IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Cyber Defence: A Hybrid Approach for Information Gathering and Vulnerability Assessment of Web Application (Cyberdrone)

Dixitkumar .V. Prajapati[1*], Deepak Upadhyay[2]

[1,2]GTU Cyber Security, Graduate School of Engineering & Technology, Gandhinagar 382028, Gujarat, India

[*]*Corresponding Author: dixitprajapati99@gmail.com, Tel.: +91-96388-39974*

DOI: https://doi.org/10.26438/ijcse/v7i5.6572 | Available online at: www.ijcseonline.org

Accepted: 15/May/2019, Published: 31/May/2019

***Abstract*—** web application information gathering (IG) and vulnerability assessment (VA) is an important step to protect the cyber defense of systems or networks and live web applications. Day by day growing internet connection everywhere remains connected to each other in the world. Web application security major captative of all cyberspace in information gathering. So there is various kind of tool available in the world for website information gathering and vulnerability assessment. Vulnerability assessment and web application information gathering tools have own format and functionality. Mostly information gathering and vulnerability assessment tools are too much costly and also some tool is open source. In market various information gathering and vulnerability assessment tools are available but they are not able to give 100 % accuracy and solution to find out particular vulnerability as per CWE. Our approach to combine multiple information gathering and vulnerability assessment tools (open source). The (Cyberdrone) tool will approach to provide good timing accuracy and efficiency also more security open source effective solutions for information gathering and vulnerability assessment on a web application. Easy to download proper reports and time will decrease using automated tools compare to manual testing.

***Keywords*—** web application, information gathering, vulnerability assessment, open source intelligence (osint) tool, and scheduler**.**

I. INTRODUCTION

Nowadays various kind of web application is launched on the World Wide Web. There are different categories of web applications. The volume of WWW (the internet) the web contains indexed at least 4.45 billion pages and the web contains Dutch indexed at least 145.64 million pages up to (Sunday, 28 October 2018) [1].

A web-application or site is a focal area of different website pages that are altogether related and can be accessed by visiting the landing page utilizing a program. Site in a manner is a joining of related interactive media content that can be gotten to utilizing a space connects. Some trendy sites incorporate Shopping (E-trade) (Amazon, Flipkart, ebay), Social Media (Facebook, Twitter, Instagram), Blogs (Business, Lifestyle, Personal), Online Gaming, Informational/Education, (Udemy, Coursera) Online Business Brochure/Catalog Websites.

Comprehensively we can classify sites into three wide ranges mostly, static, dynamic and glimmer. These sites are facilitated in various areas like .com, .in. Co. In and some more. In view of the stage like HTML, CSS, XML and implanted with CSS, javascript and some more, sites structure a graphical UI. With time, the innovation is improving, with it, the valor of sites is expanding and as the valor increment the danger likewise increments. Basically saying that however we attempt our most great to make the best sites that are easy to use and verify yet there are a few vulnerabilities or gaps that now and again goes about as vectors for assaults like SQL infusion, support flood, XSS(cross site scripting), and some more. Thus we grandstand a few stages, dialects, vulnerabilities, assaults and countermeasures in connection to sites.

The rest of paper organized as follow: Segment 2 web application. Segment 3 information gathering. Segment 4 vulnerability assessment life cycle and it's impact factor. Segment 5 literature review. Segment 6 why hybrid approaches for web application testing. Segment 7 proposed cyber drone. Segment 8 conclusion and future work.

II. WEB APPLICATION

A Web application (WA) is one sort of utilization program that is put away on a remote server and furthermore conveyed over the mode of the web a program interface. Generally, web application proposes by client necessities. Web applications have content, work, security, database and some more [18].

© 2019, IJCSE All Rights Reserved

III. INFORMATION GATHERING

First, we have to understand why information gathering is required, An Information gathering helps the target of an individual or an organization to carry out difficult steps that very hard to achieve if it is doesn't benefit so it's not worth fully. As we know information gathering is the art and act of collecting meaningful data from a various place or sources. Information gathering is also part of the footprinting [21] [23].

IV. VULNERABILITY ASSESSMENT

This is a central errand for an infiltration analyzer to find the vulnerabilities in a domain. Defenselessness appraisal incorporates finding shortcomings in a domain, plan defects and other security concerns which can cause a working framework, application or site to be abused. These vulnerabilities incorporate mis-configurations, default setups, cushion floods, Operating System blemishes, Open Services, and others. There are diverse apparatuses accessible for system managers and Pen testers to examine for vulnerabilities in a system. Found vulnerabilities are ordered into three distinct classes dependent on their security levels, i.e., low, medium or high. Besides, they can likewise be classified as endeavor range, for example, neighborhood or remote. Vulnerability assessment Helplessness Assessment can be characterized as a procedure of examination, disclosure, and recognizable proof of framework and applications safety efforts and shortcomings. Frameworks and applications are analyzed for safety efforts to distinguish the adequacy of sent security layers to withstand assaults and abuses. Powerlessness evaluation likewise perceives the vulnerabilities that could be abused, need of extra security layers, and data's that can be uncovered utilizing scanners [22].

Vulnerability Assessment Life-Cycle

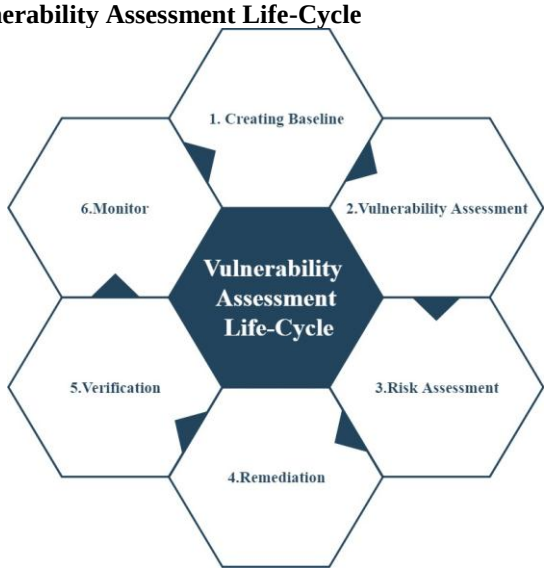

Figure 1:- Vulnerability Assessment Lifecycle.

Vulnerability Assessment life cycle incorporates the accompanying stages:

1) **Creating Baseline:** Making Baseline is a pre-appraisal period of the weakness evaluation life-cycle in which pentester or organizes head who is performing evaluation distinguishes the idea of the corporate system, the applications, and administrations. He makes a stock all things considered and resources which oversees, organize the appraisal. Besides, he likewise maps the framework, finds out about the security controls, arrangements, and benchmarks pursued by the association. At last, standard plans the procedure successfully, plans the errands and oversee them concerning need.
2) **Vulnerability Assessment:** The helplessness Assessment stage is centered on the evaluation of the objective. The evaluation procedure incorporates examination and investigation of safety efforts, for example, physical security just as security strategies and controls. In this stage, the objective is assessed for misconfigurations, default designs, flaws, and different vulnerabilities either by examining every part exclusively or utilizing appraisal devices. When examining is finished, discoveries are positioned as far as their needs. Toward the finish of this stage, certified Ethical Hacking ipspecialist.net 14-May-2018 217 weakness appraisal report demonstrates every recognized helplessness, their degree, and needs.
3) **Risk Assessment:** Hazard Assessment incorporates perusing these distinguished vulnerabilities and their effect on the corporate system or on an association.
4) **Remediation:** The remediation stage incorporates medicinal activities for these distinguished vulnerabilities. High need vulnerabilities are tended to first since they can cause an enormous effect.
5) **Verification:** The Check stage guarantees that all vulnerabilities in a situation are dispensed with.
6) **Monitor:** Observing stage incorporates checking the system traffic and framework practices for any further interruption.

Vulnerability Severity and Impact Analysis:

OWASP and SANS give the rundown of standard most prominent normal and perilous security vulnerabilities. In light of the rundown of vulnerabilities they are given the rank of security level and there effect. An association Mitre organization additionally institutionalized the general language of a wide range of vulnerabilities. Here we characterize the language of CWE-normal shortcoming count. Each weakness has possessed CWE code to slant the over the globe. Table no-1 was demonstrated the OWASP establishment kept up the top ten vulnerabilities list and furthermore rank and CWE code. All helplessness for the most part dependent on web applications. Table no-2 portrays about the CWE/SANS establishment top 2 vulnerabilities. Rundown of 2 vulnerabilities was referencing a wide range of utilization. These all are kept up by sans and

© 2019, IJCSE All Rights Reserved

soil enterprise groups. They are building up the seriousness of defencelessness and class. The weakness gives the trade off the most basic security essentials and streams. After the weakness evaluation estimation additionally before we are making arrangements for entrance testing. And furthermore, these are a guide of vulnerabilities rundown and better methodology of security and distinguish the issue [3].

Table no 1: OWASP top 10 vulnerability list CWE [3]

Rank	CWE	VULNERABILITY NAME.
A1	1027	Injections.
A2	1028	Broken Authentications.
A3	1029	Sensitive Data Exposures.
A4	1030	XML External Entities (XXE).
A5	1031	Broken Access Controls.
A6	1032	Security Misconfigurations.
A7	1033	Cross-Sites Scripting (XSS).
A8	1034	Insecure Deserialization.
A9	1035	Using Components with Known Vulnerabilities.
A10	1036	Insufficient Logging & Monitoring.

Table no 2: CWE/SANS top 25 list-2018 [4].

DIVISION	VULNERABILITY NAME	CWE ID
Insecure Interaction Between Components	Improper Neutralization of Special Elements use in an SQL Command ('SQL Injection').	CWE-89
	Improper Neutralization of Special Elements use in an OS Command ('OS Command Injection').	CWE-78
	Improper Neutralization of Input During Web Pages Generation ('Cross-site Scripting').	CWE-79
	Unrestricted Upload of File with Dangerous Types.	CWE-434
	Cross-Sites Request Forgery (CSRF).	CWE-352
	URL Redirection to Untrusted Sites ('Open Redirect').	CWE-601
Risky Resource Management	Buffer Copy without Checking Size of Inputs ('Classic Buffer Overflow').	CWE-120
	Improper Limitations of a Pathname to a Restricted Directory ('Path Traversal').	CWE-22
	Download of Codes Without Integrity Check.	CWE-494
	Inclusion of Functionality from Untrusted Control Spheres.	CWE-829
	Used of Potentially Dangerous Function.	CWE-676
	Incorrect Calculations of Buffer Sizes.	CWE-131
	Uncontrolled Format Strings.	CWE-134
	Integer Overflow or Wraparounds.	CWE-190
Porous Defenses	Missing Authentication for Critical Functions.	CWE-306
	Missing Authorizations.	CWE-862
	Uses of Hard-coded Credentials.	CWE-798
	Missing Encryption of Sensitive Data.	CWE-311
	Reliance on Untrusted Inputs in a Security Decision.	CWE-807
	Execution with Unnecessary Privileges.	CWE-250
	Incorrect Authorizations.	CWE-863
	Incorrect Permission Assignment for Critical Resources.	CWE-732
	Use of Broken or Risky Cryptographic Algorithms.	CWE-327
	Improper Restrictions of Excessive Authentication Attempts.	CWE-307
	Use of a One-Way Hash without Salts.	CWE-759

V. LITERATURE REVIEW

A survey regarding which kind of information gathering and vulnerability assessment on web application XSS recognition instrument which presents JSP indicator that scours the weakness in the website page that plays out a mechanized procedure to separate between javascript codes from a malevolently infused code and furthermore ad lib the productivity of a quick strategy check to upgrade the speed of XSS assault identification process [26]. The creator discusses different sorts of an assault like SQL infusion, CSS, broken validation and session the board, unreliable direct item reference, inability to confine URL, remote code execution and advantages of VAPT with a danger of VAPT [27]. The instrument can discover the vulnerabilities to the present security perspectives and ensure to digital assault and some great open or free source device for testing reason [5] .same author provides a solution to make one device for performing such sort of testing NETNIRIKSHAK 1.0 and this vapt test was lead on www.webscantest.com[6]. Vapt device can be incorporate how the instruments are utilized in digital resistance additionally join framework security (SS) and the author was clarified of utilizing vapt on framework security [7]. The same author extending strategy for

© 2019, IJCSE All Rights Reserved

examination instrument accuracy 'vensemble 1.0 [8]. Authors are creating half and half calculation SQL Algorithm and XSS Algorithm. Use Vulnerability scanners and web applications to investigation using the tool of Ck appscan and wvs [9]. Increment the calculation creeping segment so as to guarantee that it executed "profound" slithering. Describe Web application VA testing approach and w3af and Nikto tool for finding vulnerability [10]. Discover utilizing mechanized pen testing programming. Acunetix discovers basic dangers are tried. Powerless product patching (1) patching auth bypassing (2) patching association infusion (3) configuring firewall [11]. Fix Sqli And Blind Sqli Vulnerabilities 1) Prepared Statements (with Parameterized Queries) 2) Stored Procedures 3) Input Validation 4) Escaping All User Supplied Input 5) Least Privilege. Answers for Fixes XSS Vulnerabilities 1) Data Validation, 2) Data Sanitization 3) Output Escaping [12]. Perform Vulnerability investigation on notice tool. Total time is taken to finish helplessness filtering utilizing strategy (essential, middle, advance). Which device should the client select and there are separated into four sections A)motivation behind the checking B)cost C)programming support D)productivity using tool of 1) Nessus 2) acunetix - web weakness scanner 3) OWASP Zed assault intermediary (ZAP) [13]. Currently the security dangers of the web-based business site. Kinds of digital assault like Denial of administration assaults, SQL infusion, take client data. OWASP top ten security dangers and E-business site security evaluation framework module have two sections 1) test module2) appraisal module and Analytic chain of command process (in light of grid hypothesis) [14]. The Google hacking database (GHDB). Jsoup (java library that gives advantageous API to extricate and control information utilizing the best of DOM (archive object demonstrate), CSS (course templates) and jquery-like strategies) [15]. Systems advancement lifecycle (SDLC) seven stages 1) prerequisites definition, 2) engineering and structure, 3) execution, 4) testing, 5) sending, 6) support, 7) transfer. Early-cycle digital vulnerability assessment (ecvas) Types of ecvas Requirements CVA (rcva), an engineering and plan CVA (acva), an execution CVA (icva) [16]. Vulnerability assessment for crisis reaction plan dependent on Vulnerability evaluation, Natural dangers, Medical weakness (wellbeing hazard), Social powerlessness (calamity strikes) [17].

VI. WHY HYBRID APPROACH

The present universes there are different strategies are accessible to make a diverse thing to doing cross breed things. Crossbreed approach is a consolidates an assortment of strategies to create suggestion so as to join the strength and dispose of the downsides of the individual systems Half breed approach is a blend of two distinct philosophies or frameworks to make another and better model. Half and half philosophies acknowledge the smoothness of activities and take into consideration a progressively deft and nuanced way to deal with the work. Here we utilizing half and half methodology to make an errand to applying distinctive things. Here we are doing making web applications dependent on the consolidating two distinctive things for the same assignment and target [26] [27].

The web application has consolidated different devices and systems of data social affairs and weakness evaluation on a web application.

Highlights:
1) Can work whether the gadget is associated
2) Integration with document gadget's framework
3) Web-based administrations with incorporation.
4) An embedded program to improve got to dynamic online associates.

Here beneath we seen the figure of half breed approach for web application.

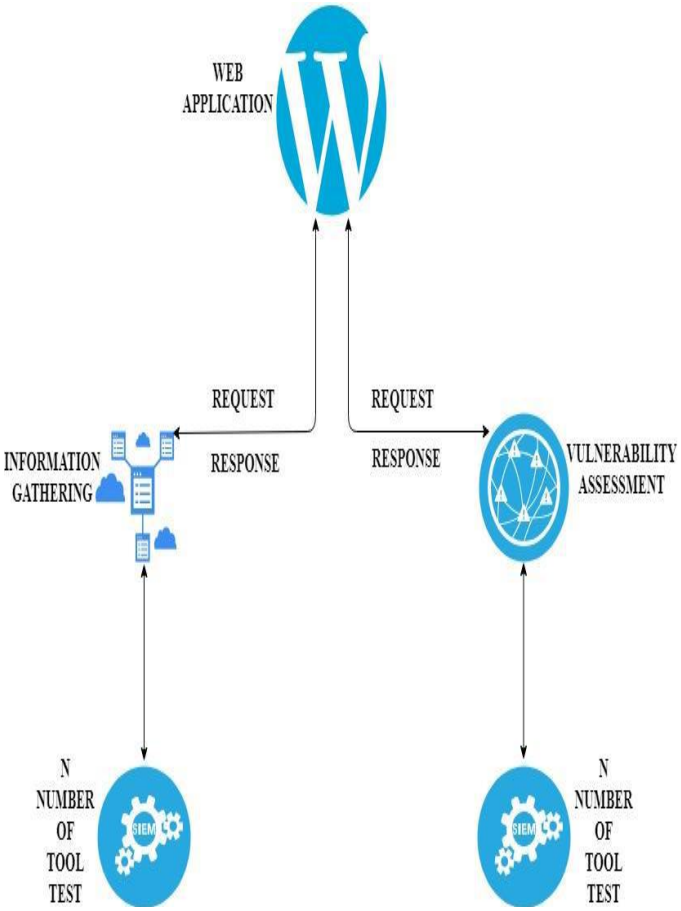

Figure 2: Hybrid Approach for Web Application

VII. PROPOSED CYBERDRONE

1) **Proposed Method**

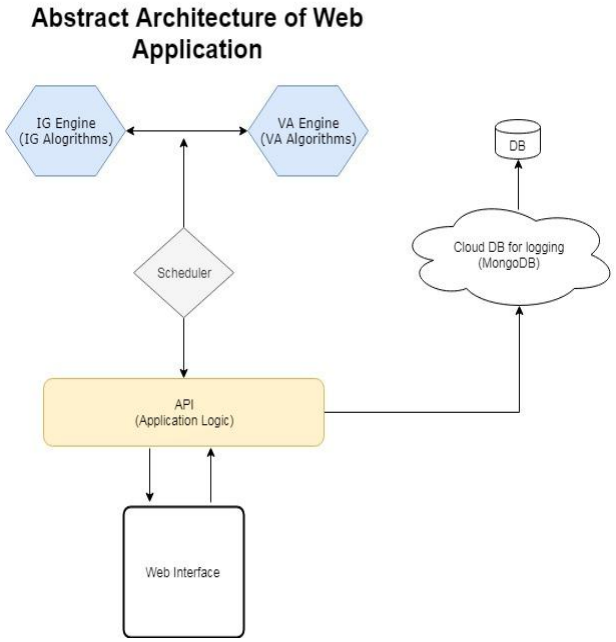

Figure 3- Proposed Method

2) **Flowchart of CYBERDRONE**

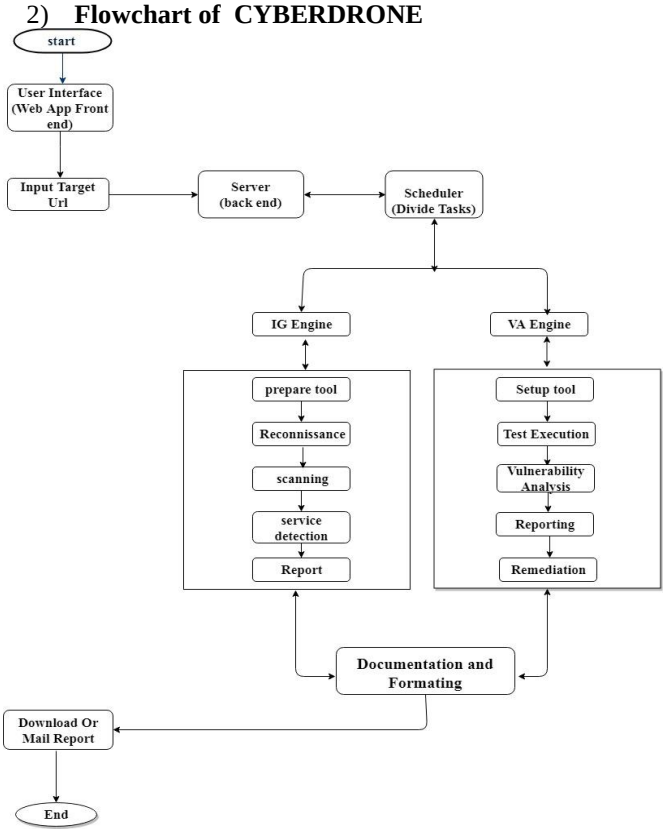

Figure 4: Flowchart of Cyberdrone

Method Description:-

Here fig-13.1 has characterized a proposed framework design of web application. This web application separated into two sections. 1) Front end (client side), 2) backend (server side). In front end client can enter just URL or focus on web application now the client will sit tight for procedure time. Here back end side API will get the objective URL. Presently API call scheduler to perform task dependent on Logic. Presently scheduler will separate into two sections 1) IG Engine, 2) VA Engine. IG motor methods data social event and VA Engine implies Vulnerability appraisal. Presently IG Engine has an instrument rundown and target then scheduler was isolated undertaking into multi stringing same as VA Engine. Furthermore, when the sum total of what task has been done as such a report will be created.

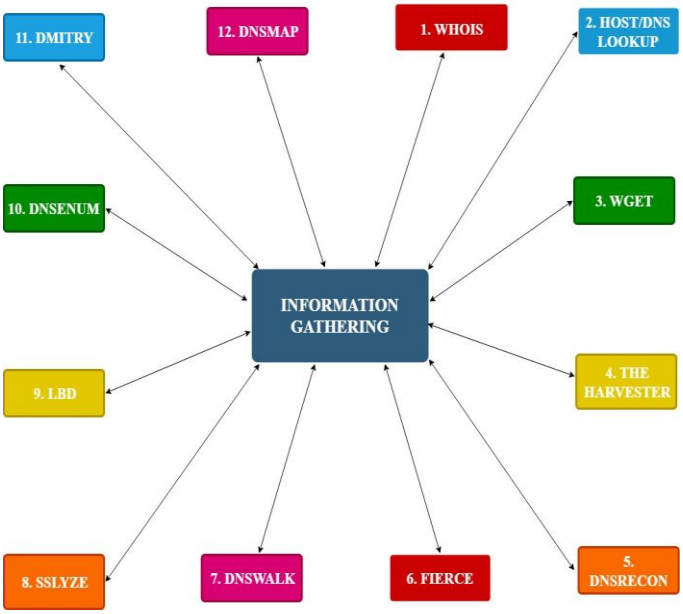

Figure 5: IG Engine Tool List [24] [25].

Figure 6: VA Engine Tool list [24] [25].

© 2019, IJCSE All Rights Reserved

3) **Scheduler:**

Here we have seen the diverse kinds of the scheduler and how they are functions. We are utilizing scheduler for jumping task for various reason. Here we are utilizing transient scheduler and FCFS (first started things out serve) in view of administrations. Our scheduler all instrument works parallel at the same time. Our principal thought process is decline time to perform data social occasion and weakness evaluation on a web application.

Scheduler has partitioned tasks into strings. So execution is quicker than others. Assume we are utilizing distinctive apparatus for doing numerous things so we can say there are times taken are high. So here are basically made from the client side enter just url. What's more, our web application can as quickly as time permits done the errand send the fitting report to you [20] [21] .

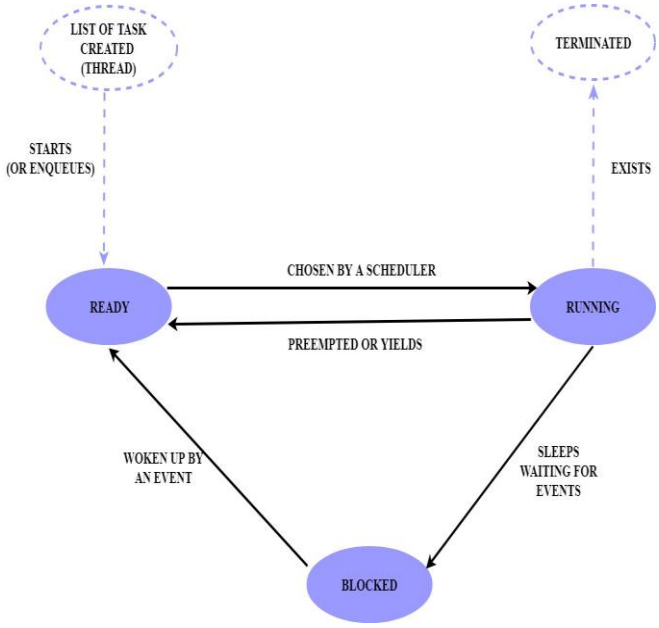

Figure 7:- How Scheduler Works

Here we seen the figure of scheduler and how its work. Scheduler gets the request from the user. Scheduler divides the task parallel and also parameter gets automatically from targeted URL.

4) *Performance measure and experimental results:*

Strategy and Technology

Front end (Web interface) :

- Html5, css3, javascript
- Frameworks: Angular 7, Bootstrap

Backend (Server):

- VA and IG Engine & Scheduler Python 3.7.x
- API: Python 2.7 & Python-Flask(Framework)
- IAAS: AWS Lambda (Amazon Web services)

Testing Environment

- **Hardware:** Asus Intel I7, Graphics Card- 4 GB, Ram 16 GB, Hard disk -1TB.
- **Software**: Ubuntu Os.
- **Internet Speed** – 10 Mbps (Tikona Broadband)

Table No 3: Comparison of Manual Testing and Cyberdrone Automated Tool (IG= Information Gathering, VA= Vulnerability Assessment)

SR NO	TOOL NAME	TOOL TYPE	TIME TAKEN INDIVIDUAL PERFORMING TOOL	CYBER DRONE
1	Host/dns lookup	**IG**	3 S	6878 Sec
2	Wget	**IG**	4 S	
3	The harvester	**IG**	12 S	
4	Dnsrecon	**IG**	7 S	
5	Fierce	**IG**	1413 S	
6	Dnswalk	**IG**	14 S	
7	Whois	**IG**	9 S	
8	Sslyze	**IG**	3 S	
9	Lbd	**IG**	4 S	
10	Dnsenum	**IG**	2 S	
11	Dmitry	**IG**	182 S	
12	Dnsmap	**IG**	723 S	
13	Nmap	**VA**	48 S	
14	Golismero	**VA**	3218 S	
15	Nikto	**VA**	1981 S	
16	Wapiti	**VA**	1302 S	
17	Whatweb	**VA**	72 S	
18	Uniscan	**VA**	549 S	
19	Wafw00f	**VA**	34 S	
20	Dirb	**VA**	20853 S	
21	Davtest	**VA**	28 S	
22	Xsser	**VA**	163 S	
TOTAL TIME IN SECOND			**30624 SEC**	**6878 SEC**
TOTAL TIME IN HOUR			**8 H, 50 M,6 S**	**1H, 54 M, 38 S**

Testing Timing Approx Ratio – 4: 1

5) Cyberdrone checks vulnerability:

1) DNS/HTTP load balancer & web application firewalls.
2) Check for Joomla, wordpress, and Drupal.
3) SSL related vulnerabilities (freak, ccs injection, heartbleed, poodle, ocsp stapling, logjam)
4) DNS zone transfer
5) Commonly open ports.
6) Sub-domain brute forcing.
7) Open directory/ file brute forcing.
8) Shallow xss, sqli, bsqli banners.

© 2019, IJCSE All Rights Reserved

9) Slow-loris dos attack, lfi (local file inclusion), RFI (remote file intrusion) & rce (remote code execution).

VIII. CONLCUSION AND FUTURE WORK

As indicated by survey assaults just as Cyber-violations are immediately created and they making a gigantic measure of dangers identified with government and modern locales. We secure the secrecy and uprightness and accessibility of data security to ensure the dangers. Here we proposed the answer for web application testing and utilizing a hybrid approach for the information gathering and Vulnerability assessment (VA) in a digital barrier. We have created a web application mechanized web application testing web application. It's incredibly supportive to the customer basically enter focused on URL and sit tight for a long time and get a reasonable report direct association and report need to list data of the objective and furthermore discover a rundown of defenselessness and remediation with legitimate way. In the future, we are intending to make a straightforward web application. Besides, the customer can not keep it together for the report. Right when the customer enters URL for testing target urls than one popup open and solicitation customer mail id for sending a report. A report will send as fast as time licenses. What's more, moreover, we are incorporating more instruments in this web application.

ACKNOWLEDGMENTS

I specially thankful to Deepak Upadhyay, Assistant Professor of GTU-Graduate School of Engineering and Technology for providing us infrastructure, motivation at Collage.

REFERENCES

[1] The size of the World Wide Web (The Internet) http://www.worldwidewebsize.com/ access on 27 October-2018.
[2] Khushal Singh, Vikas, "Analysis of Security Issues in Web Applications through Penetration Testing", International Journal of Emerging Research in Management &Technology, Volume 3, March 2014.
[3] Creative common attribution. " Top 10-2017 Top 10" access on 10 august, 2018. Https://www.owasp.org/index.php/Top_10-2017_Top_10.
[4] CWE view: weaknesses in owasp top ten(2017) https://cwe.mitre.org/data/definitions/1026.html access on 23 october,2018
[5] Sugandh Shah, B.M. Mehtre, "A Reliable Strategy for Proactive Self-Defence in Cyber Space using vapt tools and Techniques" IEEE International Conference on Computational Intelligence and Computing Research- 2013
[6] Sugandh Shah, B.M. Mehtre, "An Automated Approach to Vulnerability Assessment and Penetration Testing using Net-Nirikshak 1.0" IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT) -2014
[7] Jai Narayan Goel, Mohsen Hallaj Asghar, Vivek Kumar, Sudhir Kumar Pandey "Ensemble Based Approach to Increase Vulnerability Assessment and Penetration Testing Accuracy" 1st International Conference on Innovation and Challenges in Cyber Security (ICICCS 2016)
[8] Jai Narayan Goela, BM Mehtreb "Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology" Peer-review under responsibility of organizing committee of the 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015) doi: 10.1016/j.procs.2015.07.458
[9] Muiruri Chris Karumba, Samuel Ruhiu, Christopher A. Moturi "A Hybrid Algorithm for Detecting Web Based Applications Vulnerabilities" American Journal of Computing Research Repository, 2016, Vol. 4, No. 1, 15-20
[10] Robert Vibhandik ; Arijit Kumar Bose "Vulnerability assessment of web applications - a testing approach" 2015 Forth International Conference on e-Technologies and Networks for Development (ICEND)
[11] Insha Altaf, Firdous ul Rashid. Jawed Ahmad Dar, Mohd. Rafiq "Vulnerability Assessment and Patching Management" 2015 International Conference on Soft Computing Techniques and Implementations (ICSCTI)
[12] Nor Izyani Daud, Khairul Azmi Abu Bakar, Mohd Shafeq Md Hasan (Malaysia) "A Case Study On Web Application Vulnerability Scanning Tools " IEEE - Science and Information Conference 2014 London, UK
[13] Xia wang, ke zhang, qingtian wu (china) "A Design of Security Assessment System for E-commerce Website" IEEE 2015 8th international symposium on computational intelligence and design
[14] Ahana Roy, Louis Mejia, Paul Helling, Aspen Olmsted (Charleston) "Automation of Cyber-reconnaissance: A Java-based Open Source Tool For Information Gathering" IEEE The 12th International Conference for Internet Technology and Secured Transactions (ICITST-2017)
[15] Sonja Glumich, Juanita Riley, Paul Ratazzi, and Amanda Ozanam (USA) "BP: Integrating Cyber Vulnerability Assessments Earlier Into the Systems Development Lifecycle" 2018 IEEE Secure Development Conference
[16] Arni ariani, john lewis, pradeep K. Ray (china) "The Vulnerability Assessment For Emergency Response Plans" 2016 IEEE international symposium on technology and society (ISTAS).
[17] Dzone Web Dev Zone https://dzone.com/articles/types-of-web-applications-from-a-static-web-page-t access on 29 October 2018
[18] Hybrid approach https://searchsoftwarequality.techtarget.com/definition/hybrid-application-hybrid-app access on 3 march - 19
[19] Scheduler concept https://www.tutorialspoint.com/operating_system/os_process_scheduling.htm access on 27 Jan - 19
[20] Scheduler information https://www.tutorialspoint.com/operating_system/os_process_scheduling_algorithms.htm access on 4 jan-19
[21] Information gathering open source tool list https://securitytrails.com/blog/top-20-intel-tools access on 30 march - 19
[22] Vulnerability assessment tool list https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools access on 2 Feb. – 19
[23] Ethical hacking information gathering https://www.macfro.com/ethical_hacking_information_gathering/ access on 23 October, 2018
[24] Tool information https://www.kali.org/ access on 24 March - 19

© 2019, IJCSE All Rights Reserved

[25] Scheduler concept https://www.tutorialspoint.com/operating_system/os_process_scheduling.htm access on Jan - 19
[26] R. Saliha Bathool, K.Vijayalakshmi "Automated Detection of Legitimate Java Script Code from a Malicious Injected Code and Improvising the Time Efficiency" International Journal of Science Research In Network Security And Communication, volume -5, issue-4, august 2017.
[27] Nidhi Vora, Chandresh Parekh " Vulnerability Assessment and Penetration Testing in Web Application and Its Prevention" International Journal of Scientific Research in Computer Science, Engineering and Information Technology, volume2, issue 6, 2017.

AUTHORS PROFILE

Mr. Dixitkumar .v. Prajapati completed his bachelor degree in Computer Engineering from Ganpat University, Mehsana, and Gujarat, India in the year of 2015. Now pursuing master degree in Computer Engineering (Cyber Security) from GTU - Graduate School of Engineering and Technology.

Assistant Professor Deepak Upadhyay, GTU - Graduate School of Engineering Technology, Gandhinagar. He has 7 years of teaching experience.

© 2019, IJCSE All Rights Reserved