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

IJCSMC, Vol. 4, Issue. 9, September 2015, pg.255 – 260

REVIEW ARTICLE

Web Vulnerability Scanner by Using HTTP Method

Harshala P. Patil[1], Prof. Promod. B Gosavi[2]

[1, 2] Godavari Foundation's Godavari College of Engineering, Jalgaon, Maharashtra, India

[1] harsh28_4@yahoo.com, [2] gosavi.promod@gmail.com

Abstract: - Today website security is the most important feature of securing an organization and should be given higher priority. Day by day hackers are mainly targeting on informative websites and web-based applications like forms, sensitive area like login pages, shopping carts, dynamic pages etc. Insecure web applications causes uploading backdoors on the server which allows access to databases, website hosted servers and also allow hackers to perform illegal activities using the host server like email spamming, proxy. A victim's website can be used for criminal activities, while illegally using website's bandwidth and making its owner liable for these unlawful acts. While developing the websites, many times developers/site owners forget to remove sensitive data from website which is not supposed to be exposed to public users. Such data consists of untested vulnerable forms, database backup, and site backup in compressed format. A hacker tries to search such kind of data and tries to collect important information from it like login detail from that data.

Keywords: Obfuscation detection, Web Application Security, Automated Vulnerability Detection, Automated URL Crawling, Content Management System, Threat Detection, Automated Web Security Audit.

INTRODUCTION

Website security is most important aspect nowadays for securing an enterprise and must have a priority in any organization. Gradually more, hackers are putting their hard work on web-based applications that are accessible 24/7 from anywhere in the world, web applications that are insure give easy access to backend databases also let hackers to make illegal activities by the attacked sites. An injured party website can be used to open criminal activities like hosting phishing sites or to transmit unlawful content, as abusing the website's bandwidth and making its owner

© 2015, IJCSMC All Rights Reserved

liable for these unlawful acts. The hacking are also very keen observer newly discovered web application intrusions, also known as Zero Day exploits, are posted on a number of forums and websites known only to members of that exclusive underground group. Postings are updated daily and also used to broadcast and help further hacking. Web applications are designed to permit your website visitors to retrieve and submit dynamic content including varying levels of personal and sensitive data. If the web applications are not secure, then entire database of sensitive information can be lost. Aim of this paper is to review results of current tools, their limitations, and strategic directions for future research on web application scanning methods.

Vulnerabilities in web application security such as cross-site scripting, SQL injection and cross-site request forgeries are recognized problems with thousands of vulnerabilities reported each year. These vulnerabilities let attackers to do malicious actions which range as of gaining unauthorized account access [1]. Obtaining sensitive data such as credit card numbers [2]. The web vulnerability scanner market has become a very active commercial space. Firewalls and SSL provide no protection against web application hacking, simply because access to the website has to be made public. Most web applications are custom-made and therefore, involve a lesser degree of testing than off-the-shelf software. Consequently, custom applications are more susceptible to attack [5]. Web application vulnerability scanners are automated tools that probe web applications for security vulnerabilities, without access to source code used to build the applications.

RELATED WORK

Much work and industry effort has been dedicated to Enhanced Web Security Scanner. Manual vulnerability auditing of all web applications is complex as well as lengthy it generally involves processing a large volume of data Common Vulnerabilities and Exposures database [6]. As well as it demands high level of skill and ability to keep track of large volumes of code used in a web application hackers are regularly finding new ways to exploit your web-vulnerability statistics [7] which means that you would have to constantly monitor the security communities, and find new vulnerabilities in your web application code before hackers discover them with vulnerability and detection rate [7]. Automated web application scanner can scan your web application, identify all the files accessible from the internet and simulate hacker activity in order to identify vulnerable components [4]. Automated vulnerability scanner can also be used to assess the code which makes up a web application, allowing it to identify potential vulnerabilities which might not be obvious from the internet, but still exist in the web application, and can thus still be exploited [3]. Study automated web vulnerability scanners, with the former targeting SQLI and XSS vulnerabilities and the latter utilizing user interactions to generate more effective test cases targeting rejected and stored XSS [8]. The vulnerabilities that current black-box scanners aim to detect and their effectiveness in detecting these vulnerabilities. Study of web application vulnerability scanners, number of "vulnerability demonstration sites", such as WebGoat by OWASP [9], and AltoroMutual [10], provide vulnerability education for website developers and for sales demonstration for scanner product capabilities.

SYSTEM

The system architecture is shown below how the system works we will see it in detail.

I. URL Crawling :

URL crawler is mainly used to crawl the URL's from the search engine. If we search any keyword using search engine the crawler will find the number web pages for that particular search. When we search any One keyword it can contains number of web pages and each web page has its URL but when we click on that URL it will again number of URL's for that one web page so we can say that it is been call recursively for one single search. So basically the URL Crawler is used to crawl the web pages for the particular search it will automatically crawl the URL's and will show limited URL's or web pages

© 2015, IJCSMC All Rights Reserved

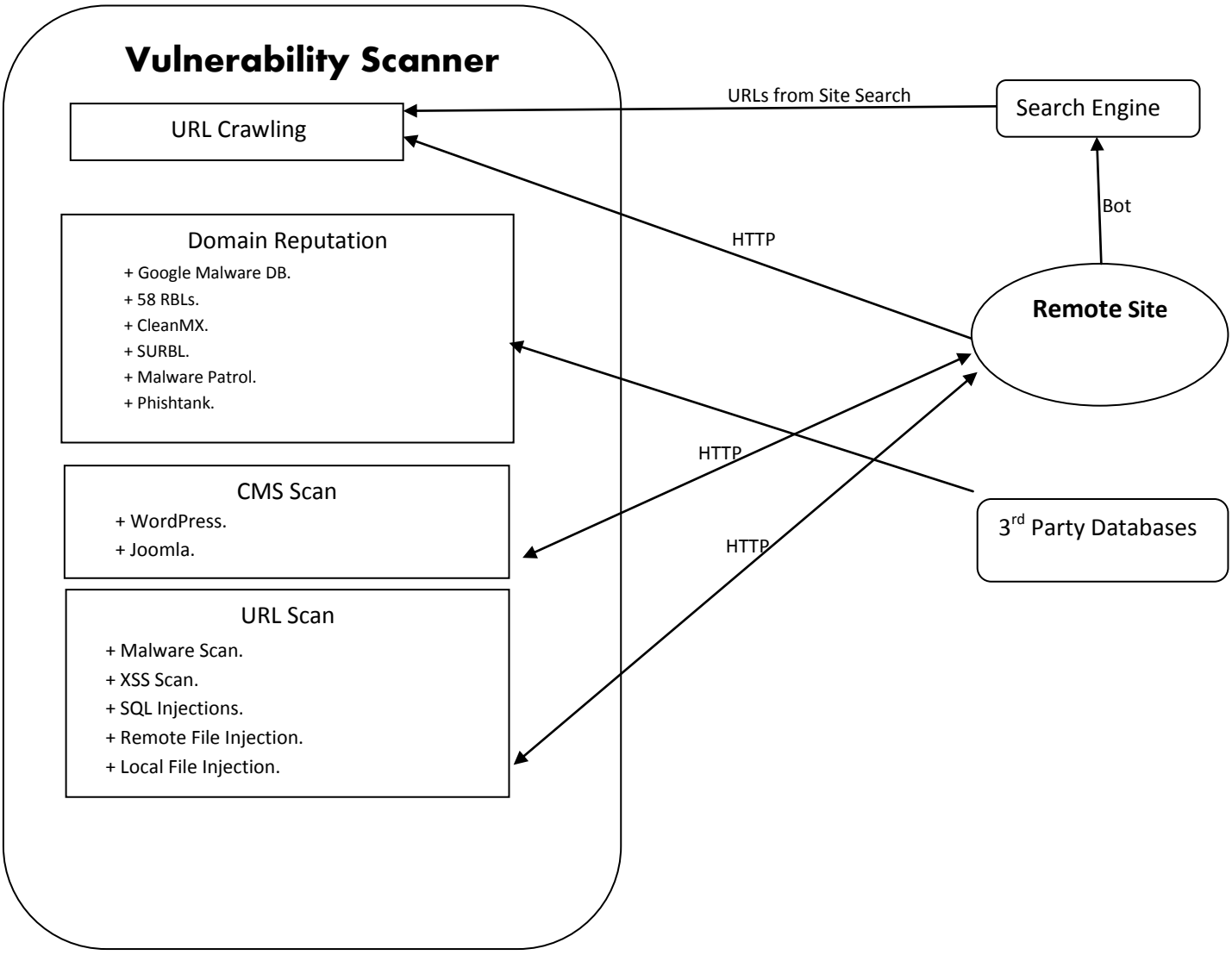
when we search any keyword the limit is given up to 6-7 web pages will show after we will search for the particular keyword.

II. Search Engine :

Search engine is mainly used for searching contents on the network here the system also used search engine for searching content various search engine are available now a days we are also using **Bing search engine** in the system for searching the contents so that the user can get the required data easily which they want. The search engine is mainly used for getting the limited data instead of getting huge number of data after applying the search.

III. Remote Sites :

When we apply search on search engine it will show us plenty of sites as our result. We get results from multiple sites and when we click on particular URL from that URL we again get multiple URL's means the sites are recursively called for this the directory traversal is used in the remote site so that the number of sites on a particular search will be appear.



© 2015, IJCSMC All Rights Reserved

IV. 3rd Party Database :

The 3rd party database is mainly used to check reputation of site and to check whether the site is corrupted. It checks if any site is black listed or not and if the site is black listed it gives the message for that it is mainly to check Vulnerability of black listed sites.

V. Domain Reputation :

Domain reputation is mainly used to check the black listed sites so that reputation for that site will check. Various domains are available for checking the reputation of sites different domains are listed in the system architecture. Domain reputation will check the vulnerability of sites using different domains mainly the RBL's are used to check mail server's IP and it checks whether the server's IP is black listed or not.

VI. CMS Scan :

Many tools are available to design the website and due to this easily available tool more changes are to cause Vulnerability. Tools like Joomla, WordPress are some example of CMS. In this the hackers check for the loopholes to detect Vulnerability. This tool are open source so it is easy for hackers to detect code also this kind of tools used specific type of format and this formats are easily available for the hackers and they detect Vulnerability easily.

VII. URL Scan :

The URL Scan is mainly done using two types of methods GET and POST. Using these two types of methods we check the Vulnerability for URL. For GET method a specific pattern is been define and for every URL these specific pattern is applied to check Vulnerability while in POST method no specific type of pattern is applied in this the whole URL is applied to check Vulnerability.

Rather than only checking for Vulnerability the system is a product which can be applied to detect Vulnerability and to solve that Vulnerability the advance part in the system is that the system is fully automated no manual work is required to do the system fully develop to be automated and anyone can understand it easily and use it. Due to automated design of system it will work fast and results will generated quickly.

FEATURES

The system has various features some of the features which the system includes are:

1. BackdoorWebShellLocater
   Scan for shells from client side machine for commonly injected locations and with their usual file names. Is the unique feature of the system which will be at client machine.

2. Domain reputation in Google, SURBL, Malware Patrol, Clean-Mx, Phishtank.
   Check whether domain is black listed with above databases. Above databases and organizations stores IP address of machine and domains which involves in malware, spamming, phishing activities.

3. Mail server IP Check in 58 RBL repositories.
   RBL (Real-timeBlack hole List) or DNSBL (DNS-based Black hole List) are list of IP addresses whose owners refuse to stop the explosion of spam. RBL usually lists server IP addresses from ISPs whose customers are responsible for the spam and from ISPs whose servers are hijacked for spam relay.

© 2015, IJCSMC All Rights Reserved

4. Scan SQL Injections for MySQL, MSSQL, PGSQL, Oracle databases.
   It is a trick that exploits poorly filtered or not correctly escaped SQL queries into parsing variable data from user input.

5. Scan XSS - Cross Site Scripting
   Type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. Detects form on the WebPages and scan for GET and POST requests.

6. Scan Malware
   Website defacement is an attack on a website that changes the visual appearance of the site or a webpage. Scans JavaScript code snippets against generic signatures it Checks for JavaScript dangerous functions like eval, base64_decode, char etc.

7. Detect and Scan CMS.
   Detect WordPress, Joomla, and vBulletine. Scan Themes, Plug-ins, unprotected admin area. User enumeration. Brut forcing for simple password detection.

8. Scan for Directory Indexing
   When a user types in a request for a page on a website, the web server processes the request, searches the web document root directory for the default file name, and then sends this page to the user. If the server cannot find the page, it issues a directory listing and sends the output in HTML format to the user.

CONCLUSION

Thus, studied the vulnerabilities of current scanner seek to identify their efficiency in detecting these vulnerabilities. And used different methods to detect vulnerabilities also tries to apply all this methods automatically so the work load will be less and vulnerabilities will easily detected different algorithm will be apply to detect the vulnerabilities for different methods. Different types of vulnerabilities are detected by different methods and required different methods to detect. Also study different web scanner available in market and trying to develop advance concept like automated tools to be used to detect vulnerabilities so that manual work will be reduce and results will be generated quickly.

ACKNOWLEDGEMENT

I am thankful to Prof. P.B Gosavi and HOD of computer department Prof. D.R Parthi for their valuable guidance and encouragement. I would also like to thank the Godavari College of Engineering, Jalgaon for providing the required facilities, Internet access and important books. At last we must express our sincere heartfelt gratitude to all the Teaching and Non-teaching Staff members of Computer Engineering Department who helped us for their valuable time, support, comments, suggestions and persuasion.

© 2015, IJCSMC All Rights Reserved

REFERENCES

[1] Strong Webmail CEO's mail account hacked via XSS. ZDNet. [Online]. Available: http://blogs.zdnet.com/security/?p=3514

[2] D. Litchfield. SQL Injection and Data Security Breaches. [Online]. Available: http://www.davidlitchfield.com/blog/archives/00000001.htm

[3] Software Assurance Tools: Web Application Security Scanner Functional Specification, National Institute of Standards and Technology Std., Rev. 1.0.

[4] Web Application Security Scanner Evaluation Criteria. Web Application Security Consortium. [Online]. Available: http://projects.webappsec.org/Web-Application-Security-Scanner-Evaluation-Criteria

[5] Acunetix Security. [Online]. Available: https://www.acunetix.com

[6] Common Vulnerabilities and Exposures. [Online]. Available: http://cve.mitre.org

[7] Web Application Security Statistics. Web Application Security Consortium. [Online]. Available: http://projects. Webappsec.org/Web-Application-Security-Statistics

[8] F. Maggi, W. K. Robertson, C. Krugel, and G. Vigna, "Protecting a moving target: Addressing web application concept drift," in RAID, 2009, pp. 2140.

[9] WebGoat Project. OWASP. [Online]. Available: http://www.owasp.org/index.php/Category:OWASP WebGoat Project

[10] AltoroMutual Bank. Watchfire Corp. [Online]. Available: http://demo.testfire.net/

© 2015, IJCSMC All Rights Reserved