International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

Testing Web Application using Vulnerability Scan

Trupti Bhosale[1], Shraddha More[2], Prof. S.N. Mhatre[3]

[1,2]Student, Information Technology, BVCOE, Navi Mumbai, Maharashtra India
[3]Professor, Information Technology, BVCOE, Navi Mumbai, Maharashtra India

---

Abstract - : *A vulnerability is a hole or a weakness in the application, which can be a design flaw or an implementation bug that allows an attacker to cause harm to the stakeholders of an application. There are many types of vulnerabilities in web application, each of which can be the target of web attack SQL injection and Cross-Site Scripting attack is a main-stream approach of web attacks. Our approach is mainly based on SQL Injection Detection method and Cross Site Scripting detection method with a crawling technique. Firstly, a user will enter an URL for checking vulnerability and click on the 'Start' to start the scanning process. After clicking on start, application start crawling for SQL injection vulnerability and Cross Site Scripting. If any vulnerability occurs it will generate in the spider log. And this detected vulnerabilities will be generated by a report so the user will get clear idea about weakness in the application.*

Key Words*: *Vulnerability Scanning, SQL Injection, XSS Attacks

1. INTRODUCTION

A vulnerability is a hole or a weakness in the application, which can be a design flaw or an implementation bug that allows an attacker to cause harm to the stakeholders of an application .Stakeholders include the application owner, application users, and other entities that rely on the application. Vulnerability scanning can be used either to find holes or plug them before they are exploited or to find holes and exploit them. There are many types of vulnerabilities in web application, each of which can be the target of web attack. SQL injection and and Cross-Site Scripting attack is a main-stream approach of web attacks. SQL injection attackers make use of the absence of data legitimacy judgment of the user input in a web application and may obtain administrator privileges with a carefully constructed SQL statements to insert special characters and commands and attack the back-end database through the input areas of web pages (such as URL, forms, etc.). Therefore, in order to ensure the security of web applications, web vulnerability scanner which is used for detecting and digging out the SQL injection vulnerability has become an essential part of network security. Through analyzing a lot of web pages from many business sites, we find that web pages has a high similarity of structure in the same directory. Therefore, on premise of ensuring a certain accuracy of vulnerability scanning, just crawling some of the pages in the same directory for testing can reach the goals of improving detection efficiency in web vulnerability scanning.

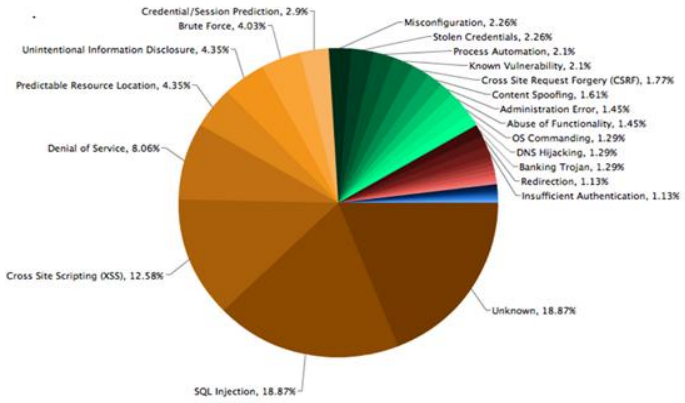


Fig.1.1 Different types of attacks

Based on the above research we propose a novel efficient web vulnerability scanning method which randomly crawls a certain number of pages in the same directory of one site. We calculates the similarity of those web pages, if the similarity reaches a certain threshold, we will acknowledge the fact that the directory pages are generated by the same template and stop crawling other pages.

1.2 LITERATURE SURVEY

Vulnerability scanning can be used either to find holes or plug them before they are exploited or to find holes and exploit them. There are May tools are exist for detecting vulnerabilities:

1.2.1 NIKTO WEB SCANEER

This is a Web server scanner that tests Web servers for dangerous files/CGIs, outdated server software and other problems. It performs generic and server type specific checks. It also captures and prints any cookies received. The Niko code itself is Open Source (GPL), however the data files it uses to drive the program are not.

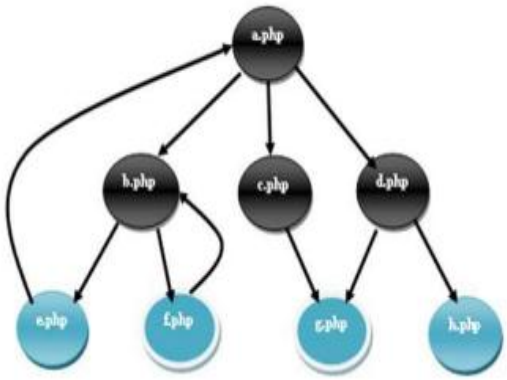
1.2.2 NMAP

This tool is used to discover hosts and services on a computer network , thus building a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host(s) and then analyzes the responses. The software provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. In Cross Site Scripting, there are following types for XSS would be occur while detecting vulnerabilities.

2. SYSTEM METHODOLOGY

2.1 Crawling the whole web application

For finding the input points we first explore the whole web application. In order to examine the entire web application it is designed in the form of a tree. Figure shows the tree structure of web application where a.php is the home or index page and the other pages are child nodes. After construction of the tree the pages are visited all the links are displayed in the working log.



2.1 Scanning attack

By sending different specially crafted attack request the proposed scanner checks if SQL injection and XSS vulnerabilities lie in a web application or not. For checking vulnerability we have defined a payload setup in which we have stored the attacks pattern related to different injection attack. We generate the attack request by appending attack pattern with the URL. After putting the attack request our tool automatically checks the response if there exist any vulnerability or not. If any vulnerability is found in the content of the response page then we can say that vulnerability exists in the input point of this page. Suppose in Sql injection, user name (user Name) by invoking request.getParameter("name")and uses it to construct a query to be passed to a database for execution (con.execute(query)). If an attacker has full control of string username obtained from an HTTP request, he can for example set it to 'OR 1 = 1; −−. Two dashes are used to indicate comments in the Oracle dialect of SQL, so the WHERE clause of the query effectively becomes the tautology name = '' OR 1 = 1. This allows the attacker to circumvent the name check and get access to all user records in the database.

2.3 Generating Report.

If any vulnerability exists in the web application, then a pdf report is generated indicating the date and time, the domain name and the SQL and XSS attacks found in tabular form.

3. PROPOSED SYSTEM

We are making a java based tool to scan the vulnerabilities of SQL Injection and XSS attacks. At the very first stage user need to enter URL for checking vulnerability. After this tool crawl each and every page of web application. Then tool will determine which type of attack is possible on particular line. Vulnerabilities attacks will be reported at the users host for further use. This tool make use of various SQL attack algorithms like Blind SQLTest ,Error based test, SQL Union Finder with their various types and XSS Attacks algorithm.

3.1 IMPLEMENTATION

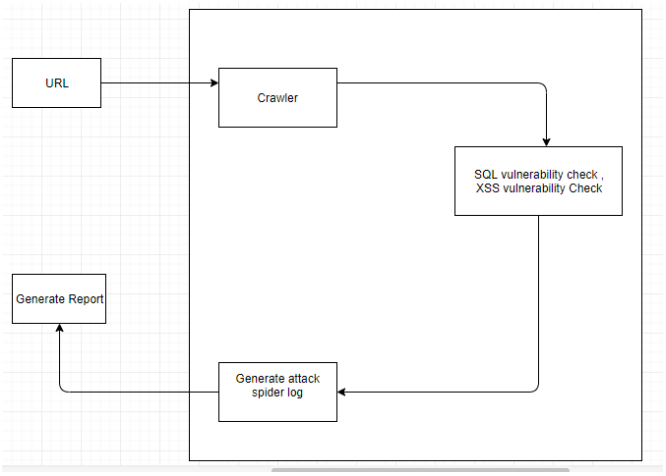


Fig.4.1 System Architecture diagram

4. CONCLUSIONS

As a conclusion, vulnerability scanning is a good process where all organizations should implement it in their daily working process. They can use any tool available out there. The organization needs to identify which one is suitable for them based from certain factor; the purpose of the scanning, cost, ease of use and software support.

In future, the organization still needs to do some research about the other potential tool that can be used for vulnerability scanning. It is important so that we can update ourselves to the latest technology out there

REFERENCES

[1] https://ieeexplore.ieee.org/document/6918247

[2] https://ieeexplore.ieee.org/document/7562694?reload=trues

[3] https://www.owasp.org

[4] Andrey Petukhov and Dmitry Kozlov, "Detecting Security Vulnerabilities in Web Applications Using Dynamic Analysis with Penetration Testing", Dept. of Computer Science, Moscow State University.

[5] OWASP Foundation, 2007, http://www.owasp.org/index.php/Top_10_2007

[6] http://cwe.mitre.org/documents/vuln-trends.html

[7] Dafydd Stuttard , Marcus Pinto "The Web application Hacker‟s Handbook Finding an Exploiting Security Flaws " second edition ©2011

[8] Xin Wang, Luhua Wang, Gengyu Wei, Dongmei Zhang and Yiqian Yang, "Hidden Web Crawling For Sql Injection Detection ", Beijing University of Posts and Telecommunications, Beijing, China. 978-1-4244-6769-3/10/$26.00 ©2010 IEEE,p.- 14-18.

[9] Nuno Antunes and Marco Vieira , "Defending against Web Application Vulnerabilities", University of Coimbra, Portugal, 0018- 9162/12/$31.00 © 2012 IEEE, vol.-2,p.- 66-72.