Proceedings of the Fifth International Conference on Trends in Electronics and Informatics (ICOEI).
IEEE Xplore Part Number:CFP21J32-ART; ISBN:978-1-6654-1571-2

IDENTIFICATION OF URL FUZZING AND SUBDOMAIN ENUMERATION USING RACCOON TOOL

Baby Shamini P
Assistant Professor
Rajalakshmi Institute of Technology
babyshamini.p@ritchennai.edu.in

Sandhiya V
CSE
Rajalakshmi Institute of Technology
sandhiya.v.2017.cse@ritchennai.edu.in

Vibilleshnee U
CSE
Rajalakshmi Institute of Technology
vibilleshnee.u.2017.cse@ritchennai.edu.in

Yamini S
CSE
Rajalakshmi Institute of Technology
yamini.s.2017.cse@ritchennai.edu.in

2021 5th International Conference on Trends in Electronics and Informatics (ICOEI) | 978-1-6654-1571-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICOEI51242.2021.9453002

***Abstract*—A vulnerability scanner is a computer program designed to assess computers, networks or applications for known weaknesses. It is a tool for reconnaissance and information gathering with an emphasis on simplicity .It will do everything from fetching DNS records, retrieving WHOIS information, obtaining TLS data, detecting WAF presence and up to threaded directory busting and subdomain enumeration. Every scan output to a corresponding file. At most of all vulnerability scanner scans are independent and do not rely on each other result it utilizes python's asyncio to run most scans asynchronously. Our tool supports Tor /proxy for anonymous routing. It uses default wordlists (for URL fuzzing and subdomain discovery) enumeration. This vulnerability scanner helps you scan your IP address ranges to discover open ports and other security vulnerabilities specific to network devices.**

Keywords- DNS records, WHOIS information, TLS data ,WAF presence, Subdomain Enumeration, Wordlist, URL Fuzzing, Subdomain Discovery.

I. INTRODUCTION

Vulnerability-scanner is a computer programmes are often used to check the security of computer, network, network, and application-based systems for known vulnerabilities. The application is used to identify the weaknesses of a given system. These scans are commonly performed to identify vulnerabilities within an asset in a network-based system like a firewall, router, web server, or other software to determine whether a security configuration or programme is broken. In addition to the authentication scans, vulnerability scanners now allow both authenticated and unauthenticated ones to be performed. authenticated scans enable the scanner to access assets that are done using protocols such as SSH or RDP and to be secured by credentials which have been handed over by the machine itself. If the scanner is able to access low-level host data, such as services and configuration information, then it will be able to retrieve information on the operating system. In general, unauthenticated scans will generate a lot of false positives and are unable to tell you what software is running on the machine's actual assets, which leaves you with a lot of guesswork and uncertainty about what you're actually looking at. Vulnerability-scanning software is a computer programmes are often used to check the security of computer, network, and application-based systems for known vulnerabilities. These scans are commonly performed to identify vulnerabilities within an asset in a network-based system like a firewall, router, web server, or other software to determine whether a security configuration or programme is broken. In addition to the authentication scans, vulnerability scanners now allow both authenticated and unauthenticated ones to be performed. authenticated scans enable the scanner to access assets that are done using protocols such as Secure Shell SSH or Remote Desktop protocol RDP and to be secured by credentials which have been handed over by the machine itself. If the scanner is able to access low-level host data, such as services and configuration information, then it will be able to retrieve information on the operating system. In general, unauthenticated scans will generate a lot of false positives and are unable to tell you what software is running on the machine's actual assets, which leaves you with a lot of guesswork and uncertainty about what you're actually looking at. The vulnerability scanner will look for URL fuzzing and subdomain enumeration in this case. There is a tool that one can use to find hidden files and directories on a webserver .This helps the user to identify files that were not supposed to be publicly available (for example, /index,/backup, and so on). To determine if software has a vulnerability, developers perform fuzz testing. There are a wide range of techniques available, and they are very cheap. As one of the most frequently used approaches to discovering vulnerabilities, fuzzing is applied to almost all

systems. The majority of vulnerabilities that are found during fuzzy testing are in the most critical crashes. Subdomain enumeration has become increasingly necessary for attackers in recent years, and various tools with various approaches have been created. Hacking reconnaissance requires the discovery of a domain's subdomains. The method of enumerating valid subdomains from one or more domains is known as subdomain enumeration. Sub list3r is a Python tool that uses a search engine to locate subdomains. It aids in the collection and gathering of subdomains for a target domain. The method will help anonymous proxy support for our tools. URL and subdomain discovery is performed using the built-in word lists. Using this port scanner will help scanner, this scanner scans your IP address ranges to locate any open ports or any potential security issues with network devices that are specific to them layers of the system.

II. RELATED WORK

Sandeep Kumar Yadav,Daya Shankar Pandey,ShrikantLade [1] they suggested a method for detecting network vulnerability. The two vulnerability scanning tools, Nessus and OpenVAS, were evaluated based on their unique features. Nessus found a total of 53 vulnerabilities, 4 of which are very critical with high risk, 4 of which are moderate risk, and 45 of which are merely informative; however, in the case of OpenVAS, reveals that after removing logs and false positives, OpenVAS found a total of 48 vulnerabilities, of which 25 are critical and four of which are moderate risk.For a given host system, 23 is a moderate standard.

Mansour Alsaleh ,Noura Alomar, Monirah Alshreef, Abdulrahman Alarifi, and AbdulMalik Al-Salman [2] they scanned the IBM scan-test environment (AltoroApp) to evaluate the quality of the scanning tools. The key goals of this research are to evaluate the performance of opensource scanners from a variety of perspectives and to look at their detection capabilities. In addition, 225 of the test cases from the Web Application Vulnerability Scanner Validation Project (WAVP) showed us the scanner weaknesses. 62% of the scanned vendors reported at least one WAVSEP case, while only 40% scanned 40% of the ones reported by Altoro Mutual XSS. The four scanners found at most 20% of the cases found SQL-related issues and at 43% of the XSS issues.

Sheetal Bairwa, Bhawna Mewara and Jyoti Gajrani [3] they dedicated this work to new ways to secure the web applications and the hosts they're attempting to discover new scanning methods to find existing vulnerabilities on the network.The techniques used for Vulnerability scanner are Static Analysis,Attackgraph Analysis and the Vulnerability Scanners are NMap,Nessus, Acunetix WVS,Nikto, Burpsuite. The Nessus scanner identifies a total of 29 vulnerabilities for Hebron website: 0 Critical, 1 High, 3 Medium, 2 Low, and 23 Informal.Acunetix WVS identifies total 537 alerts are found for Air India website- 291 Medium and 246 Informal. BURPSUITE determines the type and intensity of the vulnerability .Only Nessus, Acunetix WVS, and Burpsuite have detected the majority of the listed vulnerabilities.

Mohamed Abomharao and Geir M.Koien[4] devices and their corresponding attacks on IoT, along with their specific attributes. devices and their corresponding attacks on IoT, along with their specific attributes. Individuals,Intelligence agencies, but organised criminal organisations can pose a threat Physical attacks,Attacks on privacy, Information Attack, Access Attack, and Supervisory Control and Data Acquisition(SCADA)Attack are some of the more common and more frequent varieties of cyber attacks. Assets were defined in this paper as all important elements in the system, both tangible and intangible, that must be protected.

Jun Li ,Bodong Zhao and Chao Zhang [5] have summarises recent advances, analyses how they improve the fuzzing process, and sheds light on future fuzzing work. The strategy of coverage-based fuzzing is widely used by modern fuzzers and has proven to be quite effective and efficient. They began by contrasting fuzzing with other vulnerability discovery solutions before introducing the concepts and key challenges of fuzzing.

Jagtap, Prajakta Subhash, J Somaiya [6] have summarises that the Vulnerability testing can be used by security experts to find weaknesses in systems so that they can be repaired and protected. The vulnerability scanner's core architecture is represented in NVD, which includes information on Common Vulnerabilities and Exposures (CVE), which is a list of generic names for established vulnerabilities. The Popular Vulnerability Scoring System is a risk level categorization system for NVD (CVSS). CVSS scores take into account factors such as the attack vector, difficulty, privileges required, user engagement, and the effect of confidentiality, honesty, and handiness. The removal of the vulnerable programme, protocol, or system is ideal if it does not interfere with functionality. A security professional's ability to recognise hazardous assets and apply effective defences is enhanced by knowledge of required equipment, protocols, processes, and applications in 191 organisation. Removing a device deficiency typically has a cascading effect on many others.

Nabie Y Conteh, Paul J.Schmick [7] their overall goal of this research is to determine how vulnerable an organization's information technology infrastructure is to cyber intrusions, which includes hardware and software systems, transmission media, local area networks, wide area networks, business networks, intranets, and internet use. The paper seeks to clarify the significance and role of social engineering in network intrusions and cyber-theft in order to achieve this goal. Although technology can help reduce the impact of social

engineering attacks, the weakness lies in human behaviour, human desires, and psychological predispositions, according to the report..

Manju Kaushik , Gazal Ojha[8] have proposed that the main goal is to break through the attack. For this, we have suggested an effective mechanism in which the central authority can monitor and manage all visited IP addresses. Various methods have been suggested as a solution for SQLIAs (SQL Injection Attacks), but many of these solutions have flaws that hinder their efficacy and applicability. Data encryption and decryption in the communication channel are also beneficial for data security. We can use the DES, RSA, RC4 and RC5 algorithms for encryption and decryption. Vulnerability and Attack Injection was used in a configuration based on three web applications of varying sizes and complexities to test the techniques in a specific scenario. The results show that the tested tools are ineffective and only work well in particular situations, highlighting the existing intrusion detection tools' shortcomings in detecting SQL Injection attacks. They highlight the strengths and disadvantages of the instruments evaluated based on experimental observations.

Omar Y. Sharkasi,[9] proposed the main areas of security programmes that need immediate attention. As a result, a structure is created to aid in meeting regulatory and security standards, as well as to ensure corrective actionable guidance for new processes and techniques. While much of this article is focused on US law and industry, the research can be applied to a wide range of countries. Before using Internet of Things (IoT) technologies to control IT systems, building equipment, smartphones, and other web-enabled intelligent systems, businesses must first assess and minimise the risk of emerging technology protection. These initial steps ensure that these technologies have appropriate security measures in place to protect them from hackers. Many of these technologies are vulnerable to attacks that could interrupt building operations and, worse, allow hackers access to corporate systems.

Avinash Kumar Singh,SangitaRoy[10] they proposed a network-based vulnerability scanner solution that offers greater coverage and no false positives. This paper proposes a Network Based Vulnerability Scanner (NVS), which can detect all SQLI-vulnerable pages in a web application and generate a report that allows programmers to work on and fix only the vulnerable pages, rather than the entire web app. This approach allows programmers to focus only on the bad pages rather than the entire web app. The most significant benefit of NVS is that it produces reports in under one hour on average. Its effectiveness is largely determined by the number of systems linked to the network.

Ankit Dhatrak1, AnshumanSarkar [11] ,They proposed to illustrate the challenges of cyber security in the area of Internet of Things (IoT). Sensors have always been an essential part of the Internet of Things. RFID and WSN are examples of IoT computers. This will eventually be replaced by a wireless device that allows you to change the configuration whenever you want. As the number of Internet of Things (IoT) devices grows, so does the public's concern about their protection. As the Internet of Things (IoT) grows in popularity among the general public, protecting against cyber-attacks becomes more complicated. The Internet of Things (IoT) is increasingly merging with cloud computing and other platforms, raising concerns about its inherent vulnerabilities. As a result, in this paper, we've identified a range of cyber security threats that Internet of Things (IoT) applications face, as well as countermeasures to make IoT a more stable and safe framework.

Mamoona Humayun, Mahmood Niazi, NZ Jhanjhi, Mohammad Alshayeb & Sajjad Mahmood [12] they have proposed to discover and examine common cyber security flaws. A systematic mapping research was undertaken to achieve this aim, resulting in the identification and analysis of 78 primary studies in total. In the initial search process, 162 studies were chosen. A total of 78 papers were chosen in the final iteration based on the inclusion and exclusion criteria. Malware, phishing, SQL injection attacks, cross-site scripting (XSS), denial-of-service (DoS), session hijacking, man-in-the-middle attacks, and credential reuse are some of the most common vulnerabilities discovered in our mapping research. In the systematic mapping analysis, denial-of-service is the most discussed vulnerability (37 percent). Malware (21 percent), led by phishing, is the second most widely discussed vulnerability in the literature.

Edward S. Chang; Aridaman K. Jain; David M. Slade; S. Lee Tsao[13] they define a methodology for statistical sampling and analysis, as well as a network and host security discipline, for effectively and efficiently creating Lucent's cyber security profile. We've also devised a tool for identifying and correlating vulnerabilities in network and operating systems. By weakness, we mean the system's possible vulnerabilities that render it vulnerable to attack. The assessment of these system vulnerabilities allows for the identification and development of new techniques to protect the system from harm. This paper focuses on the use of various vulnerability scanners and their associated methodologies to detect various vulnerabilities in web applications or remote hosts across the network, as well as new methods that can be deployed to protect the network.

Angel Rajan, Emre Erturk[14] they proposed the Automated Network Vulnerability Scanners (WVS) assist in the detection of web application vulnerabilities. One of the most commonly used vulnerability scanners is Acunetix. Acunetix is also simple to set up and use. The scan results provide not only the specifics of the vulnerabilities, but also information about how to repair

them. Acunetix's technologies AcuSensor and AcuMonitor aid in the generation of more reliable possible vulnerability results. Online Vulnerability Scanners (WVS) aid in the speeding up of the vulnerability testing process for websites and web applications. This case study, which uses Acunetix as an example, is useful for familiarising students with the fundamentals of a WVS. Some protection tools are geared toward reviewing company websites, while others are geared toward handling the company's mobile devices. Scanning mobile devices for security vulnerabilities and highlighting vulnerable applications is useful for both app designers and IT support (Revankar, 2015).

Yan Wang, Peng Jia,Luping Liu, Cheng Huang, Zhonglin Liu[15] they proposed machine learning methods have been implemented as a new approach of fuzz testing. This paper examines recent research on using machine learning techniques for fuzz testing, analyses how machine learning enhances the fuzzing process and outcomes, and speculates on future fuzzing work. This paper investigates machine learning-based fuzzing models from five perspectives: algorithm collection, pre-processing methods, datasets, evaluation metrics, and hyperparameter environment. Second, this paper evaluates the efficiency of machine learning techniques for fuzz testing in established research. The evaluation's findings show that machine learning techniques have a fair capacity to predict fuzzing. Finally, both conventional fuzzers and machine learning-based fuzzers are evaluated for their ability to discover vulnerabilities.

III. PROPOSED MODEL

The proposed system defines the vulnerability assessments system we are using. The scanner is implemented in Python using an opensource tool. The DNS visual mapping in this project uses DNS dumpster, WHOIS information, TLS Data - supported ciphers, TLS versions, certificate details, and SANs, Port Scan, Services and scripts scan, URL fuzzing and directory/file detection, Subdomain enumeration - uses Google Dorking, DNS dumpster queries, SAN discovery, and brute force. To determine the website's vulnerabilities in order to enhance its security features. Numerous vulnerabilities exist on the website, and passwords are stored in a database. They are hacker-friendly. The scanner should be constructed in such a way that it is capable of scanning the entire website for vulnerability threats..

Vulnerability scanners identify and create an inventory of all of systems (servers, workstations, virtual machines, firewalls, and printers, for example) on a network, including ones that may have yet to be connected. it also performs variously recognises other devices and other properties, such as whether the device is open or closed, along with the operating system and any software attributes, and establishes user accounts in the operating system for each device it. When planning to conduct a vulnerability check, most tools may try to access default or widely used accounts in order to collect a more thorough view of the system.When it has compiled an inventory, the scanner tests each object against one or more pre-known vulnerabilities to see whether it is subject to any of them. In the event of a vulnerability scan, you will obtain a list of all systems found and listed as vulnerable, those that require attention will be marked. the system database wordlist is used in the scanner to find the expansion. The concerns and security measures mentioned below are about the network's security.

Threats	**Security properties**
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information disclosure	Confidentiality
Denial of service	Availability
Elevation of privilege	Authorization

Table1Threats and security properties of the network

In order for this system to grow, it is necessary that the software and hardware are developed simultaneously. Requirement analysis involves deciding the product's requirements and conditions by taking into consideration of all possible user needs. Input data are required for performing the task analysis, as well as the output data that results from performing the task.Vmware, virtualbox.,os:kalilinux, hdd:20gb, ram:8processor:intel i5, amd ryzen 5 are the hardware requirements . Browser -Google Chrome, Apple Safari, Mozilla Firefox, Internet Explorer, Operating System Linux, windows,, Mac. Programming language – Python 3.4 are the Software requirements used. The process of defining a system's architecture, components, modules, interfaces, and data to meet defined specifications is known as design. Also includes details about the system architecture, as well as its implementation. This system describes how it is constructed as well as what it does. System architecture explains a model's process in depth and assists us in obtaining a good understanding of the purpose executed by that model. The proposed model's system architecture is defined in, which includes the specifics of the mechanism that is carried out to ensure proper implementation. A vulnerability scanner is made up of four main components: a

Search Module, a Database Module, a Report Engine, and a User Interface. 1.All vulnerability search logic is implemented in the Scan Module, which performs device checks for vulnerabilities in compliance with the required settings. Depending on how the module is implemented, Fig 1. shows to search several resources in parallel. 2.The Database Module is a specialised database that stores information on vulnerabilities and how they are exploited (for the attacks). These data are followed by a recommendation on how to subdomain takeover may be major. Attackers may use a subdomain takeover to send spam email from the authorized domain conduct cross-site scripting (XSS), fix vulnerabilities; following the recommendations decreases the risk to the system's protection. The database is mainly used for security and intrusion detection analysis. 3.Report Engine produces reports detailing the discovered vulnerabilities based on the collected data. An significant thing to note is that the report includes suggestions for resolving the issues identified.

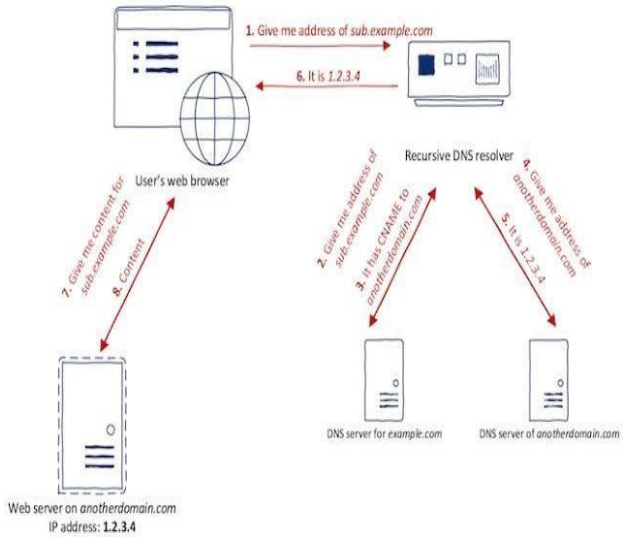

Fig 1.Subdomain Takeover

Detailed reports assist in removing the problem as soon as possible.Detected bugs without wasting time looking up details of discovered vulnerabilities The report is available in a format that is easy for the end user. 4.Users can use the UI to run the vulnerability scanner. The majority of scanners would have a graphical user interface, with the option to run the scanner exclusively via a command line interface. Most vulnerability scanners have a modular architecture, which is useful because it allows you to switch off specific features. Begin scanning based on the parameter you've chosen. The architecture includes the following elements.

A subdomain, such as help.yourdomainname.com, is a variation or forwarder address derived from your root domain name. The process of registering a non-existing domain name in order to obtain ownership of another domain. Subdomains are normally set up by your IT department, webmaster, or you for use with 3rd party services such as helpdesk applications, calendar, or mail apps, and are rarely used to host a micro website. The web browser will be given an input, such as sub.example.com. The provided input will be recursively processed and sent to the DNS server. The DNS server analyses the data and returns it to the DNS resolver. It retrieves all relevant websites and returns them to the browser. The browser searches the web server for the right match and shows the relevant website to the client. The consequences of a or impact the brand associated with the domain's credibility.

There's an explanation why this happens so frequently: Though cloud hosting is usually expensive, having a stale DNS entry is usually free. As a result, while there is an opportunity to remove inactive webpages, DNS entries are often overlooked. An intruder can now reregister the host with the cloud provider, add the organization's subdomain as an alias, and thus control what is hosted. There are many ways to expand this attack, but one is by giving the cloud DNS manager the ability to register names in the NS records of a given set of DNS.by installing the application or they can view the live video in the live video interface unit present in the drone unit. The prevention of subdomain takeovers is operational to lifecycle management in virtual hosts and DNS. this may increase the likelihood of vulnerable misconfiguration due to communication across multiple departments Develop the standard processes of provisioning and de- and de-provisioning hosts. Make everything as consistent as possible while you do the steps are proceeding.Before you can implement, you must first claim the virtual host; then, you must create DNS records.

Start taking care of the deprovisioning DNS records first. In case your organisation adds, changes, or loses a domain, you should have a current inventory of their service providers so you do not go into unnecessary amounts of money. If a vendor will notifies you of gaps in the vendor acceptance of a virtual host (by contacting you with some technical message), pressure them to verify the legitimacy of the host claim. This is part of the vendor qualification process that you can participate in on by working with your company.

For Linux users, it can be downloaded from the GitHub repository, but it is already included in Kali Linux. Applications -> Kali Linux - > Web Applications -> Web Crawlers -> dirbuster

Users of Windows: You can get it from the internet, sourceforge, or the website of the Open Web Application Security Project (OWASP).

NB: Because it is a multi-threaded Java application, Jre/Jdk (JAVA) must be installed on the system to be used.When it is

released, The Graphical User Interface(GUI) should resemble the dirbuster GUI.Enter the URL and port number of the website to be scanned (http://example.com:80/) as shown in the target URL example.

Wordlist Selection: From the GUI, navigate to where it says file with list of dirs/files, then click on the list info to see a list of available wordlists and their descriptions. Choose the required wordlist and paste it into the File with dir/file field. For Linux users, for example, /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt. For Windows users, the directory containing the wordlist should be included.

IV. RESULTS AND DISCUSSIONS

The project created a new framework as a solution and enhancement for retrieving information based on user interest. What the system shows is that the proposal achieves is to do is expand the usability of the web. when a query is made to look up a specific URLs, searching for the maximum number of occurrences can be done easily; likewise, the problem of finding more URLs can be made simpler when the parameters are already in the account for this when searching for specific ones In traditional browsers, it takes longer to retrieve larger amounts of time to narrow down the results. However, we have found that the method works, we have also discovered that it is a little more efficient without requiring any problematic actions on the part of the user. The model is highly accurate in identifying the user interest based on what keywords are entered into the URL. It assists users in collecting additional information about the URL being searched. To verify the strength of the password stored on the website, the word list is bruteforced. It will compare the current passwords in the DNS record in a more meaningful way. future iterations may provide additional effectiveness when developing/better communicating the queries and output can be developed closer to those that connection

REFERENCES

[1] SandeepKumarYadav, Daya Shankar Pandey, Shrikant Lade,“ A Comparative Analysis of Detecting Vulnerability in NetworkSystems,” Volume 7, Issue 5, May 2017.
[2] Mansour Alsaleh, Noura Alomar, Monirah Alshreef, Abdulrahman Alarifi, and AbdulMalik,Al-Salman , “Performance-Based Comparative Assessment of Open Source WebVulnerabilityScanners,”Publication 2017.
[3] Sheetal Bairwa, Bhawna Mewara and Jyoti Gajrani, “Vulnerability Scanners: A Proactive Approach to assess Web ApplicationSecurity,” Vol.4, No.1, February 2014.
[4] Mohamed Abomhara, Geir M Koien, “Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders andAttacks,”Volume4,Publication2015.
[5] Jun Li, Bodong Zhao & Chao Zhang,“ Fuzzing: a survey, ”Published:05June2018.
[6] Jagtap,PrajaktaSubhash,JSomaiya,“VulnerabilityScanning,”Publication 2012.
[7] Nabie YConteh,Paul,J. Schmick,“ Cybersecurity Risks, vulnerabilities and countermeasures to prevent social engineering attacks,”Publication Feb 2016.
[8] GazalOjha,ManjuKaushik,“Attack Penetration System for SQL Injection,”Publication April 2020.
[9] Omar Y.Sharkasi,“ Addressing Cybersecurity Vulnerabilities ,” ISACA Journal Volume 5 ,Published: 1 September 2015.
[10] Avinash Kumar Singh,Sangita Roy,“A network based vulnerability scanner for detecting SQLI attacks in web applications,”Publication March 2012.
[11] Ankit Dhatrak, Anshuman Sarkar,“Cyber Security Threats and Vulnerabilities in IoT, ”Volume: 07, Issue: 03 Mar 2020.
[12] Mamoona Humayun, Mahmood Niazi, .NZ Jhanjhi, Mohammad Alshayeb & Sajjad Mahmood , “Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study,” Published 06 January 2020.
[13] Edward S. Chang,Aridaman K,Jain,David M Slade, S.Lee Tsao, “Managing cyber security vulnerabilities in large networks,” Volume 4,Publication 14August 2002.
[14] Emre Erturk, Angel Rajan,“ Web Vulnerability Scanners: A Case Study,” Published June 2017.
[15] Yan Wang, Peng Jia,Luping Liu, Cheng Huang, Zhonglin Liu,“ A systematic review of fuzzing based on machine learning techniques,” Published 2020 Aug 18.