# Design and implementation of coldfusion-based web application firewall

Feng Fangmei[1]
Research Institute of Electronic Science and Technology
University of Electronic Science and Technology of China,P.R.China
fmei0920@126.com

Changgeng Shao[2]
Research Institute of Electronic Science and Technology
University of Electronic Science and Technology of China,P.R.China
lzscg@126.com

Dan Liu[3]
Research Institute of Electronic Science and Technology
University of Electronic Science and Technology of China,P.R.China
liudan@uestc.edu.cn

***Abstract*—Based on the comprehensively analysis of the security threats to the Web applications, the ColdFusion-based Web Application Firewall is presented, and it's implemented with CFML. The test results show that the firewall can effectively block various malicious attacks against the application layer, such as SQL injection, XSS, etc., and protect the ColdFusion-based Web applications.**

***Keywords- Web application; the security threat; Web Application Firewall; ColdFusion Introduction.***

## 1. INTRODUCTION

With the rapid development of Internet technology, the Web applications have gradually become an essential part of people's daily life. 《The 27th China Internet Development Statistics Report》 [1] released by China Internet Network Information Center (CNNIC) in 2011 shows that, in China, netizens have exceeded 450 million, e-business applications have taken the lead, the broadband penetration rate has been close to 100%. ColdFusion is an excellent cross-platform application server launched by Allaire in 1995. There are more than 10 thousand organizations and more than 120 thousand servers which are running ColdFusion over the world. [2] However, the rapid development of Web applications also poses a threat to the Web Security. 《The 2011 Safety Survey Report》 [3] released by Symantec Corp. shows that 71% of respondents have suffered the cyber-attacks in the past 12 months, and it's 75% in 2010; 92% of companies suffered economic losses because of the cyber-attacks in 2011, and it's 100% in 2010. The means of Web attack are so various that the traditional means of protection (firewall, the IPS/IDS, etc.) appeared to be inadequate. The main security threats to current web are firstly analyzed and their corresponding defensive countermeasures are given. Then based on the ColdFusion server, combined with the MySQL database, the Web application firewall system has implemented with CFML language. It provides the specific protection for a variety of application-layer attack. The test results show that it can effectively block a variety of malicious attacks to the Web applications.

## 2. WEB THREATS AND DEFENSIVE COUNTERMEASURES

A Web site may contain several components, such as a Web client, Web applications, Web servers and database, etc.. Based on the current Web technologies, any component may be a fatal security issues, facing a serious security threat. Common security threats as follows:

(1) SQL injection: the attacker utilizes programmers' overlook to detect the user input, through the normal web access capabilities, fabricates and submits the special code that contains the SQL statement to deceive the server in order to steal users' privacy (such as passwords, etc.), even to obtain the permissions to control the host. Defensive countermeasures: a) Check the user input, filter or convert the special characters in a string (varchar, text etc.), such as single quotes and comment symbol etc.. b) when an error occurs during the sql statement executing, do not display the complete error message to the user. c) Try to use views and stored procedures when creating a query.

(2) Cross-site scripting (XSS): XSS is a special attack way against the dynamic pages. The attacker embeds the malicious executable code in Web pages. Any user who accesses this page through a browser will load and execute it. Defensive countermeasures: a) Prohibit the browser in the client to load the JavaScript script automatically and prohibit the <META REFREASH> label and <IFRAME> label automatically call the program or file. b) Filter the special characters in dynamic scripting code, such as JavaScript、script、 <、>. c) Limit the input length. d) Restrict users to upload files because XSS attack often happens with Flash and other files.

(3) Denial of Service (DoS): Its purpose is to make the target server to stop providing normal services. The attacker using the security flaws existing in network protocol (TCP/IP protocol), expendable attack on the target server's resources through a variety of methods. These resources include: memory, CPU, network bandwidth etc.. Defensive countermeasures: a) Harden the operating system. Audit system and view the system's security log periodically. b) Limit the network bandwidth occupied by a specific protocol to avoid exhausting system resources. c) Configure the firewall to allow

978-0-7695-4719-0/12 $26.00 © 2012 IEEE
DOI 10.1109/CSSS.2012.170

only the necessary communications. Block unwanted ports and hostile IP address.

(4) Brute Force: Exhaust user's username, password and other information, and use cracking tools to verify them one by one, until finding the right results. Defensive countermeasures: a) Set a strong password. b) Strong account blocked. That is, if fail to log on after a certain number of times, then block the account. This strategy has a disadvantage. If the blockade strategy is too sensitive, an attacker might try to block all users, and that will result the application to DoS. Therefore, a compromise strategy is when being attacked, the application should block the account for a certain time, such as five minutes. In this way, violent attacks can be effectively prevented, and so do the DoS attacks.

(5) Path Traversal: The attacker attempts to access files outside the Web root through a specific URL request, he can make the Web application to display or execute the arbitrary files on the server. Defensive countermeasures: a) Patch to the Web server in a timely manner. b) Put the dynamic pages (such as *. cgi, *. asp, *.jsp etc.) into a protected directory, and forbid users to directly access the files under that directory.

## 3. OVERVIEW OF WEB APPLICATION FIREWALL

Web Application Firewall (WAF) specialized to protect the Web applications, test and validate the client's request and ultimately real-time block the legitimate requests. Different from the traditional security software, WAF can parse the data of the application layer, and filter the application layer data. As to the protection of Web applications, it owns the inherent advantages. At present, the Web firewall technology has the following categories [4]:

(1) Feature recognition: Each act has its own proprietary property, according to this feature, the feature recognition methods are usually using to detect viruses and worms. But there are thousands of attack ways, meanwhile, they have characteristics of both varied and inevitably similar, therefore the false alarm rate of feature recognition is relatively high.

(2) Algorithm recognition: Algorithm recognition has been optimized on the basis of the feature recognition. Firstly classify varieties of attacks, secondly through some kind of algorithm, classify the attacks which own the same characteristics into different modes, and lastly compare the different modes, rather than comparing individual characteristics.

(3) Pattern matching: Classy different acts of each attack into a particular mode, and use regular expressions to define each mode, and then match the corresponding patterns in the object string to be detected, and ultimately determine whether they are intrusion acts.

Among these three techniques, pattern matching techniques are most frequently used. Its detection efficiency is relatively higher. CFShield engine is implemented with the pattern matching technology. Based on different attacks, construct a corresponding regular expression to achieve an exact match.

## 4. OVERVIEW OF COLDFUSION

ColdFusion is an application server—(usually) resides on the same computer with a Web server, extends the functionality of Web server, and is able to complete something that the Web server usually can't [5]. ColdFusion markup language (CFML) is easy to learn, similar to HTML, while extending HTML with more powerful functionality. After installing, ColdFusion will configure the Web server to tell Web server that the files with extension. cfm, or. cfml are ColdFusion files. When requesting a ColdFusion file, the Web server should forward the request to the ColdFusion for the next process. After receiving the request, ColdFusion will resolve the ColdFusion tag, variables and functions. ColdFusion will not do any processing with the HTML files or plain text, and forward them to the Web server directly. Finally, Web server will send the results to the requester.

## 5. DESIGN OF THE SYSTEM

The WAF system (CFShield) structure shows in Figure 1. WAF, ColdFusion server and Web server resides on the same computer. It fully protects the ColdFusion Web application request, according to the session of application layer to deal with the application layer information, and thus finds the acts which violate the intended security policy.

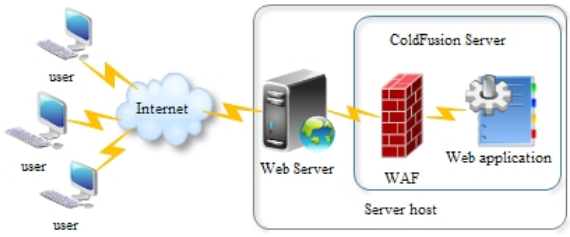


Figure 1 CFShield structure

In view of the features of ColdFusion and analysis on a variety of Web attacks, CFShield can be divided into four major functional subsystems: threat detection subsystem, audit subsystem, configuration subsystem and interactive subsystem. Its overall architecture shows in Figure 2.

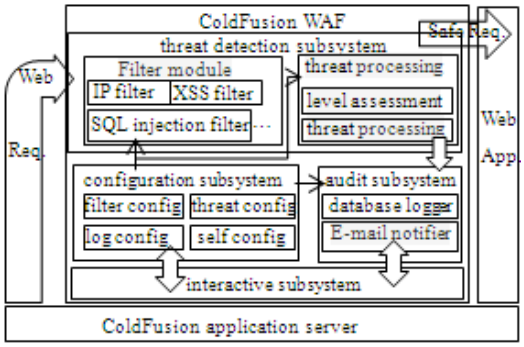


Figure2 CFShield overall architecture

### *5.1 Threat detection subsystem*

Threat detection subsystem consists of two modules: Filter modules and threat processing module. The Web requests are routed to the data filtering module via ColdFusion. Data

filtering module filters the Web requests with IP filter, SQL injection filter, XSS filter, ID filter, file upload filter, dictionary attack filter and CRLF injection filter. Threat processing module evaluates the threat level of the detected threat, compares the assessment value and the threshold set, according to the result to block request, release request or log request.

IP filter is the first filter of the filtering module, including two modes: the passive mode and the active mode. There are two working ways in passive mode. One is when the Web request violates the rules of any filter, the event_listener.cfc component and repeat_offender_listener.cfc component will be called to monitor the IP address, and then repeat_offender_filter.cfc component continues to process the request. The other is that CFShield loads IP filter according to the order of the filters. When a Web request arrives, the event_listener.cfc component and repeat_offender_listener.cfc component will be called to monitor the IP address, and then repeat_offender_filter.cfc component continues to process the request. In active mode, IP_block_filter.cfc component takes the initiative to block specified IP address in the blacklist.

SQL injection filter is secondly to be loaded. After passing IP address filter, the Web request will be transferred to SQL injection filter by threat processing module. SQL injection filter will match the request data with a series of SQL injection filtering rules, and then transfer the results to the threat processing module. Filtering rules constitute of a series of regular expressions. Such as:

*;\W*(drop|delete|union|grant|select|group|update|insert|/*|exec|sp_|xp_|create|alter|truncate|declare|cast|waitfor|shutdown)* matches the keywords of SQL injection.

*/*.**/* and *.+(--|##)\s*$* matches the comment symbol, etc..

After passing these two filters, the Web request will pass XSS filter, ID filter, file upload filter, dictionary attack filter and CRLF injection filter one by one. The design ideas of these filters are similar to the SQL injection filter whose key is to build a series of filtering rules.

### *5.2 Audit subsystem*

The log function not only provides the basis for the security event audit, but also can help administrators analyze the system security risks. The audit system logs contain the Web requests' detailed information, such as: the request URL, port number, the request IP address, time, date, and the exception description.

Audit subsystem contains the database log and the mail notification. The database log records all the information of the Web request whose threat level is higher than the log threshold. It can clearly reflect the access security state of Web application through the charts and data. Mail notification system provides an instant notification when the Web application is under attack.

### *5.3 Configuration subsystem*

The firewall administrator can customize the firewall in the configuration subsystem. Ordinary users can only view the configuration information. The filter module can be configured to set the filter order of the filter, set the IP address blacklist as well as different filters to enable and disable. The database log can be configured to enable or disable the log function and the email notification function. The threat processing module can be configured to set the threat threshold of logging and denying the Web request. The self-management module can reset the firewall. If the configuration information has been modified, the firewall must be re-initialized to read the new configuration information.

### *5.4 Interactive subsystem*

Interactive subsystem is mainly used to interact with the firewall. The subsystem includes two functions: to view the log and manage accounts. After authentication, the administrator can view the firewall logs, reconfigure the firewall, modify the administrator account information, add users and modify user information and browsing permissions. Ordinary users can view the firewall log, and modify the account information. Except for the functional integrity and ease of use, in order to improve the user experience, the interactive subsystem uses a large number of charts and statistical tables which present the firewall log to the user in the form of a web page. Through these charts and tables, users can intuitively understand the security status of the Web application server.

## 6. TESTING AND EVALUATION

In the test, CFShield is used to protect the Web-based vulnerability system—Hacme Shipping which is developed with ColdFusion and MySQL database by McAfee Foundstone. The system contains the common security threats faced by Web applications, such as SQL injection, XSS, authentication vulnerability, authorization vulnerability, etc.. It can help us learn the characteristics of the various loopholes and how to exploit these vulnerabilities to attack.

To verify the protective capabilities of CFShield, the automation tool WatchFireAppScan is used to scan Hacme Shipping before and after deploying CFShield. The test result shows in table 1.

Table 1 Test Result

| *vulnerability type* | *Number/before CFShield* | *Number/after CFShield* |
|---|---|---|
| SQL injection | 3 | 0 |
| XSS | 2 | 0 |
| Information disclosure | 8 | 0 |
| Session customized | 1 | 0 |

## CONCLUSION

After a comprehensive analysis of the main security threats to the current Web and the corresponding defensive countermeasures, the ColdFusion-based web application firewall CFShield is implemented with CFML and MySQL database. The test result shows that CFShield can effectively intercept a variety of Web attacks and protect ColdFusion web application. However, it involves so many theory and development limited that CFShield can be further optimized in several directions:

(1) Using regular expressions to build a variety of filtering rules, CFShield can match the majority of Web attacks. But the rule base is not complete and can be further expanded to improve.

(2) Since this is only first exploration of ColdFusion-based Web application firewall, it aims at achieving the basic firewall functions in this paper, so the configuration function of CFShield is not very powerful, and could be further refined, custom filtering rules to achieve, for example.

(3) Designed on the basis of the known Web attacks, CFShield cannot effectively defend the unknown ones, and can be further optimized, such as the self-learning ability of the firewall.

## REFERENCES


[1] 27th China Internet Development Statistics Report [R]. Beijing: China Internet Network Information Center. 2011-1

[2] Han Dong, Yin Cheng. ColdFusion web programming strengths and experience [J]. science&technology information,2010-9(58)

[3] Symantec announced the results of the 2011 Safety Survey Report. [EB/OL]http://storage.chinabyte.com/179/12178179.shtml

[4] Zhao Xuwei. Web application security crisis, the WAF came into being to become a weapon [N]. Network Security Technology and Application. 2008-4

[5] Ben Forta, Raymond Camden, Charlie Arehart. Adobe ColdFusion 8 Web Application Kit Volume 1: Getting Started[M].Beijing. Publishing House of Electronics Industry, 2009