JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

An Automatic Vulnerability Scanner for WebApplications with Firewall Techniques

Rathod[1], S.K. Jagtap[2], J.R. Satpute[3], A. P. Shikhare[4], K.A. Pujari[5], A.S. Pandit[6]

Department Of E&TC Eng., Smt. Kashibai Navale College of Engineering, SPPU, Pune, Maharashtra

[1]vishalr7757@gmail.com [2]skjagtap.skncoe@sinhgad.edu [3]rsatpute341@gmail.com

[4]shikhareamruta9@gmail.com [5]kapujari.skncoe@sinhgad.edu [6]anuradha.pandit_skncoe@sinhgad.edu

***Abstract*— The web applications are integral part of our day-to-day life. Almost everything is stored and manages on web. Web applications are designed for personal, commercial, and social purpose also. This omnipresence of web application makes them vulnerable. The increasing dependency on web applications have made them natural target for attackers. Injection attacks are most dangerous. To detect these vulnerabilities many researchers, develop different approaches. This paper elaborates existing web vulnerability detecting approaches with their advantages and disadvantages. Clustering approach has approached to efficiently detect the SQL Injection, Xpath Injection and Cross Site Script-Ing attacks ranked by OWASP (Open Web Application Security Project) community. The objective is to improve detection efficiency of vulnerability scanner while maintaining low false positive and false negative rate.**

***Keywords*— Vulnerability, Vulnerability Scanner, Owasp, Web Security, Web Application, GitHub, Infosec**

I. INTRODUCTION

Vulnerability scanners scan systems for known vulnerabilities, also looks for outdated components of operating systems and applications that are known to have security vulnerabilities. In other words, system look for software versions that have known bugs. Depending upon the access of the vulnerability scanner, it can also potentially find configuration errors, such as improper file sharing and similar issues. There are network-based vulnerability scanners that scan systems which sit on a network. Scanner can detect the vulnerabilities that are exploitable by network-based attacks. There are managed services available, such as Qualys and Tenable, that perform regular scanning. There are also vulnerability scanners that run on individual systems and can do an extra level of scanning to find vulnerabilities that can be exploited by someone with system accesses. Complete web vulnerabilities scanner is used to find the websites bug and after that it shows the types of bugs on that website. This project is developed by using python. There is an ever-increasing number of high-profile data breaches have plagued originations over the past decade. A great number of these cone about via so called 'injection's attacks'; the submission of malicious code to a web application. Indeed, the Open-Source Web Application Security Project (OWASP), the leading organization in the field of web app security states; 'How data input is handled by Web applications is arguably the most important aspect of security. Two factors increase the stakes of cyber struggle. Tactically and operationally, the increasing dependence of modern technologically advanced forces on networks and information create new kinds of exploitable variabilities. Second, as redeem societies including the militaries that min-or them have continued to evolve, they have become ever more dependent on a series of interconnected, increasingly vulnerable "critical infrastructures" for their effective functioning. These infrastructures not only have significantly increased the day-to-day of almost every part of our society, but system have also introduced new kinds of vulnerabilities.

II. LITERATURE SURVEY

Haibo Chen with co-researchers Junzuo Chen, Jinfu Chen, Shang Yin, Yiming Wu introduced the Open Web Application Security Project (OWASP) has summarized the top 10 web security vulnerabilities Among them, the most common and harmful vulnerabilities are the SQL injection and the cross-site scripting (XSS).[5] Zoran Djuric introduced the method to detect SQLI is attack against a database-driven web application, in which the attacker attempts to change the semantics of the original SQL statement. This is done by inserting new SQL keywords.[6] Until now the web continues to grow both in terms of the number of users and in terms of the technology used. Along with that there has also been an increase in attacks on the web. The attacks on the web cannot be separated from the vulnerabilities that exist on the web. As a first step, use of two open-source tools to scan for web vulnerabilities, OWASP ZAP and RIPS. In addition to these two tools, several other methods have been found to improve the accuracy of the scanning results, in this paper we review the article about scanning for vulnerabilities found on the web and solutions to eliminate them. We use the SLR method according to Kitchenham and Charters to review articles about web security

and vulnerabilities. After this literature survey we have automated the whole vulnerability detection process and firewall by passing techniques to bypass filtered open ports.

III. METHODOLOGY

A Here start with basic understanding of web application and its evolution history. It helps us to better understand all web attacks and its security. Also, it is equally important to understand the complexity of web applications are increasing day by day as their role in people lives increases rapidly. At the starting stage of web development static HTML was used to transform information and display pictures. But in later part as the people accessing Internet and web ubiquitously, it is difficult to satisfy the needs of the users who were accessing web applications. Therefore, as a solution to above problem evolution of web applications took place to satisfy the users by providing user conveniences such as searching, posting, and uploading. CGI, Common Gateway Interface protocol was the first standard environment which used to generate dynamic web pages. Usually, this CGI resides on a server, initially the browser send data to the CGI program on the server. According to the CGI specification HTML form data is packaged and sent in the HTTP request to the server. By using CGI mechanism users invoke a program on a web server. When a website uses CGI processing for communication, this is called web application. Therefore, GGI is the first technique which attacker used to perform attacks. Web application development evolved Ruby on Rails, ASP.NET, J2EE, PHP, AJAX, and others frameworks and standards for more effective interaction after CGI scripts. These all allow users more flexible and powerful solutions for transferring and managing data within web applications. Therefore, it is important to use secure web applications as the information processed and stored by web applications has become critical to corporations, customers, organizations, and countries. This ubiquity of web applications has made them natural target for malicious minds to perform web attacks. Web attacks are nothing but malicious act performed by the attacker to gain unauthorized data. Following sections briefly describes SQL Injection, Cross Site Scripting and X-path Injection. Web attacks are nothing but malicious act performed by the attacker to gain unauthorized data. Following sections briefly describes SQL Injection, Cross Site Scripting and X-path Injection.

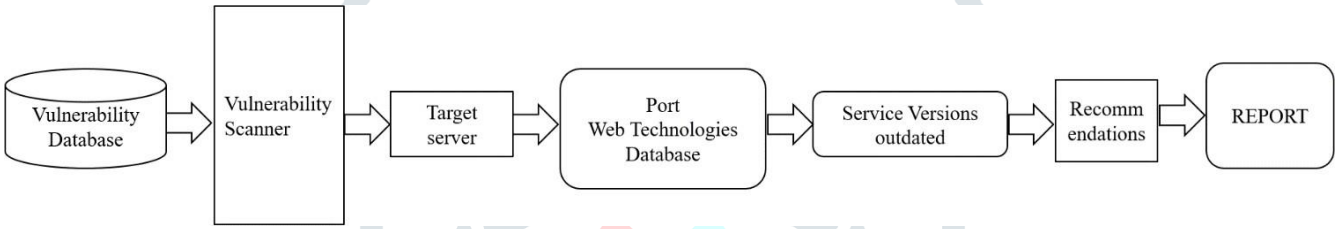


Fig.1 Block Diagram of the System

Vulnerability database is a collection of CVES of existing vulnerabilities and loop holes present in various application software's, operating system and servers. It will contain automatic signatures-based detection. All discovered vulnerabilities have assigned a CVE number. CVE, short for Common Vulnerabilities and Exposures, is a list of publicly disclosed computer security flaws. When someone refers to a CVE, they mean a security flaw that's been assigned a CVE ID number. Vulnerability Scanner in this block vulnerability scanning takes place. Vulnerability scanning is the process of discovering, analysing, and reporting on security flaws and vulnerabilities. The scanning process includes detecting and classifying system weaknesses in networks, communications equipment, and computers. In addition to identifying security loopholes, the vulnerability scans also predict how effective countermeasures are in case of a threat or attack. Vulnerable Server can be a name, a host, a port, an application, a database with an additional element to indicate whether the Target Server is enabled or disabled. Ports are an integral part of the Internet's communication model. All communication over the Internet is exchanged via ports. Every IP address contains two kinds of ports, UDP and TCP ports. The term open port refers to a TCP or UDP port number that is configured to accept packets. In contrast, a port that rejects connections or ignores all packets is a closed port. Web technologies are the various tools and techniques that are utilised in the process of communication between different types of devices over the internet and methods by which computers communicate with each other through the use of markup languages and multimedia packages. Browsers. Browsers request information and then they show us in the way we can understand. HTML & CSS. HTML is one of the first Web Development Frameworks, Programming Languages, Protocols, API Data formats, Client and server. Database contains SQL database which has parameters like username, address, password, port name, location, comment and data types. SQL injection vulnerabilities occur when application code contains dynamic database queries which directly include user supplied input. This is a devastating form of attack and BSI Penetration Testers regularly find vulnerable applications that allow complete authentication bypass and extraction of the entire database. In service versions there will be comparison between updated and outdated versions of software, services and frameworks. If service versions are found to be outdated it can be flagged as vulnerable It is tool that requires defining the report, including the type of data to retrieve, the location of data, and the method of displaying. It will mainly contain spotted vulnerabilities, prevention methods, and their CVE numbers to reduce dynamic errors.

As here to discover new vulnerabilities in web application. their already discovered vulnerabilities which is SQL Injection attack and cross site scripting attack is one of them. there are used in this project. In addition to that there are many services that

are hidden by firewall but still those services and their vulnerabilities can be discovered on their respective port numbers by directly sending finish request to server, these techniques violets the firewall rules due to which server being confused and it directly shows filtered ports and services.

A. SQL Injection Attack

In a SQL injection attack vulnerable code is inserted into a SQL query through a web page input by an attacker who wants to perform something harm.[2] Using SQL injection anybody can access sensitive or useful information. According to method of performing attack OWASP classified SQL injection into different types which are describe as Tautology: This attack injects malicious SQL tokens inside where clause and causes conditional query statements always evaluates to true. The main purpose is that to bypass the authentication and access data through vulnerable input field. Illegal/Logically Incorrect Queries: The main idea is that sending incorrect SQL query purposefully and observe the descriptive error message coming from database and take the advantage of it. These errors may contain some useful debugging information which can be used to form further attack. Union Queries contains the Union keyword in SQL can be used to gather information from more than one tables in the database. Injected queries are combined with normal query using union operator. And if used properly database takes the result of the both queries union together and sends to the user. Piggy-backed Queries: This is the kind of attack where an attacker tries to appends another query to the original legal query by using;(query delimiter). Database treat it as two queries and execute both of them. Stored Procedure: Stored procedures provide extra layer of protection. Stored Procedures is a group of SQL statements that form a logical unit stored in the database. It provides benefits like encapsulation and strong validation. Even though vulnerability may appear in stored procedures. The vulnerability here is same as in web applications. Blind Injection contains Blind Injection attacker can send a number of Boolean type queries to gain data. Timing Attacks the attack act as a preliminary step be- fore actually performing attack. Initially attacker fire malicious queries and observe the responses. We can use WAITFOR keyword to execute the queries at different times. By observing timing delays between responses attacker can guess sensitive information. Which helps them to form a next more dangerous attack.[3]

B. Cross Site Scripting Attack

XSS (cross site scripting) is result of improper validation of user input. It occurs whenever untrusted user input is injecting in the web application and it redirects to a web browser without proper validation or escaping. In Cross Site Scripting an attacker inserts malicious scripts into a dynamic web page of any third-party website which is vulnerable and act as a vehicle for this attack. When user or victim visits this website with trust that script is execute on user machine. It helps the attacker to gather data which can result in hijacking of user sessions, defacing web sites, or redirecting the user to malicious sites. XSS is further classified into reflected, stored, or DOM-based. This classification is based on the responses generated by the server, whether it includes the malicious script or it is stored on the server. Also, it depends on vulnerability lies in client side or server side.[1] Reflected or Non-Persistent XSS: Reflected XSS mostly found in search fields of a web page where the input is get reflected in the output page. When server receives malicious scripts, it does not store in a database, instead it is used to form response pages without any validation. Stored or Persistent XSS: Stored or Persistent XSS occurs when vulnerability lies in server side which allows malicious scripts injected by the attacker store in a database permanently and then references it in a webpage. Blogs, message forums and social networking sites are example where Persistent XSS cause harm to users' browser. Whenever victim visit that site this malicious code is executed in his browser every time. So, it is more dangerous. DOM Based XSS: Document Object Model is nothing but the convention for representing and working with an object in an HTML document. Inappropriate handling of a objects with associated DOM makes it vulnerable. Here client-side code itself is vulnerable, vulnerability not lies in the server-side code. Therefore, if we modify the DOM environment, the malicious code is executed in the victim's browser. In a DOM based XSS server does not include the malicious content in http response but the client-side code runs itself in a unexpected way due to malicious content. The page remains same but appearance get change. environment. Both reflected and stored XSS attacks are due to the vulnerability lies in server-side scripts so it handles user input improperly.[3]

C. Firewall Techniques

The previous section discussed using an ACK scan to map out which target network ports are filtered. However, it could not determine which of the accessible ports were open or closed. Nmap offers several scan methods that are good at sneaking past firewalls while still providing the desired port state information. FIN scan is one such technique. In the section called "ACK Scan", SYN and ACK scans were run against a machine named Para. The SYN scan showed only two open ports, perhaps due to firewall restrictions. Meanwhile, the ACK scan is unable to recognize open ports from closed ones. Example 10.6 shows another scan attempt against Para, this time using a FIN scan. Because a naked FIN packet is being set, this packet flies past the rules blocking SYN packets. While a SYN scan only found one open port below 100, the FIN scan finds both of them. The most audacious way to subvert intrusion detection systems is to hack them. Many commercial and open-source vendors have pitiful security records of product exploitability. Internet Security System's flagship Real Secure and Black ICE IDS products had a vulnerability which allowed the Witty worm to compromise more than ten thousand installations, then disabled the IDSs by corrupting their filesystems. Other IDS and firewall vendors such as Cisco, Checkpoint, Net gear, and Symantec have suffered serious remotely exploitable vulnerabilities as well. Open-source sniffers have not done much better, with exploitable bugs found

in Snort, Wireshark, tcpdump, Fake BO, and many others. Protocol parsing in a safe and efficient manner is extremely difficult, and most of the applications need to parse hundreds of protocols. Denial of service attacks that crash the IDS (often with a single packet) are even more common than these privilege escalation vulnerabilities. A crashed IDS will not detect any Nmap scans. Given all of these vulnerabilities, exploiting the IDS may be the most viable way into the target network. A nice aspect of this approach is that you do not even have to find the IDS. Sending a rogue packet to any "protected" machine on the network is usually enough to trigger these IDS bugs. [4]

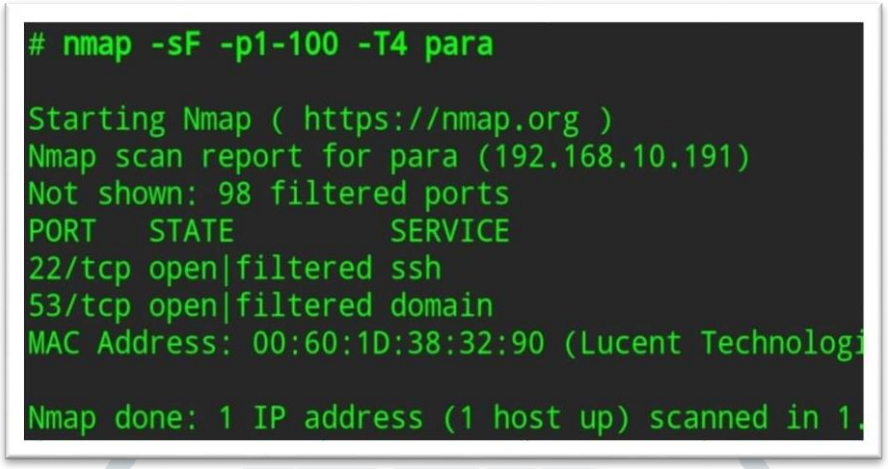
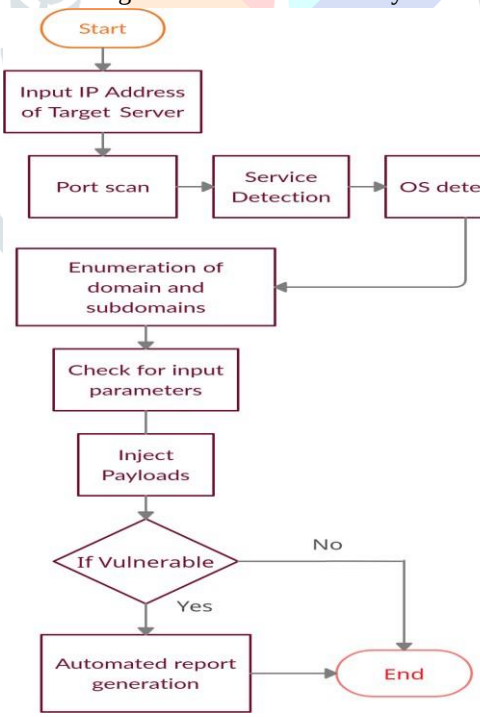


Fig.2 Filtered port scan technique by sending finish requests direct to server

IV. EXPERIMENTATION

In this section to initiate scans run the python program by entering the IP address or domain name of the target server. It will check for all packages and plugins installed in Linux operating system. Once the checks are completed, It will start scanning for open ports like 21 for FTP (File Transfer protocol),22 for SSH(Secure shell),8080 for http,443 for https and SMB services etc. and all common ports used for server as well as ports filtered by firewall by directly sending FIN request to server violating 3 way handshake that bypass firewall rules it will detect services on respective port numbers and it will detect OS used by the servers.

Fig.3 Flowchart of overall system



It will scan the open directories like admi panel, robots.txt, user.txt, php.js,.py some files leakage showing misconfigured file permissions causing expose of sensitive information and end points and input parameters. After finding suitable input parameters and query it will execute payloads consist of some malicious scripts that are intended to leak some confidential information from domain or server these payloads consist codes of javascript,php,bash and lua as signatures present in Linux resulting in detection of vulnerabilities like basic misconfigurations command injection,XSS,SQLI,LDAP,open directories,SSL TLS issues,DDOS etc. after executing payloads if the signatures get matched correctly it will flag that web application as vulnerable indicating their CVE (Common Vulnerability Exposures) and it will generate a final report.

V. RESULTS AND DISCUSSION

After the scan finishes, it will generate report in text file which will be helpful for assistance in patching and further improvement in security issues on target website or server.

Fig.4 Text File 1

After successfully completing scans, programs disclose various vulnerabilities and information about the target such as open ports like 80,443,22,21,445 which have services like http, ftp file transfer protocols secure shell and SMB service which creates open way for hackers to get inside server.

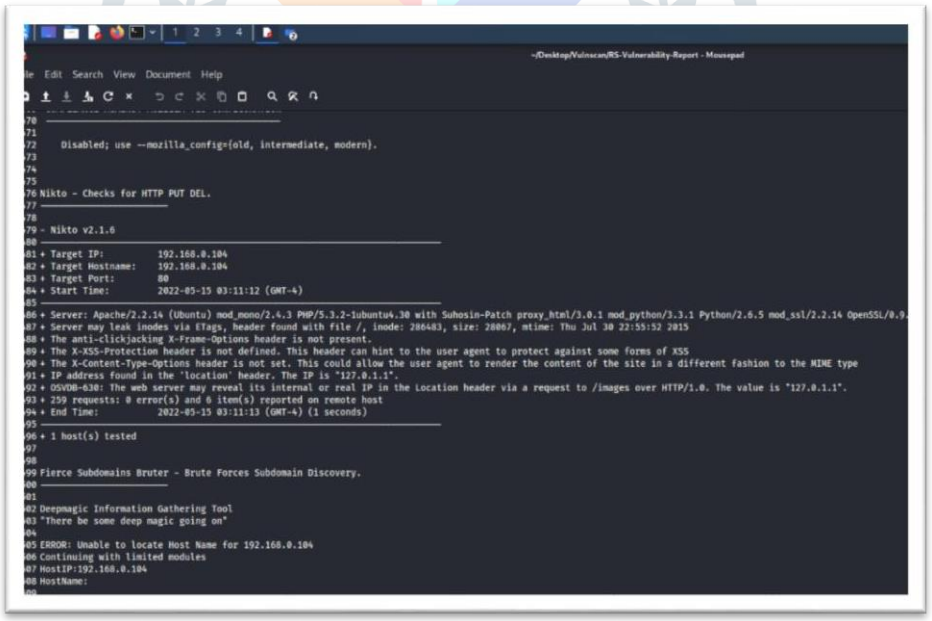


Fig.5 Text File 2

This program detected operating system info, SSL, issues, and missing headers like XSS protection, content type opens confidential directories, mismanagement of file permissions by system admin which file to be kept public and confidential. This program tested load balancing of firewalls either the server is protected from DDOS Direct Denial of Service Attack. The text file result is generated by using python script, and all the results are stored in text file.

VI. Conclusions and Future Scope

In years of vulnerability assessment and penetration testing, the best of both strategies is way to go for cybersecurity consultants and VAPT auditors. The manual approach will always be there no matter how much to look into the future but surely automated tools can be a good thing which will automate the drawbacks of vulnerability assessment up to major extent. This vulnerabilities scanner is highly flexible and customizable, depending on the severity of current and upcoming threats of web and network security plugins can be updated and can be used by security researchers and VAPT auditors to get the work done.

Acknowledgment

Efforts and perspiration alone do not contribute to the success of any project. As we have realized the importance of human factor in any constructive efforts, many people apart from project team members contributed essentially to the project's success. We wish to thank Mr. Sahil Gaikwad, (Director & Founder, Secure Era Pvt. Ltd.) and all researcher's and authors for sharing their valuable work in our cyber community. We take this opportunity to express our special thanks to all the professors of our department for their valuable guidance. Last but not the least; we would like to thank our parents for being constant source of inspiration and all our friends who have helped us directly or indirectly.

References

[1] E. Kirda, C. Kruegel, G. Vigna, and N. Jovanovic, Noxes, "A client-side solution for mitigating cross-side scripting attacks," IEEE 21st ACM Symposium on Applied Computing, 2006.
[2] Atefeh Tajpour, Suhaimi Ibrahim, Mohammad Sharifi, "The Web Security by SQL Injection Detection Tool," IJCSI International Journal of Computer Science Issues, 2012.
[3] Smita Patil, Nilesh Marathe and Puja Padiya**, "**Design of Efficient Web Vulnerability Scanner**",** IEEE International Conference on Inventive Computation Technologies, 2016
[4] www.nmap.org
[5] Haibo Chen, Junzuo Chen, Jinfu Chen, Shang Yin, Yiming Wu, Jiaping Xu, **"**An Automatic Vulnerability Scanner for Web Applications**",** IEEE 19th International Conference on Trust, 2020
[6] Zoran Djuric,"A black Box testing tool for detecting SQL injection vulnerabilities" IEEE second International Conference on Informatics and applications. 2013