Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN : 2348-4470
p-ISSN : 2348-6406

International Journal of Advance Engineering and Research Development

Special Issue on Recent Trends in Data Engineering

Volume 4, Special Issue 5, Dec.-2017

Prevention of Website Attack Based on Remote File Inclusion-A survey

P.S.Sadaphule[1], Priyanka Kamble[2],Sanika Mehre[2],Utkarsha Dhande[2],Rashmi Savant[2]

[1]*Computer Engineering,AISSMS's IOIT, Pune*
[2]*Computer Engineering,AISSMS's IOIT*

Abstract: --*A web application is a computer program that utilizes web browser and web technology to perform tasks over the internet. In recent years, millions of businesses use the internet as an effective communication channel which lets them exchange the information worth their target market and makes fast,, secure transactions. However, there are many threats which are arising to gain this valuable information which is mainly done by various kinds of attackers who uses different kind of techniques for data thief. So, the challenge is to provide the security to various web application and prevent the attacker to gain root shell access and admin passwords. In survey, observed that the attacks like RFI(Remote File Inclusion) and LFI(Local File Inclusion) are truly vulnerable. Though, these kinds of attacks are rare but the unauthorized access can harm the whole system. So, system mainly concentrates on detection and prevention of web application by using various techniques such as Dynamic Allocation, File Size Verification, Digital Signature and Sanitization of Input. The successful overcoming of these attacks will increase the security which will improve the quality of web application.*

Keywords: --*Local File Inclusion attacks,Prevent vulnerability,Remote File Inclusion Attacks, Security*

I. INTRODUCTION

These days everything on which human beings are relay works on websites and web applications. But as the usage of the website increases so as the attacks on such sites. The web application which mainly focuses on functionality and usability are attracted by various hackers which results in heavy attacks on such sites by recognizing their weaknesses and vulnerabilities. The security is the major concern from main area of development such as online monetary transactions, payment of bills, online learning, online shopping, corporation's organizations research community, government, etc.

As it is used commonly and highly there is high risk that cyber criminals can exploit the weaknesses of such web applications. From research it has seen that half of current computer security threats and vulnerabilities affect the web application.

Unauthorized access will allow attacker to gain access to back end database performing attack via front end web applications. Security is important in such web applications. Web applications have been developed in PHP language because of its prevalent and easy to develop characteristics. Web applications found to be unsecured because of the careless use of functions in PHP language and different types of vulnerabilities of coding inside web applications. Ensuring the security of millions of existing vulnerable websites is a huge challenge now days. Vulnerability scan carried out in 2013 by semantics web site vulnerabilities assessment service found that 77% of sites are vulnerable and 16% of them are critical vulnerabilities. Because vulnerabilities fount in web sites many organization lose their reputation.

Types of vulnerabilities occur in web application are SQLi, LFI, RFI ,XSS etc .In the survey focusing on LFI and RFI vulnerability. Existence of RFIvulnerability in web application is represented if, web application has some codes that will dynamically refer to an external script. The main purpose is to exploit referencing function so as

to upload malware (backdoor shell). This is occurred from remote domain. In LFI, File is injected that already exists in web application.

The objective of the project is to prevent web application from various malicious attacks of RFI and LFI by using PHP language and CSS, preventing them using Dynamic Allocation, File Size Verification, Digital Signature and Sanitization of Input prevention methods. Also to develop a web application having some weaknesses to demonstrate above mentioned attacks.

II. LITERATURE SURVEY

There are number of researches done on various web vulnerabilities which comes under Semantic URL, Cross-Site scripting, Cross-Site Request forgery, etc. In this our project comes under Semantic URL means such attacks involve a user modifying the URL discover mode to perform various actions which are not originally planned to be handled by server[2]. Survey found reviews on various vulnerabilities such as RFI, LFI, SQLi, Query string attacks[1][3][4][5][6].

Also, Studied various methods used for exploitation, testing areas and security method and tools including different algorithms which are being used[1][2][3].For preventing from the LFI attack also the various vulnerabilities and methods of LFI attacks[4].For studying more about RFI attack we have studied the RFI botnet[8].To learn more about attackers perspective and why attacker choose RFI type of vulnerability we have studied different types of exploits and learnt how the attacker gains root shell access and admin passwords[7]

Begum et.al.presentthe LFI exploitation based on RFI and SQLi.To prevent from attacks sensitive information like root user ,password ,SSH login credentials are disclosed by the system.We have also learned methods used for exploitation such as get method and post method exploitation.This paper imposes security feature which developers usually design data processing technology through HTTP POST method.Different types of files are stored in different directories to ensure security.Also ,we have studied various methods used for exploitation and security.LFI and RFI are vulnerabilities which we have concentrated on. LFI is nothing but web application's vulnerability which allows a user to include different files located in web application on server machine.RFI is one of the weaknesses in a web application by which it remotely accepts any type of user input.

J.Rina Elizabeth et alhas proposed different testing areas and types of testing.Also concentrates on the knowledge of the technique pentesting on web application, discusses the different phases, most common of this attacks can be victims as well as upgrades software tools to make the penetration test.Pentesting means a safety test with a specific objective for evaluating a system.It is the set of safety test with detector objective , the test ID terminated after the goal achieved. In this paper we have studied different types of security bases such as authentication,authorization, integrity and availability.Also the common attacks which are being used such as semantic URL,cross site scripting, HTTP request counterfeited and attacks through the database.From this we understood that RFI and LFI attacks comes under semantic URL method.

J.Jemmi Hazel et al protects the front end web application from unauthorized access.Web application front end and database back end can be accessible through web browser.For front end security vulnerability scanner is used.This system focuses on design of web application and detection and prevention of said attacks which are RFI, query string attacks, cross site scripting attacks and union attacks.It overcomes the attacks by using different algorithms such as longest sub sequence algorithm and brute force string matching algorithm.The objective is to develop a web application-bot admin and user credentials ASP.net.Also we have studied how to provide web application authentication.

G. Mir SamanTajbakhshet al concentrates on LFI vulnerability.The local file access is done by manipulating the user IP.The type LFI attacking methods are null byte poisoning, log poisoning, malicious image upload, self file in linux

environment and alternate log poisoning.In this paper we have studied that the LFI vulnerability is prevented from root cost analyze source code and defeat attack with sanitization.From this paper we have studied the importance of sanitization and how it is used as a prevention method.AntiLFIer is also used as a prevention method which allows access to only the trusted files.Prevention method checks whether the file is trust full or not.

NatasaSuteva proposed different types of attacks and the analysis done on such attacks are mentioned. Vulnerability scan carried out in 2013 by semantics website vulnerability Assessment services found that 77per cent of sites are vulnerable.The vulnerabilities found in websites many organization are loosing their reputation.This paper also focuses on prevention methods performed after performing attacks on victim's machine.This paper attack scenario on the known vulnerable web application WAckoPicko of three types of attacks-SQL Injection stored XSS and Remote File Inclusion.This application has 10 vulnerability accessible without authentication.In forensics expertise there are mail three phases acquisition, analysis, presentation.

Mr.R.Priyadarshiniproposes a solution to detect and prevent against malicious attacks over the developers web application written in programming languages like PHP, ASP.net and ASP also, it has created an API in native language through which transactions and interactions are sent to IDS server through inter server communication mechanism.IDS server is developed from PHPIDS.PHPIDS is purely a PHP based intrusion detection system which is mean to be used as server site tool. This paper detects and prevents attacks like SQLi ,lFI ,RFI and XSS types of attacks.Also the analysis of attacks is done using WAPT algorithm (Web Access Pattern Tree) which helps in recording the activities of web application and examines any suspicious behavior.

Rose Fonseca presents web applications in constant attacks by the hackers. In this paper a field study is presented on the attackers perspective by looking over real exploits used by hackers to attack web application.Results shows that SQl injection and remote file inclusion are the two most frequently used exploits and that hackers prefer easier rather that complicated attacking techniques.Root shell access and admin password are the main goals of attackers to obtain.A web application exploit may be as simple as a specially crafted URL or as complex as an automated program with hundreds of lines of code that can be compiled and executed.This field study analyses the exploits of six widely used and well known web applications such as PHP-Nuke,drupal, PHP-fusion, wordpressphpMyAdmin and phpBB.

Hugo F.Gonzalez covered attacking methods such as Remote File Inclusion, Cross Site Scripting and Code Inclusion.The principle vector of attacks or attackers are RFI.In this botnet involved in RFI attacks, the attackers are web server promised.The analysis of vulnerable site is done based on domain name, content and dynamic IP address.The tools used by attackers are contained by the hosterwhich is the host that have a web server or a FTP server.This paper mainly focuses on RFI attacks which means including other internet sites or directories in the same hard drive, this is great advantage for the programmer which neglected can result in a successful attack point and later compromising of the host.

III. LFI AND RFI VULNERABILITY

A. Local File Inclusion(LFI)

It is the process of including files that are already locally present on the server through the exploiting of vulnerable inclusion procedures implemented in the application. This application occurs ,for example when a page receives as input the path to the file that has to be included and this input is not properly sanitized, allowing directory traversal characters to be injected Since LFI occurs when path passed to "include" statement are not properly sanitized, in a blackbox testing approach we should look for scripts which take filename as parameter.

Consider the following example:-

http://vulnerable _host /preview.php?

file = exp.html

This looks as a perfect place to try for LFI. If an Attacker is lucky enough and instead of selecting the appropriate page from the array by its name, it is possible to include arbitrary files on the server.

Typical proof of concept would be to load password file-

http://vulnerable _host /preview.php?

file = ../../../../etc/pwd

If the above mentioned conditions not an attacker would see something like the following:-

Root:x:0:0:root:/bin/bash

Bin:x:1:1:bin: /bin : /sbin :/sbin /nologin

……

B. Remote File Inclusion (RFI)

RFI is an attack targeting vulnerabilities in web application that dynamically reference external scripts. The perpetrator's goal is to exploit the referencing function in an application to upload malware (eg. Backdoor shell) from remote URL located within a different domain.

In both cases, successful attack results in malware being uploaded to the targeted server. However unlike RFI LFI result aim to exploit insecure local file upload functions that fail to validate user suppliea/controlled input .

IV. METHODOLOGY

A. Dynamic Allocation Prevention method

Every page has entry stored in theHash table. In Dynamic allocation method; these entries get matched with the page which is dynamically entered. If both the entries get matched, user is allowed to procced .Else access denied for the user. This is the simplest kind of prevention method.

B. Sanitization of Input Prevention Method

Validation checks if the input meets a set of criteria. In Sanitization, it modifies the input to ensure that it is valid. So, in this method the contents are getting filtered and only the Sanitized code will be executed. This method is most promising as it allows only the non-vulnerable code to be executed ignoring all the vulnerabilities of it.

C. Digital Signature Prevention Method

A Digital Signature is a mathematical scheme for validating the authenticity of Digital message or document. In Digital Signature ,every page entered into hash table has provided an unique ID. If ID gets matched the user is allowed to proceed.

D. File size verification Prevention Method

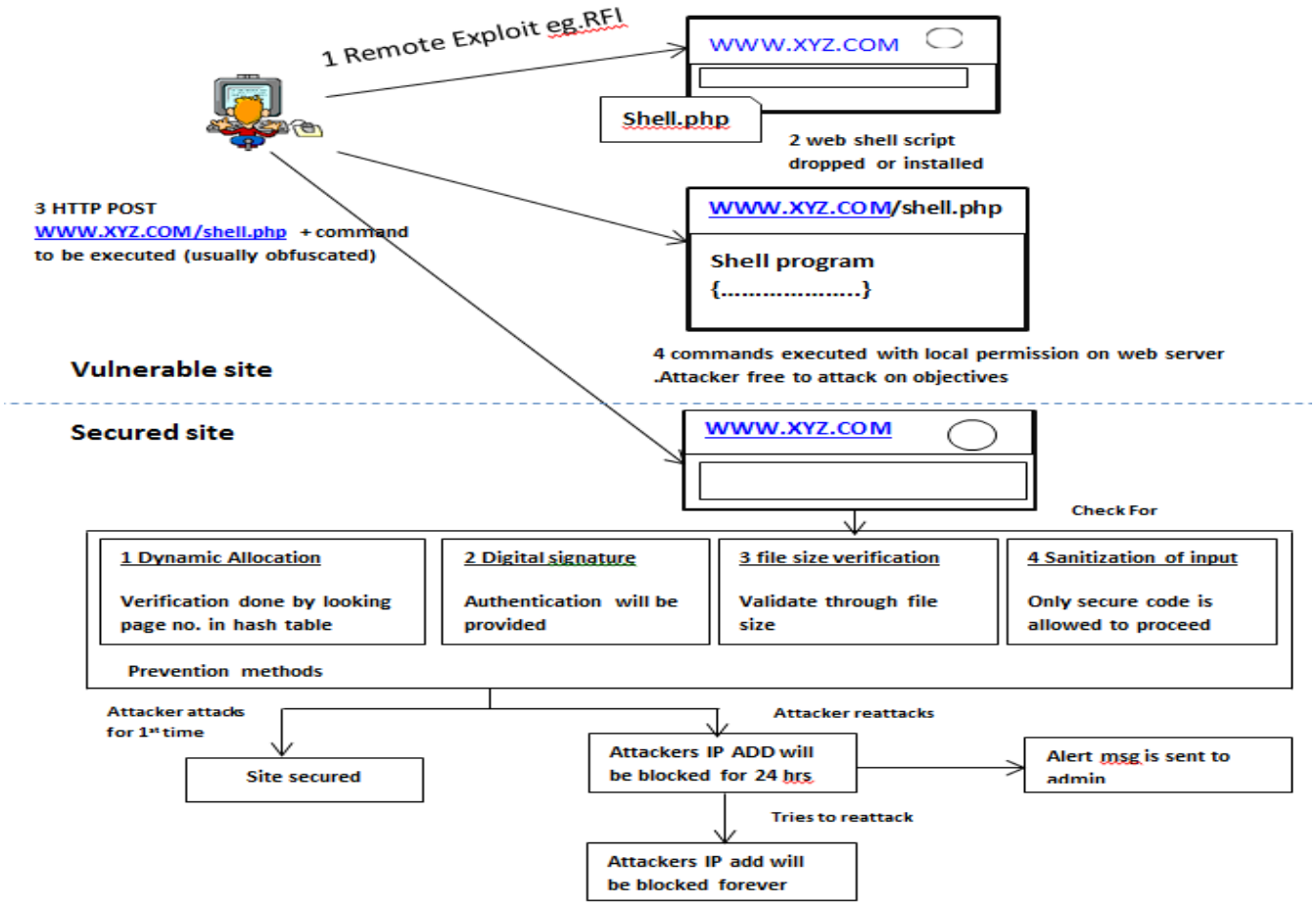
File size verification is a process of using an algorithm for verifying the integrity of file. In File size verification the input of file size is compared , this can be done by comparing two files bit by bit. But the only problem with this

method is, once in a while the file size can be matched though there are least chances of it. If we put the file size in bytes then there will be less chances of getting matched with the same file size.

V. ARCHITECTURE

This architecture consists of mainly two scenarios, the first scenario shows how exactly attack is performed. The second scenario shows, how system response when attacker tries to attack , and how it prevent from attacks by implementing prevention methods and what actions will be taken on attacker.

The below architecture shows detailed working of proposed system.



"Figure 1. Intrusion Detection and Prevention Architecture"

Basically two scenarios explain total working of the model. In first scenario,Attacker tries to inject malicious code into the page remotely. He might try to include the file or say code, where the code is vulnerable. After finding such weakness from the page the attacker is free to attack on the site , if attacker tries to include .php file into such place he will be succeed to have control on the server as the PHP code compiled directly from the server. Such kind of code is known as shell. In this scenario the attacker gains shell access.

In second scenario, it is shown how the system reacts when any user tries to access the particular site. Firstly, it will check for the prevention methods. It will compare the code or URL with each of the prevention method, if the data is corrected user is allowed to access the site. If the URL is not correct the user is not allowed to access the site as well as it might be considered as an attacker and alert message goes on server. So, the attackers IP

address will be blocked for 24hrs and the site will be secured. It might be possible that the URL which we are considering wrong is accidently put by the user. That's why users or we can say attackers IP has been blocked for 24hrs only. But, if the user/attacker tries to put such incorrected URL it is considered that he is trying to put malicious code on the site to harm the site or to gain unauthorized control. So in this case, attackers IP is blocked forever.

VI. CONCLUSION

The main goal of above survey paper is providing Prevention to website by various malware attacks. The attacks performed using LFI and RFI techniques will be prevented by this web application using different prevention methods like Dynamic Allocation method, Digital Signature method , verification of input and File Size Allocation , which will provide the security to the back end database system.

VII. REFERENCES

[1]Afasana Begum and Md. MarufHassan,"RFI and SQLi based Local File Inclusion Vulnerabilities in Web Applications",*International Workshop on Computational Intelligence(IWCI)*,12-13 Dec 2016.

[2]Rina Elizabeth Lopez De Jimenez*,"Pentesting on Web Applications using Ethical Hacking",ITCA-FEPADE,La Libertad*,30 June 2016.

[3]J.Jemmi Hazel and Dr. P.Valarmathie*,"Guarding Web Application with multi-angled attack detection",(ICSNS),*25 Feb 2015.

[4]MirSamanTajbakhsh and JamshidBagherzadeh*,"A sound framework for Dynamic prevention of Local File Inclusion ", 7th International Conference on Information and Knowledge Technology*,2015.

[5] NatasaSutevaand Mario Loleski*,"Computer Forensic Analysis Of some Web Attacks",(WorldCIS)*,2014

[6]Mr.R.Priyadarshini and Mr.Jagadiswaree*,"A Cross Platform Intrusion Detection System using Inter Server Communication Technique", IEEE-ICRTIT 2011 MIT, Anna University, Chennai.*June 3-5 2011

[7]JoseFonseca, Macro Vicira and Henrique Madeira*, "The Web Attacker Perspective-A Field Study", IEEE 21st International Symposium on Software Reliability Engineering* , 2010

[8]Hugo F.Gonzalez and Robeldo*,"Types of Hosts on Remote File Inclusion (RFI)", Electronics, Robotics and Automotive Mechanics Conference*, 2008

