial of service attacks. It also ships with a signature database to detect known attacks. Its feature list is boosted by file upload protection, server masking and information leakage engines. Its pattern recognition and signature engine both support custom entries [3].

A. Preventing Denial of Service Attacks

With Dotdefender web application firewall avoid DoS attacks because dotDefender inspects HTTP traffic and checks their packets against rules such as to allow or deny protocols, ports, or IPad dresses to stop web applications from being exploited. Architected as plug & play software, dotDefender provides optimal out of the box Protection against DoS threats and many other web attack techniques.

B. Preventing SQL Injection Attacks

With Dotdefender web application firewall avoid SQL injection attacks because Dotdefender inspects HTTP traffic and determines if web site suffers from SQL Injection or other attacks stopping identity theft and preventing data leaks from web applications. Architected as plug & play software, Dotdefender provides optimal out-of the-box protection against SQL Injection attacks and other web attack techniques. The reasons Dotdefender offers such a comprehensive solution to web application security needs are:

- Enterprise-class security against known and emerging hacking attacks
- Solutions for Hosting, Enterprise and SMB/SME
- Supports multiple platforms and technologies - IIS, Apache, Cloud ...
- Central Management console for easy control over multiple dotDefender installations
- Open API for integration with management platforms and other applications

Dotdefender blocks against various SQL Injection techniques including, but not limited to:

- Terminating queries using quotes, double-quotes, SQL comments
- Comparison queries using commands such as BETWEEN, LIKE, ISNULL
- Database manipulation commands such as TRUNCATE, DROP
- Reserved words such as CASE WHEN, EXEC
- Blindfolded injection techniques such as Boolean queries and WAITFOR DELAY
- Database-unique attacks relating to Oracle, MySQL, MS-SQL
- Signature evasion techniques such as using CONVERT & CAST
- Buffer overflow attacks via SQL Injection
- XML and Web-Services encapsulating SQL Injection techniques
- Null byte signature evasion
- HEX encoding mixtures for signature evasion
- Using SQL CHAR() for signature evasion
- Zero-day protection against MS-SQL stored procedure attacks such as MS08-040 [3].

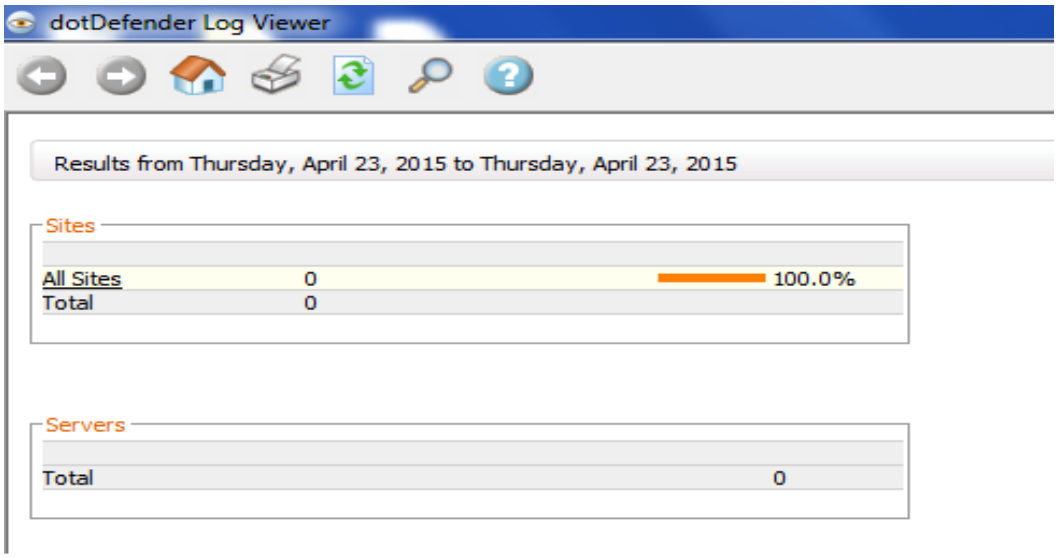

Fig. 4 Working of Dotdefender

VI. BENEFITS OF DOTDEFENDER

The main benefits of Dotdefender firewall are as –

- Powerful protection: against application attacks, session attacks and known attack sources.
- Preconfigured set of rules: best practices security right out of the box.
- Automatic live update: ensures protection against the latest threats.
- Rapid deployment: simple installation, integration, and customization.
- Software firewall: no influence on traffic or network architecture.
- System supports: a wide variety of platforms—Linux, BSD, Solaris, Mac, Windows.
- Variety of implementations: SMB customers, Hosting services, OEM solution, internal enterprise web implementation, enterprise distributed web architecture [4].

VII. CONCLUSION

Web applications have a natural sensitivity to attacks. Attacks are easy to perform compared to network attacks. For this reason web attacks are very attractive for hackers. A Web Application Firewall can be a highly effective defence for blocking newly discovered vulnerabilities or previously successful attacks. So implementing a web application firewall is a great method to protect application from web attacks. The Dotdefender tool is able to detect both known and unknown attacks that exploit the web application. It uses both the signature based model in which all the attack patterns are already stored and normal behavior model in which all the normal traffic that target the web applications are already stored in the database. Thus it can detect known attacks with signatures and also the newer attacks without signatures. By watching for unusual or unexpected patterns in the traffic it can alert and defend against unknown attacks. If a user makes an illegitimate request to a web application protected by Web Application Firewall, the request will never go to the application.

ACKNOWLEDGEMENT

I would like to thank Prof. Satheesh A for giving me this opportunity and his valuable suggestions and ideas. I also extend my word of thanks to all the authors and researches whose work and research was really helpful.

REFERENCES

[1] J. M. Waghmare, "Web Application Firewall to Protect Against Web," IJCTA, 2013.
[2] "Applicure Technology," 22 april 2015. [Online]. Available: http://www.applicure.com/.
[3] "Dotdefender," 20 april 2015. [Online]. Available: http://website-security-and-performance-review.toptenreviews.com/dotdefender-review.html.
[4] "NETCETERA," 23 APRIL 2015. [Online]. Available: https://www.netcetera.co.uk.

