International Journal of Future Generation Communication and Networking
Vol. 13, No. 2s, (2020), pp. 1190–1194

"Review:Developing a website analysis tool for vulnerability scanning and reporting"

Aishvarya Kadu[1], Bhagyashri Chalakh[2], Kanchan Gorle[3], Shivani Malpe[4]
Department of Computer Science and Engineering
Jhulelal Institute Of Technology
Session 2019-20

Abstract

There are several software package security assurance tools offered that detects and report vulnerability in web application sites .The growth within the range and size of websites will increase the necessity for higher securing those websites. Manual testing and detection of web vulnerabilities will be terribly time overwhelming. machine-driven web Vulnerability Scanners (WVS) facilitate with the detection of vulnerabilities in web applications. Acunetix[1] is one in all the wide used vulnerability scanners. Acunetix is additionally straightforward to implement and to use. The scan results not solely give the small print of the vulnerabilities, however conjointly provide info concerning fixing the vulnerabilities. AcuSensor and AcuMonitor (technologies utilized by Acunetix) facilitate generate additional correct potential vulnerability results. One in all the needs of this paper is to orient current students of laptop security with victimization vulnerability scanners. Secondly, this paper provides a literature review associated with security vulnerability scanners and also identifies a forms of vulnerabilities in internet application . This proposed work is going to be feature deep neural network to enhance the accuracy of vulnerability scanner. These can facilitate the website designer and therefore the user to scan and secure the website with high accuracy.

Keywords- *scanner, detection, website security, SQL injection, Web attack, Vulnerabilities, Exploits.*

I. INTRODUCTION

Vulnerability scanning is a security method used to identify security limitations in a computer system or websites. Vulnerability scanning can be used by individuals or network administrators for security purposes, or it can be used by hackers attempting to gain unauthorized access to computer systems or websites. Vulnerability Scanning is an inspection of the potential point of exploit on a computer on network, to identify security holes. A vulnerability Scan detects and classifies system weaknesses in computers, network and communication equipment and predicts the effectiveness of countermeasures. In vulnerability scanner machine learning algorithms are used and listed are as follows:

Naive Bayes: It is used for text classification. Using some key information that determines the characteristics of a text, it can automatically classify the text into several predefined categories. It is used in a spam filters.

ISSN: 2233-7857 IJFGCN

Q-Learning: It learns the best action of an agent. Using a behavior evaluation value called Q-value, a behavior of the agent is evaluated in a given environment, and by evaluation the agent is able to learn the optimal action. It is used for robots to learn human walking motion.

Now a day's web application is more important part of our lives. Every day millions of people use web application. A modern web application is composed of a back-end and server side parts. So many web applications are developed in Java Script, PHP, HTML, Ruby or Python. Number of attackers attack on web application. Generally attackers attack on web application code by using SQL injection and XSS (cross site scripting). Most business is conducting their business communications and transactions online. However, these websites and web applications are not completely secure. Around 30,000 websites are being attacked every day and third party websites are vulnerable to hacking. Web security scanners are automated tools and check out the web applications for security vulnerabilities, without accessing the applications source code. Networks Scanning involves identifying which hosts that are alive in the computer network which operating systems that they use, and what services they run. During the vulnerability Scan a database of vulnerability signatures is compared to the information obtained from a network scan to produce a list of vulnerability that is presumably present in the network. Detecting Vulnerability for a network is an important procedure which ensures that all the data, network-based applications and information communicated in this network is secure.

The discovering security vulnerabilities in web applications are by observing the applications output in response to a required input. This method of analysis is called black-box testing. Classical black-box web vulnerability scanners scrolling a web application to enumerate all reachable pages and then fuzz the input data (URL parameters, form values, cookies) to trigger vulnerabilities. In this paper, we propose to improve the effectiveness of black-box testing, SQL injection and XSS web vulnerability scanners by increasing their capability to understand the web application's internal state. Web vulnerability scanners help to find vulnerabilities of web applications and websites.

II. LITERATURE SURVEY

In this section came the web application attacks, counter measures of attacks, aware black box web vulnerability, and study of vulnerability scanning tool Nesses, Acunetix-Web Vulnerability Scanner, OWASP Zed Attack Proxy (ZAP), HTTP, Vulnerability scanner. We discuss some paper below.

[1]Nessus

The latest version of Nessus is 5.2.5. Nessus[2] is one of the popular vulnerability scanners. It allows scans for misconfiguration for the software that installed in the machine. It is also include detecting open ports of the machine and version of the software installed in the machine. Other than that, it also scans vulnerabilities that allow a remote hacker to control or access sensitive data on a system, denials of service against TCP/IP stack and PCI DSS audits. This is also including web application scanning; for example to detect SQL injection and cross site scripting. Nessus has come out with two versions of the release; Home Feed release and Professional release. For vulnerability reporting purposes, the Nessus scanning result can be exported to several types of file for example HTML and CVS. The organization had used Nessus since the year 2010.

[2] Acunetix-Web Vulnerability Scanner

Acunetix[1] is web application vulnerability scanning. Web Vulnerability Scanner is a web application scanning tool that can detect vulnerability for example SQL injection, cross site scripting, flaws in the

ISSN: 2233-7857 IJFGCN

underlying operating system and misconfiguration of the web server. Acunetix also able to perform advanced penetration testing tool and testing for the password protected area. It also can detect port scanning. Acunetix runs on Windows operating system; the minimum is XP. For reporting purposes, Acunetix results can be export to PDF format file. Acunetix has came out with two different versions; Professional and trial version.

[3]OWASP Zed Attack Proxy (ZAP)

Zed Attack Proxy (ZAP)[1] is a freeware vulnerability scanning tool. It was developed by Open Web Application Security Projector OWASP. OWASP ZAP Project or also known as Zed Attack Proxy is an integrated penetration testing tool for finding vulnerabilities in web applications. ZAP is an open source tool that runs either on Linux or Windows platform. It also supports multiple languages, for example French, Spanish and Arabic. The example of the vulnerability that able to detect by OWASP ZAP is HTTP Parameter Pollution (HPP) extension and SQL injection.

[4] Web Vulnerability Scanner by Using HTTP Method

Web vulnerability scanner by using HTTP method basically works on URL crawling, Search engine, Remote Site, third party database and domain reputation. This vulnerability scanner scan URL and CMS. It scan for shells from client side machine for commonly injected location and with their usual file names. It also check mail server IP. Scan SQL injections for MySQL, MSSQL, PGSQL and Oracle database. It is trick that exploit poorly filtered or not correctly escaped SQL queries. It also scan XSS, Malware and directory indexing. but the vulnerabilities of this scanner seek to identify their efficiency in detecting different vulnerabilities.

[5] SecuBat-A web vulnerability scanner

SecuBat[4] is a web application is used to find web vulnerability. Example of such vulnerability are SQL injection and cross site scripting(XSS). Using SecuBat identified a large number of potential vulnerable website. Also SecuBat discover web vulnerabilities that could be use to launch phishing attacks that are difficult to identify even by technically more sophisticated users. SecuBat has crawling component to determine the door of attacks and four attacks are used.

1) Form redirecting XSS attack
2) SQL injection
3) Simple reflected XSS attack
4) Encoded Reflected XSS attack

PROPOSED WORK

Our vulnerability scanner tends to replace the existing vulnerability scanners for the scanning process which is a time consuming, less interactive and highly expensive. The main features of this vulnerability scanner and reporter will be creating report and find various types of vulnerabilities, storing Scanning data, process initiation, and after that it generates a report of whole scanned websites. Advantages of the Proposed work are User friendly UI design, fastest Crawler, and fastest scanner Search for a particular websites if once it is used.

Web vulnerability scanner has proposed such as the following:

- Maintenance of an up-to-date report of vulnerabilities.
- Detection of genuine vulnerabilities without an excessive number of false positives.
- Ability to conduct multiple scans simultaneously.
- Ability to perform trend analyses and provide clear reports of the results.

ISSN: 2233-7857 IJFGCN

- Recommendation for countermeasures to eliminate discovered vulnerabilities.

ISSN: 2233-7857 IJFGCN

IV. CONCLUSION

We plan to develop vulnerability scanner and reporter for web application. In the previous work website scanning is done with the help of document scanning techniques.
This proposed work focuses to add deep neural network to improve the accuracy of vulnerability scanner. This paper surveys about different web application scanner and some important security properties of web application. Reports from different scanners produce different test results/report which reduces the vulnerability of web application. A good scanner should find as many numbers of vulnerabilities as possible. The main problem with Web scanners is that most of them give false positives results. A good scanner should avoid reporting false positives as much as possible. A single vulnerability opens a door for many attacks. False positives are hard to resolve so testers have to waste a lot of time to test manually and identify the vulnerabilities.

REFERENCES

1. Abdulqader, F. B., Thiyab, R. M., & Ali, A. M. (2017). The impact of SQL injection attacks on the security of databases. In Proceedings of the 6th International Conference on Computing and Informatics (pp. 323-331).
2. Kirti randhe, “Security Engine for prevention of SQL Injection and CSS Attacks using Data Sanitization Technique", IJIRCCE, 2015.
3. J. Fonseca,N. Seixas, M. Vieira, and H. Madeira, “Analysis of Field Data on Web Security Vulnerabilities", IEEE Transaction on dependable and secure computing, vol. 11, no. 2, march/april 2014.
4. Jose Fonseca, Marco Vieira, and Henrique Madeira, “Evaluation of Web Security Mechanisms Using Vulnerability and Attack Injection", IEEE transaction on Dependable and secure computing, Vol. 11, No. 5, 2014
5. Zoron Djuric, “Black Box TestingTtool for Detecting SQL Injection Vulnerabilities", IEEE, 2013.
6. Abdul Razzaq, Khalid Latif,H.Farooq ahmad, Ali Hur, Zahid anwar and Peter Charles Bloodsworth, "Semantic security against web applicationattacks", ACM, 2013.
7. Nilima R. Patil and Nitin N. Patil, April, 2012. “A comparative study of network vulnerability analysis using attack graph”, in Proceedings of National Conference on Emerging Trends in Computer Technology (NCETCT-2012) .
8. Peng Li and Baojiang Cui, December, 2010, “A Comparative Study on Software Vulnerability Static Analysis Techniques and Tools”, in Proceedings of the IEEE International Conference on Information Theory and Information Security (ICITIS), pp.521-524.
9. Nilsson J., 2006, “Vulnerability Scanners”, Master of Science Thesis at Department of Computer and System Sciences, Royal Institute of Technology, Kista, Sweden
10. H.S. Venter, J.H.P. Eloff, (2004), Vulnerability forecasting –a conceptual model, University of Pretoria, SA, Department of Computer Science.
11. Oleg Sheyner, Joshua Haines, Somesh Jha, R. Lippman and J. M. Wing, May, 2002. “Automated generation and analysis of attack graphs”, in Proceedings of IEEE Symposium on Security and Privacy.

ISSN: 2233-7857 IJFGCN