Journal of Population Therapeutics & Clinical Pharmacology

RESEARCH ARTICLE
DOI: 10.47750/jptcp.2023.30.15.005

Website Vulnerability Scanner

Deeptha R.[1*], K.Sujatha [2], D.Sasireka[3], R. Neelaveni [4], R.Pavithra Guru[5]

[1]Assistant Professor, Dept. of Information Technology, SRM Institute of Science and Technology, Ramapuram, Chennai, India.

[2,3,4,5] Assistant Professor, Dept. of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, India.

***Corresponding author:** Deeptha R, Assistant Professor, Dept. of Information Technology, SRM Institute of Science and Technology, Ramapuram, Chennai, India, Email: deepthar@srmist.edu.in

Submitted: 25 April 2023; Accepted: 16 May 2023; Published: 05 June 2023

ABSTRACT

In today's world, cyber security has become an important leap in the form for jobs, education. But the reality is the only a few are aware of the major wed vulnerabilities. Some statistical studies show that small scale industries are directly and indirectly connected to the world of internet, but penetration testing, we are going to do this project. In a website if there are any vulnerability, the website can easily hack. So, using penetration testing we are going to built a scanner which will find the vulnerabilities the website. With the help of vulnerability scanning in a website, inspection of the potential points of exploit on a website to identify security holes. A vulnerability scan will deduct and classifies system weeness. It will also deduct bugs in a website and communication equipment. It will predict effeteness of counter measure.

Keywords: *Cyber security, vulnerability, penetration testing, website scanning*

INTRODUCTION

Web application, penetration testing is the practice of simulating attacks in the system. To gain access to sensitive data, with the proposed of determining whether a system a secure or not. These attacks are performed either internally are externally on a system, and they help provide information about the target systems, identify vulnerabilities with in them. And uncover exploits that whether remediation and security measures are needed. There are several keys to benefits to incorporation requirements. Pen testing is explicitly required in some industries, and performing web applications. Pen testing helps to meet the requirements.

It helps you who access infrastructure. Infrastructure, like fire walls and DNS servers, in public facing. Any changes made to the infrastructure can make a system vulnerable. Web application, pen testing helps to identify in a real-world attack that could be succeed at accessing these systems. It identifies vulnerabilities in a web application pen testing identifies loopholes in a applications are vulnerable routes in infrastructure – before an attacker does. It helps to confirm security policies. Web applications pen testing accesses existing security policies for any weaknesses. Therefore, vulnerability scanners are used to scan the network and software applications.

LITERATURE REVIEW

Project Title: Websecurity And Vunerabilitys Author Name: H Yulimanton 1,2*, H L H S Warnars1, B Soewtiol, F L Gaol1 And E Abdurachaman 1 Year Of Publishing : 2020

The web continues to grow and attacks against the web continue in increase. This paper focuses in the literature review on scanning web vulnerabilities and solutions to mitigate web attacks. Vulnerability scanning methods will be in reviewed as well as framework for improving web security. This research is the basis for future work that will end with the elaboration of web scanning and security with the aim of proposing better innovations.

Project Title: Vulnerability Scanning Author Name: Prajakta Subhash Jagtap, K J Somaiya Year Of Publishing: 2018

Scientific advances of higher education institutions make them attractive targets for malicious cyberattacks. Modern scanners such as Nessus and Burp can pinpoint an organization's vulnerabilities for subsequent mitigation. However, the correction reports generated from the tools typically cause important info overload whereas failing to produce unjust solutions. Consequently, higher education institutions lack the appropriate knowledge to improve their cybersecurity posture. However, while not understanding vulnerabilities in a very system, it would be difficult to conduct successful network defence in order to prevent intruders in the real world. Therefore, vulnerability scanning is a key element to the success of cybersecurity curriculum. In this paper, we tend to review the state of the art of current open-source vulnerability scanning tools. Literature survey is done on vulnerability, vulnerability scanning, vulnerability scanning tools, security vulnerabilities, system security and application security, malicious cyber-attacks shows that a lot of work is being carried out in vulnerability assessment and reporting. In this report gives exhaustive study on vulnerability scanning tools. We presented two main aspects in this paper vulnerability scanning and reporting. Then we identify the gaps in relevant practices and presenting selected results, we highlight future directions and conclude this research. We provide thorough descriptions on the top open-source network vulnerability scanning tools. We then propose our hands-on labs research design in detail on network vulnerability scanning that we design specifically to enhance the cybersecurity curriculum.

Project title: A Framework for Web Application Vulnerability Detection Author name: Asra Kalim, C K Jha, Deepak Singh Tomar, Divya Rishi Sahu Year of publishing: 2017

Hardly a facet of human life is not influenced by the Internet due to the continuous proliferation in the Internet facilities, usage, speed, user friendly browsing, global access, etc. At flip side, hackers are also attacking this digital world with new tactics and techniques through exploiting the web application vulnerabilities. The analysis of these vulnerabilities is of paramount importance in direction to secure social digital world. It can be carried out in two ways. First, manual analysis which is error prone due to the human nature of forgiveness, dynamic change in technology and fraudulence attack techniques. Second, through the existing web application vulnerability scanners that sometime may suffer from generating false alarm rate. Hence, there is a need to develop a framework that can detect different levels of vulnerabilities, ranging from clientside vulnerabilities, communication side vulnerabilities to server-side vulnerabilities. This paper has carried out the literature survey in direction of identifying the new attack vectors, vulnerabilities, detection mechanism, research gaps and new working areas in same field. Continuous improvement in framework is easy. Hence, a framework is proposed to overcome the identified research gap

Project title: Web Vulnerability Scanners Author name: Angel Rajan, Emre Erturk Year of publishing: 2015

Cloud security is one of the biggest concerns for many companies. The growth in the number and size of websites increases the need for better securing those websites. Manual testing and detection of web vulnerabilities can be very time consuming. Automated Web Vulnerability Scanners (WVS) help with the detection of vulnerabilities in web applications. Acunetix is one of the widely used vulnerability scanners. Acunetix is also easy to implement and to use. The scan results not only provide the details of the vulnerabilities, but also give information about fixing the vulnerabilities. AcuSensor and

AcuMonitor (technologies used by Acunetix) help generate more accurate potential vulnerability results. One of the purposes of this paper is to orient current students of computer security with using vulnerability scanners. Secondly, this paper provides a literature review related to the topic of security vulnerability scanners. Finally, web vulnerabilities are addressed from the mobile device and browser perspectives.

Project title: A Systematic Literature Review on the Characteristics and Effectiveness of Web Application Vulnerability Scanners Author name: Suliman Alazmi (Member, IEEE), and daniel conte de leon (Member, IEEE) Year of publishing: 2017

Web applications have been a significant target for successful security breaches in the last few years. They are currently secured, as a primary method, by searching for their vulnerabilities with specialized tools referred to as Web Application Vulnerability Scanners (WVS's). Although, these dynamic approaches of testing have some advantages, there is still a scarcity of studies that explore their features and detection capabilities in a systematic way. This article reports findings from a Systematic Literature Review (SLR) to look into the characteristics and effectiveness of the most frequently used WVS's. A total of 90 research papers were carefully evaluated. Thirty (30) WVS's were collected and reported, with only 12 having at least one quantitative assessment of effectiveness. These 12 WVS's were evaluated by 15 original evaluation studies. We found that these evaluations tested mostly only two of the Open Web Application Security Project (OWASP) Top Ten vulnerability types: SQL injection (SQLi) (13/15) and CrossSite Scripting (XSS) (8/15). Additionally, only one work evaluated six of the OWASP Top Ten vulnerability types and for only one scanner. We also found that the reported detection rates were highly dissimilar between these 15 evaluations. Based on these surprising results we suggest avenues for future directions.

Project title: Web Vulnerability Scanners, case study Author name: Emre erturk, Angel rajan Year of publishing: 2017

Cloud security is one of the biggest concerns for many companies. The growth in the number and size of websites increases the need for better securing those websites. Manual testing and detection of web vulnerabilities can be very time consuming. Automated Web Vulnerability Scanners (WVS) help with the detection of vulnerabilities in web applications. Acunetix is one of the widely used vulnerability scanners. Acunetix is also easy to implement and to use. The scan results not only provide the details of the vulnerabilities, but also give information about fixing the vulnerabilities. AcuSensor and AcuMonitor (technologies used by Acunetix) help generate more accurate potential vulnerability results. One of the purposes of this paper is to orient current students of computer security with using vulnerability scanners. Secondly, this paper provides a literature review related to the topic of security vulnerability scanners. Finally, web vulnerabilities are addressed from the mobile device and browser perspectives.

Project title: Analysis of Automated Web Application
Security Vulnerabilities Testing Author name: parish touseef ,khubai amjad alam, abid jaml, hamza tauseef, sahar ajmal, bisma rehman, sumaira Mustafa Year of publishing: 2019

In recent years, the global spread of web risks have proposed an immediate demand for security models and prevention mechanisms. This study preliminary findings analyze an extensive literature review on web application vulnerabilities security testing. Out of an initial set of 237 studies, 30 studies were finally included as Primary Research Studies (PRS) by assuring two research questions. The results reveal that SQL injection followed by XSS and Sensitive data exposure are the most recurring 8 risks of web applications. Similarly, Invalidated Redirects and Forwards/Under Protected APIs have received little attention by research community. The scope of this study is also extended to web application vulnerabilities testing and identification of relevant data sets. This paper also recommends future possibilities to enhance the security approaches for protection against the risks

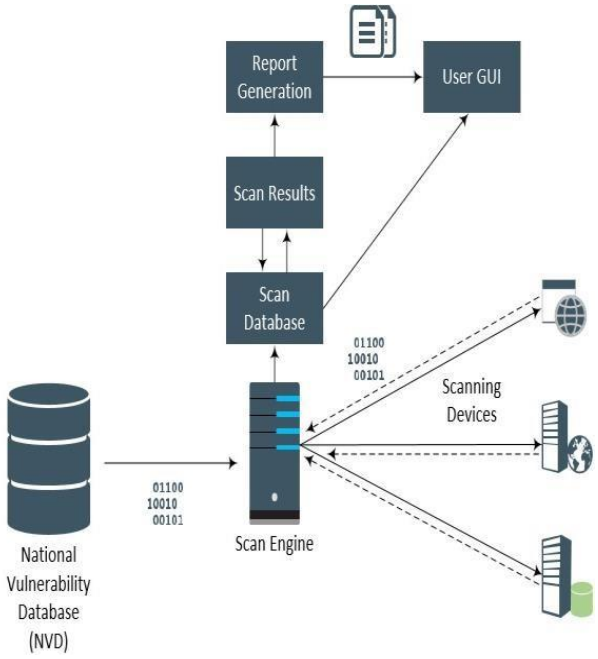

FIGURE 1: Vulnerability scanner

SYSTEM ANALSIS

Objective

For testing and evaluating vulnerability using scanner, a vulnerable web environment has to be formulated. This is a fulfilled by vulnerable web applications that are specially has designed to provide users, the environment to identify the attacks and the way to rectify it. This section deals with some of the scanners that can evaluate the vulnerabilities of a web applications

Nmap

Nmap stands for network mapper which is a free opensource command-line tool. Nmap is an informationgathering tool used for recon reconnaissance. Basically, it scans host and services on a computer network which means that it sends packets and analyses the response. Listed below are the most useful scans which you can run with the help of Nmap tools. Nmap is a port scanner that is used to scan the ports. It takes an IP address and captures all the information related to it. If an IP address is provided, then it finds the host to which it belongs to. It also finds the number of ports that are running on that particular host, number of ports that are opened, number of closed ports, services provided by these ports, which may be TCP or FTP oriented. It predicts the type of operating system that is being connected to the system. The topology of the host is recorded in the form of graphical format which shows the various gateways through which the local machine accesses that host. If the ports are opened, then the attacker can easily make unauthorized access to the host. A number of various ports can be scanned using Nmap. This scan is used to scan the TCP ports. It completes the 3-ways handshake process which means the host tries to makes a connection with the target before any communication happens between the system. Using this command your system sends a SYN packet and the destination responds with SYN and ACK packets which means the port is listening and your system sends an ACK packet to complete the connection.

Nessus

Nessus is a vulnerability scanner that lists out the vulnerabilities in the remote host. It provides both internal and external scan. Internal scan is related to the host within a particular router. External scan involves the host outside a particular router. Web application tests can also be performed using the scanner. There are two ways in which scanning can be performed, either it can be done at first instance or a template can be formulated for a host and launch this to scan the host. Multiple scanning of the host can be done at once. Vulnerability can be evaluated by Nessus using four types of severity high, medium, low and informal. Results are saved automatically as soon as the scan of the particular

10 host is completed. The results are provided in two ways-vulnerabilities by plug-in and vulnerabilities by host. The first one classifies all the vulnerabilities during the scan and lists out the outs affected by these vulnerabilities. It generates a report that can be used to fix the vulnerability. The latter addresses the issues related to host, follow up scans and assessment is done accordingly. The results can be exported in any desired format. Nessus is based on client-server architecture. Each session is controlled by the client and the test is done on the server side. More than 100 websites can be scanned using Nessus. A penetration test, meanwhile, is an authorized attack on your own systems a form of ethical hacking that exploits vulnerabilities so that a pen tester can attempt to gain access to systems and data. The idea is to see how easy or difficult it is to overcome your defences, testing the hypothetical risks found during a vulnerability assessment. Pen testers use a well-known arsenal of "white hat" hacking tools to complete their sanctioned attacks, including the Social Engineering Toolkit and Pen Testers Framework. But a pen tester's manual skill and creativity are just as important to successfully find an exploitable system, map the network, gain access to other systems and test defences. Think of it as the infosec version of criminal profiling: Only by imagining the mindset of a malicious hacker and mimicking their activities can a well-intentioned pen tester truly understand the risk an organization faces and adequately prepare to face it.

Acunetix

Acunetix is an automated web application security testing tool that checks the web application by checking for web vulnerabilities like SQL injection, cross-site scripting and exploited vulnerabilities. Acunetix scans a web site or web application that is accessible via a web browser. Acunetix offers a strong solution for custom based web applications utilising Javascript, AJAX. Acunetix has an advanced crawler that finds any file. The scanning is performed in three steps target specification, site crawling and structure mapping and pattern analysis. In target identification, the target is checked with an active web server and hosts any web application. Information is collected regarding web technologies, web server type and responsiveness for appropriate filtering tests. In structure mapping and site crawling, the index file of a web application is fetched first, determined by the URL. Received responses are taken to get inks, input fields that create a list of directories and files inside the web application. Pattern analysis is executed against the web application.

Nikto

Nikto is a command-based tool that is used to scan specific targets. It uses Perl language to scan the web application. It performs security checks against dangerous files. Attackers look for web application vulnerabilities so that they can gain access to outdated Apache servers. It is a free and open-source scanning tool therefore IT enterprises can easily identify the security flaws in the organization and take necessary steps to shield and upgrade the system. The tool is able to find servers that were not developed by the enterprise.

Burp Suite

Burp scanner is a tool for automatically finding vulnerabilities in a web application. It is designed to be used by security testers. It is a proxy-based tool package. It consists of various functional specifications. The tools offered by burp suite are spider, proxy, intruder, repeater, sequencer, decoder, extender and scanner. In the first step, a proxy is set in the browser. After the proxy is set, the burp suite is about to begin. The burp window [7] has many tab specifications like proxy, intruder, spider, repeater, sequencer, and scanner, where each has got its own sub-tabs. For instance, proxy tab has three sub tabs -intercept, proxy and options. Proxy tab is used to fix the proxy and configure it. At this time, the intercept tab remains with it. A xampp server is installed in the system which is developed to scan the system. Through this, the username and password of the user can be identified, provided that the intercept tab remains off. Intruder tab is used to automate customized attacks against web applications. Spider tab provides the crawler feature for the application test. Repeater tab is used to modify the HTTP request and analyse their responses. Scanning performs scanning of the hosts. Scanning involves testing of hosts for the vulnerabilities inside it. Burp suite identifies the type of vulnerability and its severity

System Requierment
Software Requirement

- Python
- Linux (Preferred kalis os, as it is shipped with almost all the tools)

Hardware requirement

- Some of the hardware requirements for the projects are computer, laptop (or)
- MAC
- A Hardware disk – 250GB, minimum of 4 to 8GB ram for the some other o Hardware devices like keyword and a mouse.
- For network a stable wi-fi modem for network stability.

System Architecture
Architecture Diagram

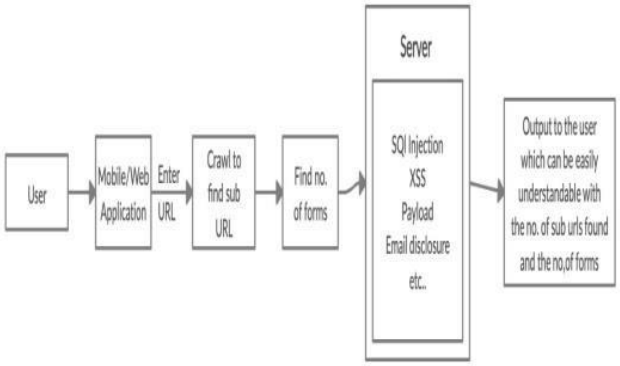

FIGURE 2: Architecture Diagram

Proposed Method

With the increasing development of the internet, web applications have become increasingly vulnerable and are exposed to unauthorized attacks. To deal with this problem, many online scanners are available in the market. But most of them are not able to detect all the vulnerabilities available. If a situation arrives where the scanner we use cannot detect 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 the vulnerabilities like SQL injection, cross site scripting, broken authentication, payload, email disclosure. The vulnerability scanner scans the website and checks whether the above vulnerabilities are identified while scanning. the overall design of the vulnerability scanner. The scanner is available as either 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 if the above mentioned vulnerabilities are present in the URL or not. If present, it will list out the vulnerabilities and some other additional information regarding the URL like sever information, technology information, certification information, etc

SQL Injection

User gives his username and password through a web application. Web application has stored the given details to the SQL server. An attacker gives HTTP requests that are sent to the web server to inject commands to the SQL server in order to gain system level access. The vulnerable web application allows this malicious code to be placed on an SQL server, thus making it possible for the attacker to use SQL commands to get user account credentials. How SQLI vulnerability can be exploited? During an SQLI attack, a malicious code is given as an input to a function that calls an SQL query, which is called immediately. Injection allows the user to add malicious code via a web application to another system. These attacks include calls to an operating system through system calls, the use of external programs via shell commands, and also calls to backend databases. Injection is a weak point where the user can insert a malicious code of his interest. Malicious code is embedded with the user input data and passed to the application. If

user input data is not properly filtered in the system, in that case, the interpreter processes the malicious code as a normal legitimate user input and the system outputs accordingly. The level of risk associated with SQL injection is high. An attacker can exploit the data and steal necessary information from the web application

Cross Site Scripting

Cross site scripting (XSS) vulnerability occurs when there is a possibility of inserting a malicious code by an unauthorized user. Thus, the XSS flaw is as a result of not validated or sanitized input parameters. There are three types of XSS: NonPersistent, called Reflected XSS; Persistent or Stored XSS; vulnerability occurs when a web application accepts the user's malicious request. This is then echoed to the application's response in an unsafe way. Persistent XSS vulnerability occurs when a web application accepts the malicious request, stores in a data source and which then displays the information from the request to a wide range of users. DOM-based XSS vulnerability does not involve server validation.

The attack works on a web browser, avoiding the server side. The DOM environment in the victims browser is modified by the original client-side script, and as a result of that, the payload is executed. In Cross-Site Scripting, attackers exploit the user's trust over a vulnerable web application. In this attack, malicious JavaScript or html codes are inserted through user input fields to a page. It generally occurs when the application sends user input data as a part of a webpage, without properly validating to the user's browser. The risks associated with Cross-Site Scripting include a hijacking session, an unauthorized changing of the contents of application, redirecting the application to another website, and insertion of some malicious codes or links. The level of risks is high. By the hijacking session, attackers can get secret and important information

Broken Authentication

The user authentication typically involves the username and password of the user. When the authentication process weakens, the attacker can get the credentials of the user. Authentication is an act of verifying the identity of a user, allowing access to resources in an information system. It refers to the process of verifying either a user, which requests to communicate with either the whole application or with a part of it in order to make sure that only the intended user can get access to the application and its resources. A session is a sequence of all the activities between a client and a web server for a particular login and logout period. The activities are generally associated within the login and log out period of the same user. So, there is a different session for each different user. For a number of different reasons, a web application requires to hold session information. For example, there may be different contents to deal with according to the preference, or the type of user; or there may be security issues. Effective authentication and proper session management are important for a web application to be secure.

The level of risk associated with the authentication and session management is high. Attackers usually gain access to the system through hijacking a username and a password or session IDs. They can access secret information and data while pretending that they are the legitimate user of the application.

Abbreviations and Acronyms

DNS- Domain Name System
IP- Internet Protocol
TCP- Transmission Control Protocol
AJAX- Asynchronous Javascript And Xml
HTTP- Hyper Text Transfer Protocal
XSS- Cross Site Scripting
DOM- Document Object Model

System Modules

System Description

The system comprises 1 major module with their submodules as follows:

- Target URL
- Scanning
- Malware Detection Using python script, the URL, will be passed and will be *Detected as good or bad
- Detecting SQL Injection
- sub-domain Scanning ect.,
- Final vulnerability report

System Implementation
Coding and testing
Coding
Once the design aspect of the system is finalized the system enters into the coding and testing phase. The coding phase brings the actual system into action by converting the design of the system into the code in a given programming language. Therefore, a good coding style has to be taken whenever changes are required and it easily screwed into the system.

Testing
Testing is performed to identify errors. It is used for quality assurance. Testing is an integral part of the entire development and maintenance process. The goal of the testing during this phase is to verify that the specification has been accurately and completely incorporated into the design, as well as to ensure the correctness of the design itself. For example the design must not have any logic faults in the design before coding commences, otherwise the cost of fixing the faults will be considerably higher as reflected. Detection of design faults can be achieved by means of inspection as well as walkthrough.

Test Data and Output
Unit Testing
Unit testing is conducted to verify the functional performance of each modular component of the software. Unit testing focuses on the smallest unit of the software design (i.e.), the module. The whitebox testing techniques were heavily employed for unit testing

Functional Testing
Functional test cases involved exercising the code with nominal input values for which the expected results are known, as well as boundary values and special values, such as logically related inputs, files of identical elements, and empty files. Three types of tests in Functional test:

- Performance Test
- Stress Test
- Structure Test

Testing Techniques / Testing Strategies
Testing
Testing is a process of executing a program with the intent of finding an error. A good test case is one that has a high probability of finding an as-yet –undiscovered error. A successful test is one that uncovers an as-yet- undiscovered error. System testing is the stage of implementation, which is aimed at ensuring that the system works accurately and efficiently as expected before live operation commences. It verifies that the whole set of programs hang together. System testing requires a test consists of several key activities and steps for run program, string, system and is important in adopting a successful new system. This is the last chance to detect and correct errors before the system is installed for user acceptance testing.

White box testing
This testing is also called Glass box testing. In this testing, by knowing the specific functions that a product has been designed to perform, tests can be conducted that demonstrate each function is fully operational at the same time searching for errors in each function. It is a test case design method that uses the control structure of the procedural design to derive test cases. Basis path testing is a white box testing. Basis path testing:

- Flow graph notation
- Cyclomatic complexity
- Deriving test cases
- Graph matrices Control

J Popul Ther Clin Pharmacol Vol 30(15):e43–e53; 05 June 2023.

CHAPTER-8 RESULT

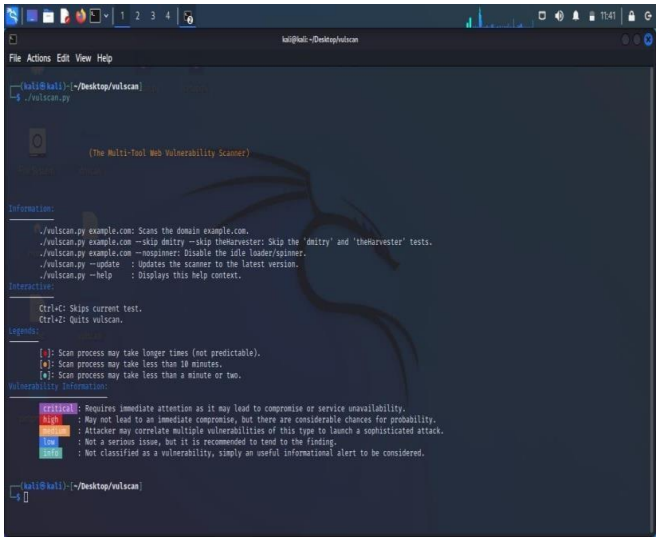

FIGURE: 3 Interface

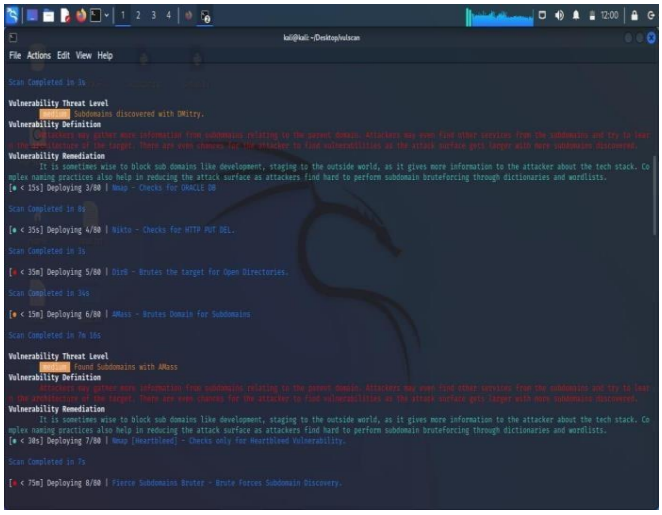

FIGURE 4: Vulnerability threat level

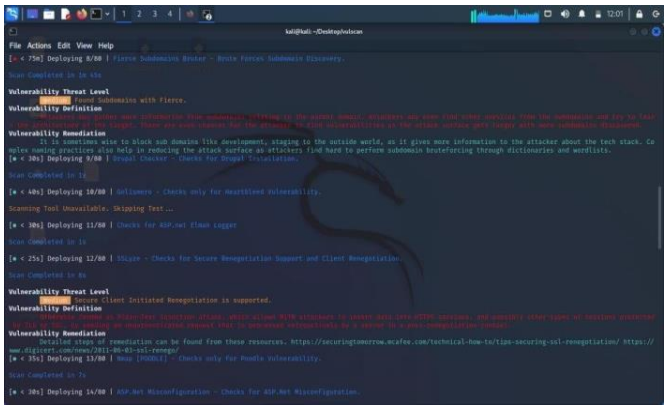

FIGURE 5: Vulnerability remediation

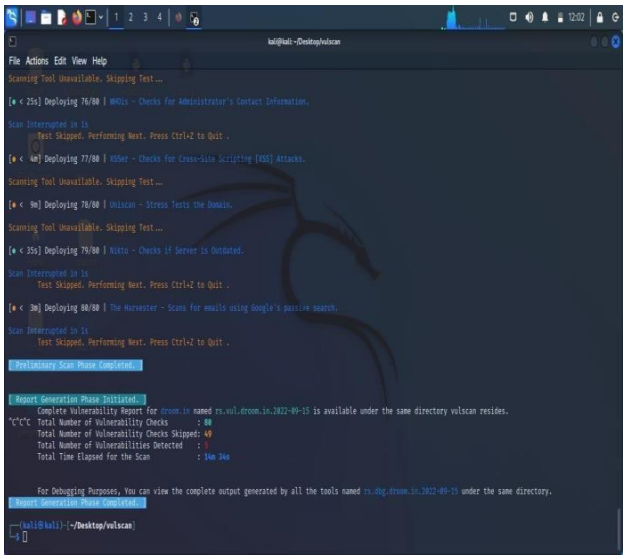

FIGURE 6: Final output

CONCLUSION

Penetration testing is the exploitation of vulnerabilities present in an organization's network. It helps determine which vulnerabilities are exploitable and the degree of information exposure or network control that the organization could expect an attacker to achieve after successfully exploiting vulnerability. No penetration test is or ever can be "just like a hacker would do it," due to necessary limitations placed on penetration tests conducted by "white hats." Penetration testing depends on the types of vulnerabilities. Vulnerabilities can be thought of in two broad categories—logical and physical. One normally thinks of logical vulnerabilities as those associated with the organization's computers, infrastructure devices, software, or applications. Physical vulnerabilities, on the other hand, are normally thought of as those having to do with either the actual physical security of the organization, the sensitive information that "accidentally" ends up in the dumpster, or the vulnerability of the organization's employees to social engineering. Vulnerabilities might also exist due to a lack of company policies or procedures or an employee's failure to follow the policy or procedure.

Regardless of the cause of the vulnerability, it might have the potential to compromise the organization's security.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 all- rounder in scanning web vulnerabilities. The above proposed scanner is best suited for beginners who are not aware of the complex steps of scanning. Vulnerability scanning identifies the security vulnerabilities in an organization. Vulnerability assessment provides the organization with the awareness and risk associated with the organizations working environment and work accordingly. The advantage of using vulnerability scanner is that it identifies known security exposures before attackers find them.

REFERENCES

1. Mansour Alsaleh, Noura Alomar, Monirah Alshreef, Abdulrahman Alari and AbdulMalik Al- Salman, "PerformanceBased Comparative Assessment of Open Source Web Vulnerability Scanners", (2017)
2. Sheetal Bairwa, Bhawna Mewara and Jyoti Gajrani, "Vulnerability Scanners: A Proactive Approach to Assess Web Application Security", (2014)
3. S. El Idrissi, N. Berbiche, F. Guerouate and M. Sbihi, "Performance Evaluation of Web Application Security Scanners for Prevention and Protection against Vulnerabilities", (2017).
4. Acunetix:https://www.acunetix.com/vulnerabilityscanner/
5. Nikto: https://hackertarget.com/nikto-website-scanner/
6. Burp Suite: https://portswigger.net/burp
7. YU Shiyuan, WANG Yutian, LIU Xin, "Burp Suite Extender Apply in Vulnerability Scanning", (2018).

8. Balume Mburano, “Evaluation of web vulnerability based on OWASP Benchmark”, (2017).
9. Deepika Sagar, Sahil Kukreja, Jwngfu Brahma, Shobha Tyagi, Prateek Jain, ”Studying Open Source Vulnerability Scanners For Vulnerabilities In Web Applications”, (2017).
10. Kinnaird McQuade, “Open Source Web Vulnerability Scanners”, (2014).
11. Y.Makino and V.Klyuev, “Evaluation of web vulnerability scanners,” IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), (2015)

J Popul Ther Clin Pharmacol Vol 30(15):e43–e53; 05 June 2023.