Template Based Vulnerability Scanner

Tejas Jadhav[1], Gaurav Popalghat[2], Kiran Marne[3], Sayyed Kashifali Parvejali[4]
[1,2,3,4]*Department of Information Technology, SKN Sinhgad Institute of Technology and Science, Lonavla*

Abstract: In today’s world, Cyber security has become an essential leap in the form of jobs and education. But the reality is that only a few are aware of the significant web vulnerabilities. Some statistical studies show that small-scale industries are directly and indirectly connected to the Internet. Still, they are not aware of the substantial web vulnerabilities of their web application. Since website hosting has become common nowadays, most web applications are prone to attacks and malicious attacks of web applications. Assessing and avoiding these vulnerabilities requires deep knowledge of these vulnerabilities. There are numerous online scanners available on the Internet that provide only paid limited service. The tools are made in a way that they can only operate in a command line interface or any programming language. So, it is difficult for an average person to use the scanners without previous knowledge. This paper presents a vulnerability scanner that scans the website and detects specific vulnerabilities, along with its location and solution.

Keywords - Vulnerability, vulnerability assessment, Shodan, Nessus, Burp Suite, National Vulnerability Database.

1 INTRODUCTION

Web applications have become integral to everyday life, but many are associated with vulnerabilities. In this era, where website hosting has become cheap and easy, security still needs to catch up. Such vulnerabilities can risk small-scale to large-scale industries. The exploitation of vulnerability by an An Unauthorized person demands quick recovery of these flaws so that reputation of the organization can be recovered. Therefore, vulnerability scanners can widely evaluate a website's known weaknesses and vulnerabilities. Many applications are becoming online, but how secure these applications are is a matter of concern. Thus, finding vulnerabilities that may cause severe risks to users' security becomes necessary. Vulnerability assessment means detecting the vulnerabilities before an attacker can use them. It is not only performed on a particular application, but it can be run on any platform on which the application is run. This strategy only considers all the factors that can provide the correct answer for the assessment of the vulnerability and security of the system. Therefore, vulnerability scanners are used to scan the network and software application.

2.RELATED WORKS

A. Various Vulnerability Scanner: A Survey

- Acunetix Vulnerability Assessment Engine: It's an entire web application security testing solution that will be used alone and as a part of complex environments. It offers built-in vulnerability assessment and vulnerability management, also as many options for integration with market-leading software development tools. It is not an opensource tool. It is the most expensive tool available.
- Burp Suite Web Vulnerability Scanner: Burp Scanner uses PortSwigger’s world-leading research to automatically assist its users in automatically hunting out an honest range of vulnerabilities in web applications.
- Qualys Web Application Scanner: WAS’ dynamic deep scanning covers all apps on your perimeter, in your internal environment and under active development, and even APIs that support your mobile devices. It also covers public cloud instances and provides instant visibility of vulnerabilities like SQLi and XSS.

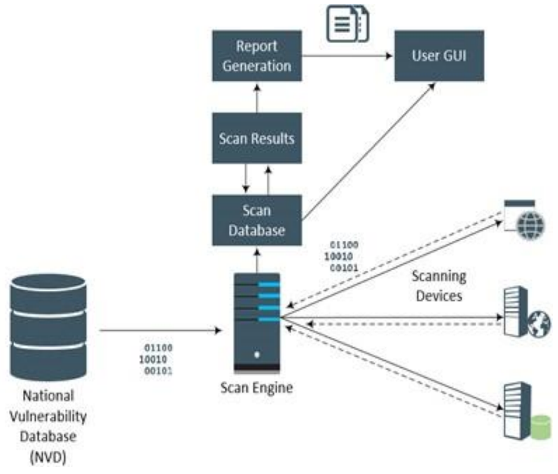
3.MECHANICS OF A SCANNER

The mechanics of a scanner is a three-step process, crawling, simulation of attacks (fuzzing) and response analysis. In the first step, the scanner crawls into the web application that is part of the application and associated input pages and makes an index of all the visited pages. If the crawling mode is poor and the scanner has yet to reach the vulnerability, the scanner will surely miss the vulnerability. The scanner sends some attacking patterns to the previously identified inputs in the fuzzing step. For each information and each exposure for which the scanner tests, the attacker module generates values that trigger the vulnerability.

In the response analysis phase, the result of the fuzzing stage is monitored to check if the web application is vulnerable and provide feedback to other modules. In the past, many popular websites have been hacked. Attackers are active now and exploit the data without the user's knowledge. That is why the security of web applications has become essential these days. Web application security scanning is a software program that tests the web. applications and identifies security vulnerabilities. The scanner does not scan the source code, but they only detect the vulnerabilities.

4.PROPOSED METHOD

With the increasing development of the internet, web applications have become increasingly vulnerable and are exposed to unauthorized attacks. Many online scanners are available in the market to deal with this problem. But most of them can only detect some of the vulnerabilities publicly. If a situation arrives where the scanner, we use cannot see the vulnerability, then the attacker can easily crawl into the system and exploit the data and resources. Our proposed method is a vulnerability scanner which detects vulnerabilities like SQL injection, cross-site scripting, broken authentication [8], payload, and email disclosure. The vulnerability scanner scans the website and checks whether the above vulnerabilities are identified while reviewing. Fig-1 shows the overall design of the vulnerability scanner. The scanner is available as either a mobile or web application. The user can submit the URL in the application, where the scanner will crawl into the URL to check for the sub-URLs. The scanner then identifies whether the vulnerabilities mentioned earlier are present in the URL.



5.OTHER SPECIFICATIONS

A. Advantages

- Supports automated and reliable crawling.
- Optimized use of the number of threads to control the load on the target application.
- Detailed vulnerability analysis.
- User-friendly GUI.

B. Limitations

- Model can currently handle non-CAPTCHA registrations and logins.
- Possible to detect first-order SQL Injection and XSS vulnerabilities through automated scanning.
- Current focus is on small to medium-sized web Applications.

C. Applications

Identifying and reporting vulnerabilities present in a web application.

6.CONCLUSION

The results of our comparative evaluation of the scanners confirmed again that scanners perform differently in different categories. Therefore, no scanner can be considered an allrounder in scanning web vulnerabilities. The above-proposed scanner is best suited for beginners who need to be aware of the complex scanning steps. Vulnerability scanning identifies the security vulnerabilities in an organization. Vulnerability assessment provides the organization with the awareness and risks associated with the organizations working environment and work accordingly. The advantage of using a vulnerability scanner is that it identifies known security exposures before attackers find them.

REFERENCE

[1] Hannes Holm, Teodor Sommestad, Jonas Almroth, Mats Persson"A quantitative evaluation of vulnerability scanning." 2016.

[2] Binny George1, Jenu Maria Scaria1, Jobin B1, Praseetha VM2."Web Application Security Scanner for Prevention and Protection against Vulnerabilities" 2020.

[3] Prajakta Subhash Jagtap 1M.Tech Student 1K J Somaiya College of Engineering. "Vulnerability Scanning ." IJEDR 2020.

[4] Pranav Gadekar, Samruddhi Kulkarni, Shalaka Kulkarni, Shruti More "Automated Web Application Vulnerability Scanner" IJERCSE 2021.

[5] Yongjun Xia1, a, jin Wang1, b, Chang Liu1, and Kaiming Yu "Design and Implementation of Vulnerability Scanning Tools for Intelligent Substation Industrial Control System Based on Openvas" ESMA 2019